XXV CONGRESSO DO CONPEDI - CURITIBA

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

IRINEU FRANCISCO BARRETO JUNIOR

SALETE ORO BOFF

CINTHIA O. A. FREITAS

D598
Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI/UNICURITIBA;

Coordenadores: Cinthia O. A. Freitas, Irineu Francisco Barreto Junior, Salete Oro Boff – Florianópolis: CONPEDI, 2016.
Inclui bibliografia
ISBN: 978-85-5505-338-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: CIDADANIA E DESENVOLVIMENTO SUSTENTÁVEL: o papel dos atores sociais no Estado Democrático de Direito.
1. Direito – Estudo e ensino (Pós-graduação) – Brasil – Congressos. 2. Governança. 3. Novas Tecnologias. I. Congresso Nacional do CONPEDI (25. : 2016 : Curitiba, PR).

CDU: 34

CONPEDI
Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Florianópolis – Santa Catarina – SC
www.conpedi.org.br

XXV CONGRESSO DO CONPEDI - CURITIBA

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

O grupo de trabalho Direito, Governança e Novas Tecnologias II, do XXV Congresso Nacional do Conselho Nacional de Pesquisa e Pós-Graduação em Direito (Conpedi), foi realizado na cidade de Curitiba, no dia 09 de dezembro de 2016. Os artigos apresentados no GT reafirmam a relevância do Conpedi enquanto espaço de divulgação e debates sobre temas jurídicos que apresentam interface com as inovações tecnológicas, avanços nos meios de comunicação digitais e o crescimento da capacidade de processamento e análise de massas de dados, assim como os respectivos reflexos desses fenômenos no Direito.

Foi o que se viu nesse GT. A originalidade dos trabalhos foi observada pela atualidade dos temas elencados nos artigos. A sessão foi inaugurada com pesquisa sobre a governança global e seus reflexos na justiça ambiental, pesquisa teórica que perpassa os papeis da governança civil, empresarial e pública como indutores da governabilidade e da boa gestão governamental. Os princípios e garantias preconizados no Marco Civil da Internet foram objeto de significativo número de estudos, coligidos no GT, o que denota a importância dessa legislação para a comunidade científico-jurídica. Essas abordagens miraram a Neutralidade da Rede, garantias de privacidade e intimidade, proteção de dados pessoais e decisões judiciais que suspenderam aplicações, com seus reflexos nos usuários. Abordagens inovadoras permearam a reflexão de pesquisadores que escreveram sobre a teoria do Estado na era informacional, direito ao esquecimento e a possibilidade de responsabilização penal de provedores de internet. Também merece destaque artigo que tratou a rede mundial de computadores na perspectiva empresarial, ao tratar de ambientes de coworking, makerspace e hackerspace. A sessão foi encerrada com pesquisa sobre as tecnologias de Big Data e mineração de dados, sob a ótica do direito constitucional, abordagem inédita que trata do exponencial avanço na produção e capacidade de processamento de dados e seus reflexos na dignidade da pessoa humana.

O corolário de temas abordados reitera a relevância e a atualidade dos estudos jurídicos sobre os efeitos da Sociedade da Informação, conceito formulado por Manuel Castells, sobre o direito e a sociedade global, nas suas mais diversas nuances. A aceleração do ritmo e ampliação do alcance dessas transformações são inexoráveis, o que certamente permitirá uma duradoura agenda de discussão nos eventos vindouros do Conpedi.

As temáticas discutidas foram aprofundadas em ricos debates no transcorrer e ao término do GT, nos quais os pesquisadores puderam interagir mutuamente, aprofundar sua compreensão sobre os artigos apresentados e apontar inúmeras possibilidades de novas interações e pesquisas conjuntas, uma vez que houve perceptível convergência entre os temas abordados e as linhas de pesquisa dos membros do grupo de trabalho.

Os coordenadores do GT convidam os leitores para desfrutarem do teor integral dos artigos, com a certeza de profícua leitura, e encerram agradecendo pela honraria de dirigir os debates com a participação de pesquisadores altamente qualificados.

