16ª ENTREMENTES
SEMANA ACADÊMICA DA FADISMA
ISSN: 2446-726X Edição: 16ª Ano 2019

AS NOVAS NUANCES DO DIREITO À PRIVACIDADE E À INTIMIDADE ORIUNDAS DA SOCIEDADE DA INFORMAÇÃO: A LEI 13.709/18 E A TECNOLOGIA DA CRIPTOGRAFIA COMO FORMA DE PROTEÇÃO DE DADOS PESSOAIS DO CONSUMIDOR

THE NEW NUANCES OF THE RIGHT TO PRIVACY AND INTIMITY FROM THE INFORMATION SOCIETY: LAW 13.709/18 AND CRYPTOGRAPHY TECHNOLOGY AS A WAY OF PROTECTING CONSUMER PERSONAL DATA

Marcelo Refosco[1]
Cristiane Penning Pauli de Menezes[2]

Resumo
O presente artigo tem como objetivo trazer um dos problemas que a atual sociedade informacional está enfrentando: a exposição de dados pessoais oriundas das relações empresariais digitais. Assim, emerge a necessidade do enfrentamento da tecnologia da criptografia, como meio apto a proteger o consumidor imbricado na era digital. Esse trabalho busca trazer à baila a evolução da criptografia ao longo dos anos, chegando no modelo que é utilizada hoje nas grandes empresas. Assim, buscou-se responder a seguinte problemática: em que medida a tecnologia da criptografia, somada a nova legislação de proteção de dados (Lei 13.709/18), efetivamente traz segurança à proteção de dados do consumidor nas relações digitais? Para tanto, utilizou-se como método de abordagem o dedutivo e como o procedimento o estruturalista. O trabalho foi estruturado em três seções: a primeira buscou trazer a proteção constitucional do direito à privacidade e à intimidade. Em um segundo momento buscou-se explorar a tecnologia da criptografia como mecanismo apto a garantir a proteção de dados e, por fim, buscou-se trazer o estado da arte da proteção de dados pessoais no Brasil. Como resultado parcial verificou-se que a recente Lei Geral de Proteção de Dados Pessoais tem o intuito de dar maior transparência e tutelar mais fortemente o direito à privacidade dos usuários da sociedade informacional, ainda, entendeu-se que em que pese a criptografia auxilie na proteção de dados, ainda é evidente a ausência de legislação que tutele a forma pela qual a criptografia é utilizada. A área de Concentração é Cidadania, Políticas Públicas e Diálogo entre Culturas Jurídicas, a linha de pesquisa, Direito Privado e Repersonalização do Direito Civil e o trabalho encaixa-se no GT de Novos Direitos.
Palavras-chave: Criptografia. Direito à privacidade e à Intimidade. Lei Geral de Proteção de Dados Pessoais. Sociedade Informacional.

[1] Autor. Acadêmico do 8º semestre do Curso de Direito da Faculdade de Direito de Santa Maria - FADISMA. E-mail: mrefosco@terra.com.br.
[2] Autor. Advogada, professora e mestre em Direito. Doutoranda no Programa de Pós-graduação em Processos e Manifestações e Processos Culturais - Universidade Feevale. E-mail: cristiane.pauli@fadisma.com.br

ISSN: 2446-726X Edição: 16ª Ano 2019

Abstract
The present article has as object to bring one of the problems that the current information society is facing: the exposure of personal data from digital business relationships. Thus emerges the need to confront the technology of encryption as a means to protect the consumer embedded in the digital age. This work seeks to bring to light the evolution of cryptography over the years, reaching the model that is used today in large companies. Thus, we sought to answer the following problem: to what extent does encryption technology, added to the new data protection legislation (Law 13.709/18), effectively bring security to consumer data protection in digital relations? Therefore, the deductive method and the structuralist procedure were used as approach method. The work was structured in three sections: the first sought to bring constitutional protection of the right to privacy and intimacy. Secondly, we sought to explore the technology of cryptography as a mechanism capable of ensuring data protection and, finally, sought to bring the state of the art of personal data protection in Brazil. As a partial result, it was found that the recent General Law on Personal Data Protection is intended to provide greater transparency and more strongly protect the right to privacy of users of the information society, in addition, it was understood that, despite the fact that encryption assists in data protection, the absence of legislation to protect the way in which encryption is used is still evident. The area of concentration is Citizenship, Public Policy and Dialogue between Legal Cultures, the research line, Private Law and Repersonalization of Civil Law and the work fits in the New Rights GT.
Key-words: Encryption. General Law on Personal Data Protection. Informational Society. Right to Privacy and Intimacy.