Profa. Dra. Cinthia O. A. Freitas - PUC-PR

Prof. Dr. Irineu Francisco Barreto Junior - FMU-SP

Profa. Dra. Salete Oro Boff - Imed, IESA, UFFS

O DIREITO À PRIVACIDADE E OS LIMITES À FUNÇÃO FISCALIZADORA DO ESTADO EM FACE DA PROTEÇÃO DE DADOS CRIPTOGRAFADOS

THE RIGHT TO PRIVACY AND THE LIMITS OF THE STATE TO THE SUPERVISORY FUNCTION IN FACE OF PROTECTED ENCRYPTED DATA

Andy Portella Battezini [1]
Vinícius Borges Fortes [2]

Resumo

A pesquisa tem como propósito avaliar o direito à privacidade e sua importância no contexto das restrições impostas pelo Estado no uso da criptografia para a proteção de dados pessoais. O estudo analisa as múltiplas dimensões do direito à privacidade; evidencia o potencial técnico da criptografia como mecanismo de proteção e sigilo das informações; e contrasta os riscos aos quais a privacidade vem sendo exposta no âmbito Estatal. A pesquisa é realizada com o método hipotético-dedutivo, e a técnica de pesquisa é a investigação bibliográfica.

Palavras-chave: Direito à privacidade, Proteção de dados pessoais, Tecnologia da informação, Criptografia

Abstract/Resumen/Résumé

This research intended to evaluate the right to privacy and its importance face to the restrictions imposed by State at the encrypted communications for personal data protection. It aims to analyze how multiple dimensions of the right to privacy; to evidence the technical potential of encryption as protection mechanism and confidentiality of information; and contrast the scratchs to which the privacy being exposed in the state scope. For conducting this paper, it will be appreciated with the hypothetical-deductive method, and the search technique concentrated if the bibliographical research.

Keywords/Palabras-claves/Mots-clés: Right to privacy, Personal data protection, Information technology, Cryptography

[1] Advogada, especialista em Direito Tributário e Gestão de Pessoas pela Universidade Anhanguera – Uniderp. Mestranda em Direito Democracia e Sustentabilidade pela Faculdade Meridional. E-mail: andy_battezini@hotmail.com

[2] Pós-Doutor pela VUB, Bélgica. Doutor em Direito pela UNESA, RJ. Professor Permanente do Mestrado em Direito da IMED. Visiting Scholar no LSTS/VUB, Bélgica. E-mail: viniciusfortes@imed.edu.br

INTRODUÇÃO

À medida que as novas tecnologias de informação e comunicação (TIC'S) estão avançando, aumenta a probabilidade de os indivíduos estarem sendo vigiados e verem suas liberdades ameaçadas. A criptografia, como mecanismo hábil a proteger o sigilo das informações pessoais e da própria liberdade civil, começa a ser rediscutida pelo direito, e a perder sua força no panorama atual, considerando que as próprias autoridades estão a optar por caminhos que venham a restringir a utilização deste mecanismo, sob o pretexto da segurança nacional.

Recentemente, no ano de 2015 e 2016, quatro decisões de tribunais inferiores (TJ/SE, TJ/SP e TJ/RJ) determinaram o bloqueio temporário do aplicativo *WhatsApp*. O fundamento da decisão jurídica foi motivado pelo descumprimento, por parte do aplicativo, em face de uma ordem judicial que determinou a disponibilização do conteúdo das conversas entre usuários suspeitos de utilizarem de suas ferramentas de mensagens instantâneas e chamadas de voz para combinar e cometer crimes. A recusa em descumprir a decisão fundou-se na impossibilidade da guarda de informações, cujo acesso é indisponível, considerando a inviabilidade de compreensão do conteúdo cifrado pelo provedor do serviço.

Todavia, há de se considerar que a legislação pátria ainda é omissa, pois tanto o Marco Civil da Internet, em vigor desde 2015, quanto o Anteprojeto da Lei de Dados Pessoais, ainda em tramitação no Congresso Nacional, em nada dispõe sobre o funcionamento ou a violação da rede de encriptação, o que vem a gerar um ambiente jurídico-digital conturbado.

A Diretriz Europeia 95/46/CE, revogada em maio deste ano, é determinante referência na proteção de dados, pois confere ampla proteção ao seu titular, inclusive no tocante ao consentimento da coleta e do tratamento de tais dados, e ainda, ao incorporar o direito de ser esquecido, quando este entender não ser mais necessário a guarda e disponibilidade de suas informações.

Nesse viés, o objetivo geral é avaliar a admissibilidade e adequação das decisões judiciais que determinaram o bloqueio de serviços e aplicações de internet que utilizam a criptografia como recurso de proteção de dados pessoais de seus usuários. Enquanto os objetivos específicos são: analisar as múltiplas dimensões do direito à privacidade; evidenciar o potencial técnico da criptografia como mecanismo de proteção e sigilo das informações; e contrastar quais riscos pode afetar o direito à privacidade.

Já o problema de pesquisa reside diante da relevância jurídico-social do direito à privacidade para o exercício da democracia na internet, pode-se dizer que são juridicamente

admissíveis e adequadas as decisões judiciais de bloqueio de acesso a serviços e aplicações de internet que utilizam a criptografia como recurso de proteção de dados pessoais, enquanto atos restritivos de direitos civis impostos pelo Estado?