Introdução

O Estado possui a função de regulamentar a vida em sociedade criando deveres e obrigações a todos que dela participa. Com a evolução da sociedade presencial para uma sociedade informacional, muitos comportamentos foram alterados e em razão deste processo, conflitos de interesses distintos daqueles já existentes surgiram. Assim, o Estado tem que buscar criar mecanismos para tutelar os novos conflitos e assim o fez com a criação da Lei Geral de Proteção de Dados Pessoais que será abordada logo mais.

O presente artigo tem como objetivo apresentar um dos problemas que a sociedade informacional está enfrentando que é a exposição de dados pessoais oriundas das relações empresariais digitais, assim como a emergente a necessidade do enfrentamento da tecnologia da criptografia, como meio apto a proteger o consumidor na era digital.

ISSN: 2446-726X Edição: 16ª Ano 2019

Para alcançar o objetivo geral, a pesquisa irá discutir através do método de procedimento estruturalista sobre a proteção de dados pessoais e o uso da criptografia para proteger o direito de privacidade desses dados. Para o desenvolvimento da pesquisa adotou-se o método de abordagem dedutivo, levando em consideração que a partir de uma ideia central irá transpor premissas pertinentes ao tema e, a partir dela será feita a conclusão.

A justificativa do trabalho se dá pela necessidade de mostrar a importância da proteção aos dados pessoais que a maioria das pessoas não dá ao não se importar com o que é feito com os dados produzidos por eles próprios e ter a falsa percepção que as empresas não monitoram as suas atividades dia após dia.

1 A sociedade informacional e o direito à privacidade e a intimidade

A tutela constitucional consagrada no inciso X[3] do artigo 5º da Carta Magna, refere-se a inviolabilidade à intimidade, a vida privada, a honra e a imagem (BRASIL, 1988). As referidas previsões legais abrangem o direito da personalidade das pessoas físicas e das pessoas jurídicas. Assim sendo, tanto a intimidade quanto privacidade protegem a liberdade da vida privada e cuidam da esfera secreta do indivíduo, tutelando a vida privada no que se refere, dentre outros, o modo de viver, as relações afetivas, os hábitos, a imagem, os *hobbies*, etc. (BAHIA; DOURADO, 2017, p. 128).

Os conceitos constitucionais de intimidade e vida privada apresentam grande interligação (MORAES, 2018). Embora a jurisprudência e uma parte considerável da doutrina não as distingam, há os que o façam, estando o direito à intimidade como parte do direito à privacidade, que seria mais amplo (MENDES; BRANCO, 2018). Mais claramente, uma parte da vida humana, chamada de vida privada, se passa no âmbito familiar, dos amigos, ou seja, em face de um grupo determinado e escolhido. Uma outra, desenvolve-se diante dos olhos de todos: é a vida "pública" *lato sensu*, em face a um público indeterminado. Essa parte compreende as

[3] Art. 5º, X, CF/88: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

ISSN: 2446-726X Edição: 16ª Ano 2019

relações com os outros seres humanos em geral: relações de comportamento no trabalho e no lazer onde as informações são compartilhadas. (FERREIRA FILHO, 2011, p. 350).

Hodiernamente, o grande gargalo que permanece é saber diferenciar quais informações são públicas e quais informações são privadas, visto que grande parte delas são digitais[4] e estão acessíveis com apenas um clique.