Em conseguinte, a justificativa de pesquisa sustenta-se nas transformações de cunho social e tecnológico que visam revisar as lacunas jurídicas que dão margem para eventuais intervenções por parte do Estado e de terceiros, no intuito de se apoderar de informações sigilosas que versem sobre a esfera privada do indivíduo.

Para a construção da presente pesquisa utilizar-se-á o método hipotético-dedutivo, com a finalidade de apresentar os aspectos teóricos mais específicos, para assim confirmar ou refutar as hipóteses preliminarmente formuladas e apresentadas, enquanto solução do problema. O método de procedimento será tipológico, pois pretende-se alcançar um modelo jurídico adequado a proteção da intimidade e da vida privada perante as inovações tecnológicas. A técnica de pesquisa concentra-se na investigação bibliográfica de textos doutrinários, meios eletrônicos e coleções particulares.

1 A DIMENSÃO DO DIREITO À PRIVACIDADE FRENTE ÀS NOVAS TECNOLOGIAS DE COMUNICAÇÃO E INFORMAÇÃO

A preocupação com a privacidade nos dias atuais demanda uma nova ordem. O que no passado estava direcionado ao "direito de estar só", ou de se isolar (WESTIN, 1967), hodiernamente compreende algo muito mais profundo, pois a privacidade está condicionada não apenas ao direito de personalidade no âmbito da honra e da intimidade, mas, sim, como um direito humano fundamental, consagrado na liberdade de escolha e na autonomia do ser.

O marco inicial do debate acerca da privacidade decorreu de um artigo de Samuel Warnes e Louis Brandeis intitulado *The Right to Privacy* (WARNER; BRANDEIS, 1980), o qual discorria a invasão dos espaços da vida privada e doméstica através dos mecanismos tecnológicos, tendo como exemplo as fotografias e jornais. Esse debate, que teve origem no século IX, rompeu com a tradição que relacionava a privacidade apenas a aspectos de cunho patrimonialista (DONEDA, 2006), trazendo um novo panorama da privacidade, aludida ao direito de proteção da personalidade, tendo em vista a dimensão e o alcance proporcionado pelo desenvolvimento tecnológico (DONEDA, 2006).

Para Danilo Doneda (2006), a inserção da privacidade na vida moderna hoje demanda algo muito mais complexo do que o simples direito de estar sozinho. Há uma

tendência em adaptar o Direito com as transformações sociais, e isso foi determinante para ensejar o nascimento da privacidade como dispositivo dotado de Direito, e que em consonância com a proteção de dados pessoais, instituem uma projeção da personalidade do indivíduo, fazendo, portanto, jus à proteção constitucional.

A Constituição Federal Brasileira é cristalina ao reconhecer, nos termos do artigo 5º, inciso X, a proteção da vida privada, da honra e da imagem como direito fundamental. Contudo, existem outras normas que asseguram o direito à privacidade com mais rigidez, como é o caso da inviolabilidade do domicilio e da correspondência, previsto nos incisos XI e XII do Texto Legal, além de outros documentos de abrangência internacional a exemplo da Declaração Universal dos Direito do Homem (1948); a Convenção Europeia para Salvaguarda dos Direitos e Liberdades Fundamentais (1950); a Convenção Americana dos Direitos do Homem (1969) (WEINGARTNER NETO, 2002).

A despeito de sua essencialidade, insta destacar que a privacidade insere-se nos chamados direito de personalidade, isso significa dizer que ela está tutelada pelo princípio da dignidade da pessoa humana, o que vem a assegurar maior proteção e garantia para o desenvolvimento do cidadão (LIMBERGER, 2007). Nesse sentido, cabe ao próprio modelo Democrático de Direito assegurar a efetividade material, principalmente no tocante à dignidade da pessoa humana, considerando ser o seu mais alto grau de especificidade em relação aos demais direitos, como bem destaca Dias e Boff (2012).

Quanto à delimitação do conceito de privacidade há de se considerar a pluralidade de definições trazidas pela doutrina, principalmente no tocante a diferenciação entre o termo privacidade e intimidade e vida privada. Embora todas elas possuam um conteúdo bem próximo, a intimidade apresenta-se vinculada a dignidade da pessoa humana (LIMBERGER, 2007), e ainda, mais especificamente "à proteção de uma vida confortável, a resguardo de intromissões de estranhos. Por isso, pode se considerar a intimidade como aquela que parte de sua existência não comunicável, ou de reserva" (LORENZETTI, 1998, p.492).

Enquanto a privacidade, que de acordo com Rodotá pode ser definida como "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada" (RODOTÁ, 2008, p.122). Ou ainda, conforme Alan Westin: "privacidade é a reinvindicação de indivíduos, grupos, instituições para determinar, quando, como e em que extensão, informações sobre si próprios devem ser comunicadas a outros" (WESTIN, 1967, p.7). Em sentido mais amplo, José Afonso da Silva a define como:

> [...] um conjunto de informações acerca do indivíduo que pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde, e em que condições, sem isso pode ser legalmente sujeito. A esfera da inviolabilidade, assim, é ampla, abrange o modo de vida doméstico, nas relações familiares e afetivas em geral, fatos, hábitos, local, nome, imagem, pensamentos, segredos, e, bem assim, as origens e os planos futuros do indivíduo (SILVA, 2009, p. 206).

Nesse sentido, entende-se a privacidade como a faculdade de obstar a intromissão de pessoas alheias nas preferências pessoais de cada indivíduo, bem como no acesso à informação e divulgação sobre áreas de interesse e de manifestação existencial, inerentes à própria individualidade do ser. Por outro lado, a intimidade reflete uma zona mais restrita da pessoa, ou seja, "[...] aparenta referir-se a eventos mais particulares e pessoais, a uma atmosfera de confiança" (DONEDA, 2006, p.109).

Logo, a vida privada situa-se no campo externo, partindo do pressuposto de que a pessoa não queira divulgar para terceiros os atos de seu próprio conhecimento ou de um determinado círculo de pessoas (ALONSO, 2005), distinguindo do conceito de intimidade apenas atrelada ao indivíduo no seu sentido isolado, sem acesso ou participação de outras pessoas no âmbito particular.

Tais projeções terminológicas ainda demonstram-se relevantes nos dias atuais, todavia é necessário frisar que o conceito de privacidade, intimidade e vida privada são passiveis de novas interpretações conforme determinado tempo e lugar, considerando a natureza dinâmica humana. E ainda, com o advento das novas tecnologias de comunicação e informação (TCI'S), o debate à respeito da privacidade ganhou uma nova dimensão, e consequentemente um novo desafio tanto para a esfera pública quanto para a privada.

Nesse viés, cumpre aqui destacar que a privacidade, fruto de uma noção pré-informática, com a presença dos meios tecnológicos veio para remodelar o panorama da segurança jurídica e da proteção de dados pessoais. Isso significa dizer que quanto maior for o avanço das novas tecnologias, maior é a chance dos dados pessoais e da vida privada serem violados. Em que pese no centro de uma sociedade democrática de Direito, em que a condição da privacidade figura-se no bojo da dignidade da pessoa humana, o Estado não pode se desincumbir de demonstrar como e quanto a democracia está (e pode ser) aliada ao desenvolvimento tecnológico, por isso a necessidade em incorporar legislações especificas integrando o direito à privacidade e à proteção de dados pessoais.

2 O ÂMBITO NORMATIVO DA PROTEÇÃO E SEGURANÇA DAS INFORMAÇÕES - UM ESTUDO COMPARADO ENTRE A LEGISLAÇÃO BRASILEIRA E DA UNIÃO EUROPEIA

Uma das mais importantes inovações no que diz respeito à Internet, trazida recentemente pelo ordenamento jurídico brasileiro, é conhecida popularmente como Marco Civil da Internet. A Lei n.12.965/2014 possui vinte e cinco artigos, dividida em cinco capítulos, e abrange questões como a proteção à privacidade de dados; o respeito à liberdade de expressão; o reconhecimento da escala mundial da rede; os direitos humanos; o desenvolvimento da personalidade; o exercício da cidadania em meios digitais; a pluralidade e a diversidade; a abertura e colaboração; a livre iniciativa, a livre concorrência e a defesa do consumidor; e a finalidade social da rede (BRASIL, 2014).

A efetivação do Marco Civil garantiu maior proteção no âmbito do direito fundamental à privacidade, pois tanto a guarda como a disponibilização dos registros de conexão e de acesso e aplicações de Internet passaram a ser amparadas no contexto da preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (BRASIL, 2014).

Além do mais, a Carta da Internet trouxe inovações no tocante a proteção de dados pessoais, assegurando o tratamento dos dados envolvendo a coleta, o uso e o armazenamento de modo claro, completo, para a finalidade almejada (BRASIL, 2014).

Assim como o tratamento, o consentimento do titular quanto à utilização de tais dados também deve ser destacado das demais cláusulas contratuais. Isso implica também na possibilidade de exclusão definitiva dos dados pessoais que tiverem sido fornecidos para determinada aplicação de internet, a requerimento do interessado, ao término da relação entre as partes (BRASIL, 2014).