Pela primeira vez na história, as mudanças que estão ocorrendo na sociedade estão se dando pelas mãos da tecnologia da informação. O modo como os seres humanos interagem, relacionam-se e trocam informações, está em constante processo de transformação, numa transição de modelos. Segundo Castells, essa transição vem ocorrendo com a sociedade desde o início do final do século XX, quando três processos distintos se uniram, que foram: a necessidade da economia por novos mercados de capital, produção e comércio e flexibilidade administrativa; as demandas da sociedade que estavam em uma grande busca por liberdade individual e uma comunicação franca; e os avanços sem precedentes da informática e da telecomunicação. Assim, surge uma nova estrutura social que ele denomina de sociedade em rede (CASTELLS, 2003, p. 8).

Esta sociedade em rede foi crescendo e ganhando corpo conforme a *internet* foi se expandindo. Se no princípio a *internet* era usada restritamente no ambiente militar, acadêmico e de pesquisa, conforme foi saindo destes ambientes restritos, uma quantidade muito grande pessoas tiveram acesso a ela e as informações nela contida.

Para muitos, a *internet* é um dos principais avanços tecnológicos da humanidade (LEONARDI, 2012, p. 28). A descentralização e a velocidade que o conhecimento é transmitido, assim como a acessibilidade das informações, é algo nunca antes visto na história da humanidade. O avanço tecnológico com o advento dos microcomputadores, dos *softwares* e da necessidade de aumentar a produtividade do setor econômico, fez com que o papel fosse

[4] "Os documentos digitais têm duas origens distintas: os que já nascem digitais e os que são gerados a partir da digitalização. Ambos são codificados em dígitos binários, acessíveis e interpretáveis por meio de um sistema computacional. O documento digitalizado é a representação digital de um documento produzido em outro formato e que, por meio da digitalização, foi convertido para o formato digital. [...] Todo documento digitalizado é um documento digital, mas nem todo documento digital é um documento digitalizado" (ESTADO VIRTUAL, s.d.).

ISSN: 2446-726X Edição: 16ª Ano 2019

substituído pelos *bytes*[5] e as informações fossem armazenadas na nuvem[6]. Hoje, quase tudo está na rede, a exemplo de quando se faz a carteira de identidade, quando se abre uma conta no banco, quando se compra um produto, de alguma forma as nossas informações pessoais saem daquele ambiente local e são transferidas para o ciberespaço[7] por meio de computadores ligados a *internet* transpondo fronteiras e distâncias, numa comunicação globalizada (LÉVY, 1999, p. 31-45).

O que iniciou como uma forma de melhorar os processos nas empresas e órgãos públicos, se tornou em um instrumento massivo de geração de informações. O ambiente virtual trazido pela *internet* mudou a forma como os seres humanos se inter-relacionam, fazendo do mundo virtual a extensão do seu próprio quarto, ou melhor, da sua própria identidade. O ser humano expõe os seus hábitos e as suas intimidades e de seus familiares, assim como piscam os olhos, é algo automático, espontâneo, culminando numa exposição voluntária inconsciente da vida privada.

Assim, como já referido, vive-se um período de transição. Em 1988, quando o poder constituinte legislou sobre a intimidade no inciso X do artigo 5º, o contexto da palavra era outro, tinha um viés de tutelar a vida privada e a intimidade em relação a inviolabilidade à casa, das correspondências, das comunicações telegráficas, telefônicas e de dados, como expresso nos

[5] Byte é uma unidade de informação digital equivalente a 8 bits. Cada byte representa um único caractere de texto num computador (FURUTANI, 2017).
[6] O armazenamento em nuvem é um serviço que permite armazenar dados ao transferi-los pela Internet ou por outra rede a um sistema de armazenamento externo mantido por terceiros podendo ser acessados de qualquer local e sendo independentes de aplicativos para que tenham acessibilidade de qualquer dispositivo. Há aqueles que incluem armazenamento pessoal, armazenando e/ou fazendo backup de e-mails, fotos, vídeos e outros arquivos pessoais de um indivíduo, e aqueles que permitem que as empresas usem o armazenamento em nuvem como uma solução de backup remoto com suporte comercial para o qual a empresa pode transferir e armazenar de forma segura seus arquivos de dados ou compartilhá-los entre locais (MICROSOFT, 2010).
[7] Pierre Levy define o ciberespaço como o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores. Incluídos aí o conjunto dos sistemas de comunicação eletrônicos na medida em que transmitem informações provenientes de fontes digitais ou destinadas à digitalização (LÉVY, 1999, p. 93).