Outro ponto que merece ênfase e representa uma evolução da eficácia da legislação em território brasileiro é o que diz respeito à operação de coleta, armazenamento, guarda e tratamento de registros e de dados pessoais ou de comunicações que ocorram no espaço nacional. A legislação brasileira prevê seu respeito obrigatório, incidindo no direito à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, desde que pelo menos um dos terminais esteja localizado no Brasil, mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior (BRASIL, 2014).

Apesar da garantia estabelecida pela Lei 12.965/2014, não há no Brasil uma lei específica sobre o uso e a privacidade dos dados pessoais. Todavia, existe uma proposta em andamento no Congresso Nacional, o Anteprojeto de Lei de Proteção de Dados Pessoais (PL 5.870), com a finalidade de dispor sobre o tratamento de dados pessoais para garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural (BRASIL, 2015).

Assim como o Marco Civil, o anteprojeto brasileiro estabelece dezoito definições técnicas a serem consideradas na esfera da aplicação normativa, além de recepcionar o consentimento como um dos elementos essenciais da tutela dos dados pessoais. Para fornecer o consentimento, a proposta prevê que o titular deve ser informado de forma ostensiva sobre a finalidade e período de uso, como ele se dará e o âmbito de sua difusão. O titular poderá ainda revogar seu consentimento a qualquer tempo e sem qualquer cobrança (BRASIL, 2015).

Observa-se que a pretensa lei é fruto de um trabalho com Ministério da Justiça em parceria com o Observatório Brasileiro de Políticas Digitais do Comitê Gestor da Internet no Brasil e que teve por base a Diretiva Europeia de Proteção de Dados Pessoais (EC 95/46) e a lei de proteção de dados canadense (ALMEIDA; CRESPO. 2016). Para o presente estudo, cumpre analisar a Diretriz Europeia como modelo de regulamentação e inovação no ambiente da proteção a e inviolabilidade dos dados pessoais.

A Diretriz Europeia 95/46/CE aprovada em 24 de outubro de 1995, representa um avanço na esfera jurídica, principalmente no âmbito da proteção, segurança e tratamento de dados pessoais e do fluxo de informações no mercado interno. Essa Diretriz é resultado de um documento baseado na Lei Francesa de 1978, e da Recomendação da Organização para Cooperação e Desenvolvimento Econômico (OCDE) de 1980, denominada “Convenção de Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal” (GARCIA, 2003, p. 151-154), e que posteriormente veio a se aprimorar para Diretiva de 95/46, considerando que o regulamento anterior não contemplava questões envolvendo a atualização tecnológica e a proliferação de dados online (CONVENÇÃO DO PARLAMENTO EUROPEU, 1981).

A questão de dados pessoais na União Europeia encontra-se em fase tão avançada que além de todos os países disporem de uma agência, comissão ou departamento responsável pela proteção de dados pessoais e pela fiscalização da aplicabilidade do Regulamento Europeu, recentemente, em maio de 2016, essa Diretriz veio a ser revogada para o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.

Destacam-se as principais atribuições da Diretiva 2016/679: a) estabelecer as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados

pessoais e à livre circulação desses dados; b) defender os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais; c) a livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais (PARLAMENTO EUROPEU E CONSELHO, 2016).

A atual Diretiva conta com noventa e nove artigos, e visa a uniformização do tema entre os países-membros da União Europeia, além de trazer mais segurança jurídica aos usuários e empresas que atuam no ramo.

Ademais, entre as novas atribuições está a ampliação da definição de dados pessoais, que possibilitou uma maior transparência no tratamento de dados de usuários por parte das empresas, além de ter reforçado a necessidade de consentimento para a coleta e tratamento desses dados. Um dos principais destaques introduzidos pela lei é o "direito de ser esquecido" relativo à possibilidade de o usuário solicitar a exclusão de dados pessoais não essenciais de bases de dados (PARLAMENTO EUROPEU E CONSELHO, 2016).

Não obstante, verifica-se que a tutela do direito ao esquecimento, atribuída pelo ordenamento europeu, tem íntima relação com o direito à privacidade e a própria dignidade humana, pois assim como privacidade, trata-se de um direito subjetivo em que o cidadão resguarda o direito ou não de ter sua vida exposta. O direito ao esquecimento faculta ao usuário o tempo de permanência que seus dados devam ficar salvos perante terceiros.