ISSN: 2446-726X Edição: 16ª Ano 2019

incisos subsequentes XI[8] e XII[9], e no artigo 220[10] da referida lei, que mitiga à liberdade de comunicação social (BRASIL, 1988). Não pensava-se que um dia a sociedade iria se expor dessa maneira e que tudo estaria tão dinâmico. Desta feita, como resguardar que um arquivo compartilhado entre dois indivíduos não chegue às mãos de terceiros?

Diante da acelerada disseminação de informações da sociedade informatizada e por ser um campo novo, é inevitável que surjam conflitos de interesses distintos daqueles já existentes. Devido à dinâmica da sociedade e o seu próprio comportamento, nem sempre se tem uma lei que tutele aquela situação, nestes casos, os operadores do direito se encontram diante da chamada lacuna da lei.

Assim, em situações em que haja uma lacuna legislativa, a comunidade jurídica necessita adaptar a legislação existente que se adequa melhor ao fato por meio da analogia, dos costumes e dos princípios gerais do direito, como preceitua a Lei de Introdução ao Código Civil no seu artigo 4º[11] e o Código de Processo Civil no seu artigo 140[12] (SOUZA FILHO, 1997, p. 5-6).

2 O uso da criptografia como proteção de dados informacional: desafios e possibilidades

A proteção da intimidade e da privacidade já são pauta de longínquas batalhas. Isso porque, ao longo da história sempre se buscou uma forma de comunicação segura, para que não

[8] Art. 5º, XI, CF/88: "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial" (BRASIL, 1988).
[9] Art. 5º, XII, CF/88: "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal" (BRASIL, 1988).
[10] Art. 220, CF/88: "A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.
§ 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV [...]" (BRASIL, 1988).
[11] Art. 4º, LINDB: "Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito" (BRASIL, 1942).
[12] Art. 140, CPC: "Art. 140. O juiz não se exime de decidir sob a alegação de lacuna ou obscuridade do ordenamento jurídico. Parágrafo único. O juiz só decidirá por equidade nos casos previstos em lei." (BRASIL, 2015).

ISSN: 2446-726X Edição: 16ª Ano 2019

revelasse segredos e estratégias dos antigos reinos e povoados aos povos inimigos. Assim, a busca por uma forma de mascarar uma mensagem para que somente o destinatário conseguisse ler, sempre foi algo perseguido e a sua busca cada vez mais importante conforme as informações foram tornando-se mais valiosas (SILVA, F., 2008).

A criptografia e a esteganografia caminharam juntas na história e foram utilizadas para garantir a comunicação entre indivíduos de forma segura. A diferença entre elas é que enquanto na primeira se busca ocultar o significado da mensagem, embaralhando as informações, na segunda, se busca ocultar a mensagem em si, tentando mascarar a sua presença. Porém, a esteganografia tem uma fraqueza: se o inimigo conseguir interceptar a mensagem, o seu conteúdo é descoberto. Diante disso, a criptografia foi sendo aperfeiçoada ao longo dos anos, pois é mais segura que a esteganografia (SILVA, F., 2008).

Criptografar um dado no mundo da informática significa tornar aquela informação privativa entre o remetente e o destinatário, sendo inteligível para terceiros não envolvidos (ZÚQUETE, 2008, p. 25). A criptografia se dá por meio de um conjunto de técnicas e algoritmos matemáticos que “converte dados legíveis em algo sem sentido, com a capacidade de recuperar os dados originais a partir desses dados sem sentido” (BURNETT; PAINE, 2002, p. 11).

Há dois tipos de criptografia: a criptografia simétrica e a criptografia assimétrica, também conhecidas por chave privada e chave pública (MARCACINI, 2002, p. 18/24).