Há de se ressalvar também o artigo 23º, o qual prevê o Direito da União e dos Estados Membros e a quem estejam responsáveis o seu tratamento ao contratante ou subcontratante, de limitar por meio de medida legislativa as obrigações e os direitos que compreendem o respeito a transparência das informações e comunicações, as decisões individuais, a comunicação de uma violação de dados pessoais ao titular de dados, e os princípios relativos a proteção de dados.

A finalidade deste dispositivo permeia-se na essência dos direitos e liberdades fundamentais que constituem uma sociedade democrática, visando assim, assegurar especialmente as situações que envolvam a segurança do Estado, a defesa, e a segurança pública (PARLAMENTO EUROPEU E CONSELHO, 2016).

Nesse sentido, verifica-se que tais direitos podem ser relativizados quando o processamento de dados pessoais for necessário para segurança e defesa do Estado, da população, da prevenção, da investigação e da repressão de infrações penais, inclusive aquelas que versam sobre interesse financeiro ou econômico do Estado-membro ou da União

Europeia, para possibilitar o exercício de determinadas funções públicas ou ainda para proteger direitos e liberdades alheias (PARLAMENTO EUROPEU E CONSELHO, 2016).

Não obstante, segundo o Diploma nenhuma entidade pode, portanto, iniciar alguma atividade automatizada de tratamento de dados pessoais sem antes notificar o comissário ou agente público responsável pela supervisão dessa atividade, principalmente em casos que ofereçam um elevado risco às liberdades e direitos da pessoa titular dos dados. Desse modo, proíbe-se a escuta ou a intercepção de comunicações ou a vigilância de comunicações e ainda a utilização dos dados de tráfego sem o consentimento dos titulares, garantindo-se, assim, uma maior proteção às liberdades individuais.

Outro aspecto identificado na Diretiva no artigo 32º e que vai ao encontro da proposta abordada diz respeito à segurança dos dados pessoais, em especial a segurança no tratamento, a qual prevê:

> 1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:
> a) A pseudonimização e a cifragem dos dados pessoais; [...] (PARLAMENTO EUROPEU E CONSELHO, 2016)

Com base nesse dispositivo, constata-se a facticidade em utilizar-se de tecnologias de cifragem, ou seja, de métodos de encriptação a fim de permitir maior segurança quanto ao tratamento das informações. A legislação pátria ainda é omissa quanto à necessidade ou não de utilização da criptografia no tratamento de dados pessoais, mas há de se considerar a sua efetividade como forma de garantia na confidencialidade e integridade das mensagens transmitidas, conforme será demonstrado mais especificamente no tópico seguinte.

3 A IMPORTÂNCIA DA TECNOLOGIA CRIPTOGRAFADA NAS RELAÇÕES DE SEGURANÇA E DE PRIVACIDADE

Com o exponencial aumento das TIC'S, questões como a privacidade, o anonimato e a segurança nas transmissões de dados repercutiram com mais força no cenário global, principalmente após o ataque as torres gêmeas nos Estados Unidos no ano de 2011, e com as revelações de Edward Snowden no início de 2013, reportando provas de que a NSA (National

Security Agency – NSA, na sigla em inglês), monitora milhares de dados de usuários online, telefonemas, interceptando praticamente todo e qualquer tipo de informação, não apenas em solo americano, mas também de outros países, inclusive o Brasil.

O caso de Snowden representou uma reviravolta nas questões envolvendo a violação do direito à privacidade e o sigilo dos dados pessoais, pois de acordo com as informações apresentadas pelo ex executivo do FBI, a NSA estava construindo uma superestrutura que permite a interceptação de qualquer informação, isso tudo sem qualquer controle prévio ou consentimento, o que vem a configurar um desrespeito ao direito à privacidade dos cidadãos.

Diante desse cenário, depreende-se a importância do uso da criptografia como mecanismo que visa proteger o sigilo das informações. O termo criptografia, originário do Grego, significa *kriptós* que corresponde a escondido, oculto e *grafo* de grafia (YOSHIDA, 2001). Já a sua definição, segundo ensina Yoshida: "É a arte ou ciência de escrever em cifra, de forma a permitir normalmente que apenas um destinatário a decifre e compreenda" (YOSHIDA, 2001), ou ainda, a criptografia também pode ser entendida como propósito de prevenir ou dificultar o acesso não autorizado à informações.

Em tese, a chave criptográfica dispõe de uma informação secreta que somente o titular pode ter acesso, e por meio dela permite que o destinatário final possa ter ciência do conteúdo que vier a ser disponibilizado. A sua principal finalidade é garantir a segurança de todo o ambiente computacional, em que pese nos meios de transmissão e de armazenamento que necessitem de sigilo em relação às informações.

Por mais que a criptografia esteja em voga nas últimas décadas, no Egito, desde 1900 A.C. ela já era usada para substituir alguns hieróglifos por outros considerados mais importantes e até mesmo mais bonitos. Essa substituição teve como fundamento evitar que o documento que continha a mensagem que levava o caminho para tesouro viesse a ser roubada (SOUZA, 2011) e (SIMON, 2001).

Antes de 1800 a criptografia era exclusivamente manual, utilizada apenas com técnicas de papel e lápis, e ao decorrer do tempo foi substituída por máquinas que permitiam com que "o operador desta, usando a tabela e manipulando a máquina podia enviar uma mensagem criptografada" (FRANÇA. 2005, p.5).

Com o advento da Segunda Guerra Mundial, os alemães desenvolveram uma máquina conhecida por Enigma, "que consistia em um teclado ligado a uma unidade codificadora" (FRANÇA, 2005, p.5). Este codificador possuía três rotores separados, sendo que suas posições determinavam como cada letra no teclado seria codificada, e cada rotor

podia ser posicionado em 26 modos diferentes. "Isto significava que a máquina podia ser regulada em milhões de modos diferentes" (FRANÇA. 2005, p.5).

Com o passar do tempo, os sistemas criptográficos antigos perderam a eficiência devido à facilidade com que eram decodificados. Na atualidade, a criptografia mais comum é a denominada criptografia em rede, compreendida basicamente como uma mensagem criptografada por algoritmos, gerando diversos códigos que passam a executar a encriptação. "Para se utilizar a criptografia convencional de maneira segura é necessário se ter dois requisitos: Um algoritmo de criptografia forte e manter a chave secreta de forma segura entre o receptor e o emissor" (SOUTO, 2005, p.42).

Um dos mecanismos baseados na tecnologia da criptografia e que vem sendo discutido com mais ênfase na atualidade é chamado de rede *Blockchain*. A arquitetura da *Blockchain* se baseada em chaves criptografadas, e tem como principal escopo proteger a base de dados públicos, isso tudo sem a presença de um intermediário. Através da rede *blockchain* um computador é interligado ao outro diretamente de forma descentralizada, sem a permanência de um terceiro que possa assegurar o consenso das informações que são compartilhadas e distribuídas.

A *blockchain* apresenta vários atributos essenciais, com a utilização da criptografia informações referentes à autenticidade e autoria mantém-se protegidas, impossibilitando fraudes. Logo:

> Os projetos que contribuem hoje para seu avanço têm o código aberto e se pautam em transparência e colaboração. Esses atributos, combinados aos demais, fazem com que se trate de uma tecnologia à prova de censura, permitindo então usos inovadores como votações eletrônicas e plataformas participativas para o desenvolvimento de leis ou orçamentos públicos (ALEIXO; RADU, 2015).

Desse modo, com a *blockchain*, informações que antes só poderiam ser realizadas unicamente através de fontes centralizadas perderam sua importância. O potencial da tecnologia *blockchain* deu espaço a serviços livres de censura ou discriminação, predominando a transparência, inclusive possibilitando a construção de ferramentas participativas (votações, pagamentos) para as mais diversas finalidades, e de maneira descentralizada (ALEIXO; RADU, 2015).

Hoje, empresas reconhecidas internacionalmente já aderem ao uso da criptografia, a exemplo do *Google, Yahoo, Whatssap,* com o intuito de reforçar a privacidade dos clientes, bem como garantir a segurança de suas informações em rede.

No Brasil, de acordo com o Centro de Estudos, Respostas e Tratamentos de Incidente de Segurança, a criptografia tem como principal objetivo:

> 1. Proteger os dados sigilosos armazenados no computador, como por exemplo, um arquivo de senhas;
> 2. Criar uma área (partição) específica no computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
> 3. Proteger backups contra acesso indevido, principalmente, aqueles enviados para áreas de armazenamento externo de mídias;
> 4. Proteger as comunicações realizadas pela Internet, como os e-mails enviados/recebidos e as transações bancárias e comerciais realizadas (CERT BR).

Já, em âmbito internacional, a Organização para Cooperação e Desenvolvimento econômico (OCDE) que atende ao uso seguro das tecnologias da informação para garantir a confidencialidade e integridade dos dados e especialmente a proteção da vida privada, elaborou as Linhas de Orientação para uma Política de Criptografia adaptadas pelo Conselho em 1997, que visam, entre outros:

> – Promover a utilização da criptografia de forma a aumentar a confiança nas tecnologias e assim proteger a informação, designadamente os dados pessoais e consequentemente a vida privada;
> – Tomar medidas para que a criptografia não ponha em risco a segurança pública, o cumprimento das leis e a segurança nacional;
> – Fomentar a existência de políticas e legislações compatíveis e a troca de experiências entre os diversos Estados e organizações (CERT BR).