Na criptografia simétrica, uma mesma chave ou senha é utilizada para cifrar e decifrar a mensagem, Então, a chave que cifra deve ser fornecida ao destinatário para que ele possa descodificar, e aí tem dois problemas: primeiro que essa chave tem que ser mantida em total sigilo para que a segurança da informação seja preservada (MARCACINI, 2002, p. 18-19), e em segundo, que se o destinatário quiser alterar a mensagem que lhe foi enviada, ele pode, pois o destinatário possui a chave que o remetente usou para cifrá-la. Logo, essa informação pode sofrer alterações que não são de conhecimento do remetente (ARAUJO, 2016).

Já na criptografia assimétrica, que é a utilizada no *WhatsApp* entre outros aplicativos, utiliza-se um par de chaves diferentes entre si: uma chamada de chave pública e outra chamada de chave privada. Essas duas chaves funcionam como complemento uma da outra, elas se

ISSN: 2446-726X Edição: 16ª Ano 2019

"relacionam matematicamente por meio de um algoritmo, de forma que o texto cifrado por uma chave apenas seja decifrado pela outra do mesmo par" (ARAUJO, 2016).

Melhor explicando, cada usuário possui duas chaves, uma pública e outra privada. Quando se quer mandar uma mensagem criptografada para alguém, usa-se a chave pública para cifrar o texto, e somente a chave privada é capaz de decifrá-la, nem mesmo a chave pública que a gerou consegue decifrá-la. A chave pública pode ser distribuída a todos para que as pessoas possam utilizá-la no programa que faz a criptografia e gere uma mensagem que só será possível decifrá-la com a chave privada do usuário que proprietário daquela chave pública. Logo, diferentemente da criptografia simétrica que usava a mesma chave para cifrar e decifrar, aqui a chave capaz de decifrar, fica em poder do proprietário, não há exposição dessa chave.

Um exemplo prático dessa criptografia é: se "B" deseja enviar uma mensagem criptografada a "A", este deve ter acesso chave pública de "A", que a usará para cifrar a mensagem. Uma vez a mensagem cifrada, "B" a envia a "A" que através da sua chave privada irá usá-la para decifrá-la. Se "A" quiser mandar uma mensagem cifrada a "B", "A" deve conhecer a chave pública de "B". Caso "C", intercepte a mensagem entre "A" e "B" e tente decifrá-la com qualquer uma das chaves públicas de "A" ou de "B", só irá embaralhá-la ainda mais.

Logo, com essa forma de criptografia onde as chaves pertencem ao próprio usuário do aplicativo, aliado ao fato do *WhatsApp*, como a empresa fala, não armazenar as mensagens nem as privadas dos seus usuários, o único modo de ter acesso a essas mensagens é através do aparelho celular de cada uma das pessoas envolvidas na comunicação.

Porém, para além da tecnologia que foi criada pelo homem no âmbito da sociedade informacional, é preciso buscar compreender o estado da arte da proteção dos dados pessoais no âmbito da sociedade informacional. Dessa forma, abaixo será abordada a Lei de Proteção de Dados e o Marco Civil da *Internet.*

3 O marco civil da *internet* e a lei geral de proteção de dados pessoais como facilitadores da tutela protecionista dos consumidores da era digital

ISSN: 2446-726X Edição: 16ª Ano 2019

O Marco Civil da *Internet* de 2014 veio para guiar a proteção de dados pessoas, tendo em vista que já havia uma deturpação do modo de utilização da *internet* por todos os *players* da rede mundial de computadores. Após diversos debates acalorados entre governo, provedores de acesso à *internet*, usuários e empresas provedoras de conteúdo digitais foi, finalmente, sancionada a lei que estabelece princípios, garantias, direitos e deveres para o uso da *internet* no Brasil (BRASIL, 2015, p. 1-10) que tinha como função "de servir como uma constituição da *internet* na garantia de direitos como: neutralidade da rede, liberdade de expressão e privacidade na *internet*" (SILVA, L., 2015, p. 50).

Um ponto importante da Lei 12.965/2014, conhecida como Marco Civil da *Internet*, é justamente a previsão da obrigação dos provedores de conexão guardarem os *IP's*[13] dos *sites* navegados pelos usuários, possibilitando o seu monitoramento das atividades na rede e consequentemente terminando com a privacidade dos usuários. De outro lado, em contraponto, tornou possível rastrear os *sites* visitados por aquele que esteja sob investigação de ilícitos e que tenha sido solicitado o seu histórico de navegação por meio de requisição judicial.

Oportuno destacar que uma das particularidades da sociedade em rede é a rapidez que novos conceitos, formas relacionamentos e até mesmo a evidências de novos conflitos são criados, contrastando com o pragmatismo da ciência jurídica. Logo, necessitou-se criar outras formas de regular novos dilemas da sociedade informacional, culminando na atual Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18). Antes dela, os dados pessoais eram tratados por legislações esparsas, como a Constituição Federal, o Código de Defesa do Consumidor, a Lei de Acesso à Informação, a Lei do Cadastro Positivo e o já mencionado Marco Civil da *Internet.*

A Lei 13.709/18, que entrará em vigor em agosto de 2020, foi criada para regulamentar o tratamento de dados pessoais de clientes e usuários por parte de empresas públicas e privadas que detém os dados pessoais. Inclusive, a Lei Geral de Proteção de Dados Pessoais (LGPD) traz um conceito amplo de dados pessoais, apontando que "qualquer informação relacionada a pessoa natural identificada ou identificável", como um nome, um número, *e-mail*..., mesmo que a identificação não seja de forma direta - que seja necessário ser processada em conjunto com

[13] O IP (ou Internet Protocol) é uma identificação única para cada computador conectado a uma rede (BRITO, 2013).

ISSN: 2446-726X Edição: 16ª Ano 2019

outras - essas informações são consideradas dados pessoais, e consequentemente, estarão protegidas pela LGPD (PERONGINE, 2018).

Além dos dados pessoais, a LGPD busca regulamentar diversos outros temas referente a proteção de dados, como o respeito à privacidade, à inviolabilidade da intimidade, da honra e da imagem, à autodeterminação informativa; ao desenvolvimento econômico e tecnológico e a inovação; à livre concorrência e defesa do consumidor e aos direitos humanos liberdade e dignidade das pessoas entre outros (BRASIL, 2018).

Hoje, vive-se no âmbito de economia digital, onde tudo é transformado em dinheiro e um nicho de mercado que está em alta é justamente a comercialização dos dados pessoais. Boa parte do cotidiano das pessoas gira em torno de dados. Quando se faz um pedido de uma tele-entrega, dados como nome, telefone e endereço são informados pelo contratante do serviço. Da mesma forma, quando se vai ao supermercado, os dados atinentes aos documentos pessoais é perguntado e todas essas informações são armazenadas nos banco de dados dessas empresas, sem um prévio conhecimento dos clientes e o mais grave, sem saber qual o real destino desses dados.

Empresas como *Facebook* e *Google* que nos anos 2000 eram *startups*, hoje são empresas globais, justamente criando modelos de negócios baseados em coleta, tratamento e análise das informações pessoais de seus usuários (FGV DIREITO SP, 2017). Elas coletam as informações inseridas pelos seus usuários ou de acordo com os hábitos de navegação, e posteriormente são traçados perfis de usuários para oferecer anúncios digitais pagos, que geram receitas às empresas detentoras dessas informações e que não são repassadas aos verdadeiros donos das informações, ou seja, os usuários.

Quando um aplicativo como *Facebook* é baixado e utilizado pela primeira vez, é necessário aceitar os "Termos de Uso" e a "Política de Privacidade" que a empresa proprietária do aplicativo impõe aos seus usuários. Estes instrumentos jurídicos buscam regulamentar a relação entre o aplicativo e os seus usuários a fim de proteger a empresa de quaisquer violação de privacidade quanto ao uso dos dados. O conteúdo contido em cada um desses instrumentos muda conforme a empresa e o ramo do negócio, mas basicamente, o "Termo de Uso" trata do objetivo e das regras de conduta do aplicativo, e a "Política de Privacidade" versa,

ISSN: 2446-726X Edição: 16ª Ano 2019

principalmente, como as informações produzidas pelos seus usuários serão usadas pela empresa.

Nesta seara, a recente Lei Geral de Proteção de Dados Pessoais traz diversas garantias ao consumidor, como por exemplo, a obrigatoriedade por parte das empresas de informar quais dados e o qual a finalidade do seu uso, assim como a expressa autorização do usuário para que as informações prestadas sejam armazenadas (BRASIL, 2018), o que fará com que várias empresas adequem suas políticas de privacidade.

Outro ponto relevante a se discutir é a proteção dos dados quanto ao seu armazenamento e transferência dessas informações. De nada adianta a tutela em dar segurança aos usuários na coleta, tratamento e análise dos dados, se as empresas responsáveis por eles não investirem em segurança para armazená-los, nem quando estão coletando.

Essa é uma discussão que já está presente no campo jurídico brasileiro, principalmente, quando discute-se o acesso a dados do aplicativo *WhatsApp*, que – oportuno ressaltar – já foi alvo de batalhas judiciais onde por diversas oportunidades[14] a justiça brasileira ordenou acesso aos seus dados e por questão da forma como o aplicativo foi desenvolvido, não se conseguiu ter acesso às informações nele transmitidas.

O gargalo, como visto, está justamente na tecnologia empregada para a criptografia das informações que são transmitidas dentro do aplicativo, o que torna o aplicativo um ambiente bastante seguro e privado de comunicação garantindo uma certa proteção ao seu direito de privacidade e intimidade.

Conclusão

Hodiernamente, a sociedade informacional é responsável por produzir uma quantidade enorme de informações pessoais que acabam por ser coletados e comercializados sem o devido respeito ao direito à privacidade das informações.

[14] A título de exemplo, o processo nº 5003809-05.2017.4.04.7004 do TRF 4ª região, que multou o *Facebook* (empresa proprietária do *WhatsApp*) em R$ 23.221.305,00 por descumprimento de decisões judiciais.

ISSN: 2446-726X Edição: 16ª Ano 2019

Neste sentido, indubitavelmente o avanço da tecnologia propiciou o aperfeiçoamento da tecnologia da criptografia, o que tornou paulatinamente os aplicativos ambientes seguros e privados de comunicação, garantindo uma certa proteção ao seu direito de privacidade e intimidade.

Frisa-se, assim, que a Lei Geral de Proteção de Dados Pessoais foi criada com o intuito de disciplinar diversos assuntos sobre a proteção de dados pessoais e regulamentar o tratamento de dados pessoais entre usuários, empresas e governo. Tais previsões, que antes encontravam-se esparsas em diversas legislações do ordenamento jurídico brasileiro, a exemplo do Marco Civil da *Internet.*

De outro lado, não se pode ignorar que ainda é cedo para trazer digressões acerca da completa implementação por parte das empresas e dos órgãos públicos no que tange às obrigações previstas na LGPD. Assim, é necessário aguardar a prática dos conflitos de interesses que irão surgir, mas, sem dúvida, trata-se de um grande passo no que diz respeito a transparência e aos que nascem da necessária proteção dos dados pessoais nas relações entre os entes públicos, empresas e os indivíduos.

Referências

ARAUJO, Edmar. **Criptografia assimétrica:** novidade no Whatsapp é aliada de longa data do Brasil. CryptoID, 2016. Disponível em: ttps://cryptoid.com.br/banco-de-noticias/criptografia-assimetrica-novidade-no-whatsapp-e-aliada-de-longa-data-do-brasil/. Acesso em: 20 maio 2019.

BAHIA, Flávia; DOURADO, Sabrina (Coord.). **Direito Constitucional**. 3. ed. Recife: Armador, 2017.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em 18 mai. 2019.

_____. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 maio 2019.

ISSN: 2446-726X Edição: 16ª Ano 2019

_____. **Decreto-Lei nº 4.657, de 4 de setembro de 1942**. Lei de Introdução às normas do Direito Brasileiro. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm>. Acesso em 18 mai. 2019.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 08 set. 2019.

_____. **Lei n. 12.965, de 23 de abril de 2014.** Marco civil da internet: Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2015. (Série legislação, n. 164). (Livro eletrônico).

BRITO, Edivaldo. **O que é o IP? Descubra para que serve e qual é seu número**. Techtudo, 2013. Disponível em: https://www.techtudo.com.br/artigos/noticia /2013/05/o-que-e-o-ip-descubra-para-o-que-serve-e-qual-e-seu-numero.html. Acesso em: 10 set. 2019.

BURNETT, Steve; PAINE, Stephen. **Criptografia e Segurança:** o guia oficial. Rio de Janeiro: Elsevier, 2002.

CASTELLS, Manuel. **A galáxia da Internet.** Rio de Janeiro: Jorge Zahar, 2003.

ESTADO VIRTUAL. **O Documento Digital e o Documento Digitalizado são a Mesma Coisa?**. Disponível em: https://www.estadovirtual.com.br/o-documento-digital-e-o-documento-digitalizado-sao-a-mesma-coisa. Acesso em: 18 maio 2019.

FERREIRA FILHO, Manuel Gonçalves. **Aspectos do Direito Constitucional Contemporâneo**. 3. ed. São Paulo: Saraiva, 2011. (Livro eletrônico).

FGV DIREITO SP. **Um Novo Mundo de Dados**: relatório final. Grupo de Ensino e Pesquisa em Inovação. São Paulo: FGV, 2017. (Livro eletrônico).

FURUTANI, Karola. **Entenda a diferença entre bits e bytes e como isso interfere na transmissão de dados dos seus dispositivos**. Positivo, 2017. Disponível em: https://web.stanford.edu/class/cs101/bits-bytes.html. Acesso em: 17 maio 2019.

LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012.

LÉVY, Pierre. **Cibercultura**. 34. ed. São Paulo: Editora 34, 1999.

MARCACINI, Augusto Tavares Rosa. **Direito e Informática:** uma abordagem jurídica sobre criptografia. Rio de Janeiro: Forense, 2002.

ISSN: 2446-726X Edição: 16ª Ano 2019

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 13. ed. rev. atual. São Paulo: Saraiva Educação, 2018. (Livro eletrônico)

MICROSOFT. **O Que é Armazenamento em Nuvem?** Microsoft Azure, 2010. Disponível em: https://azure.microsoft.com/pt-br/overview/what-is-cloud-storage/. Acesso em: 18 maio 2019.

MORAES, Alexandre de. **Direito Constitucional**. 34. ed. São Paulo: Atlas, 2018. (Livro eletrônico).

PERONGINI, Maria Fernanda Hosken. **Lei Geral de Proteção de Dados**: um resumo da LGPD. Legalcloud, 2018. Disponível em: https://legalcloud.com. br/lei-geral-de-protecao-de-dados-resumo-lgpd/. Acesso em: 10 set. 2019.

SILVA, Fernanda Taline da. **Um pouco da história da criptografia**. *In:* SEMANA ACADÊMICA DA MATEMÁTICA, XXII, Cascavel: Unioeste, 2008. Disponível em: http://projetos.unioeste.br/cursos/cascavel/matematica/xxiisam/artigos/16. Acesso em: 19 maio 2019.

SILVA, Luciana Vasco da. Direito de Privacidade no Direito Brasileiro e Norte Americano. **Revista Eletrônica do Curso de Direito - PUC Minas Serro**, Serro - MG, n. 11. jan./ago. 2015. Disponível em: http://periodicos.pucminas.br/index.php/DireitoSerro/article/viewFile/8968/8603. Acesso em: 18 maio 2019.

SOUZA FILHO, Carlos Frederico Marés de. O Direito Constitucional e as lacunas da lei. **Revista de Informação Legislativa**, Brasília, v. 34, n. 133, p. 5-16, jan./mar. 1997. Disponível em: http://www2.senado.leg.br/bdsf/bitstream/handle/id/188/r133-01.PDF. Acesso em: 18 maio 2019.

ZÚQUETE, André. **Segurança em Redes Informáticas**. 2. ed. Lisboa: FCA, 2008.