Nessa lógica há de se considerar que a criptografia como ferramenta apta a garantir um sistema de segurança e de proteção para as liberdades civis representa a salvaguarda do direito à privacidade e da proteção de dados pessoais. Se o direito à privacidade é um direito fundamental amparado pela Constituição Federal, não cabe a ele ser violado e estar vulnerável a constantes intromissões e ameaças, sejam por terceiros ou também pelo próprio Estado. Por isso, a necessidade em ampliar o debate legislativo e reaver as lacunas que deixam os indivíduos a mercê de uma vigilância estatal.

4 OS LIMITES DA INTERVENÇÃO DO ESTADO NA TUTELA DA PRIVACIDADE E DOS DADOS PESSOAIS

Traçada a importância do direito à privacidade e da criptografia no ambiente do sigilo e da proteção da vida privada, cumpre-se analisar a questão da intromissão do Estado na

esfera privada dos indivíduos, em especial, nos assuntos que envolvam a tutela de informações criptografadas.

A presença de um Estado limitador, há muito tempo formalizou técnicas de controle e de vigilância sob a perspectiva em prol da convivência harmônica da sociedade, entretanto, com a chegada da Internet novas formas de comando se concretizaram. As ideias de "sociedade disciplinar" e "sociedade de controle" apontadas nas obras de Michel Foucault (1987) e Gilles Deuleze (1992) ainda se mantém vivas no panorama atual, contudo, não na forma de castigo e de restrição de liberdade por desobedecer ao soberano, mas sim, nas ramificações das TCI'S.

Isso se justifica, diante do aumento demasiado em monitorar e privar as liberdades civis por técnicas de controle e rastreamento que muitas das vezes estão sob o domínio das instituições estatais. Evidencia-se, nesse sentido, a importância da reflexão abordada por Cella e Rosa, em que "É preciso ter olhos ávidos para identificar os resquícios do controle ilimitado, que despercebidos chegam ao senso comum. Existe uma linha tênue entre a função do Estado protetor para o Estado limitador, a exemplo disso há a sociedade disciplinar e a sociedade de controle" (CELLA e ROSA, 2013).

Essa mudança, na forma de exercício do poder de disciplinar e controlar as pessoas por meio da tecnologia, não demanda apenas de um privilégio do poder Estatal, mas também das próprias iniciativas privadas que, muitas vezes de forma conjunta, estabelecem novos artefatos de vigilância e espionagem. Por isso a preocupação crescente com a preservação do direito à privacidade e aos dados pessoais.

Por mais que o direito à privacidade esteja consagrado como um direito humano fundamental no ordenamento jurídico pátrio, conforme já abordado no decorrer da pesquisa, verifica-se um aumento do controle por parte dos agentes estatais sobre as relações entre particulares, por isso a necessidade em avaliar se o interesse estatal em monitorar a segurança pública das informações pode se sobrepor ao direito à privacidade. Diante desta questão, cumpre analisar o posicionamento de Herminia Campuzano:

> Hasta hace pocos anos podíamos decidir cómo, a quién y en qué circuntancias queríamos que nuestros datos personales fueran objeto de difusión. Aceptábamos que en determinadas ocasiones era obligado proporcionar información personal a determinados organismos públicos, pero podíamo negarnos a facilitarlos cuando consderábamos que no existia una razón justificada para ello. La realidad actual resulta bien distinta; la excesiva, incontrolada y, en algunos casos, injustificada recolección automatizada de los datos de carácter personal, asi como el mal uso que en determinadas ocasiones los organismos públicos y privados pueden hacer de ellos, origina que el individuo pueda ver totalmente cercenado su derecho a la vida privada (CAMPUZANDO TOMÉ, 2000, p.58).

Em que pese o avanço das tecnologias terem contribuído ainda mais para vigilância dos indivíduos, ainda se faz difícil estabelecer um equilíbrio entre os meios destinados a garantir a segurança do Estado e da sociedade e em contrapartida assegurar o respeito pela privacidade e proteção de dados. Há um impasse em solo democrático, como é o caso do Brasil, que demanda não apenas as liberdades civis dos indivíduos, mas também na "constatação de que os responsáveis pela proteção de dados pessoais encontram-se politicamente posicionados sempre de forma desvantajosa em relação aos burocratas encarregados de coletar tais informações" (VIEIRA, 2007, p.210).

Não obstante, há de se considerar a insuficiência por parte do sistema político-jurídico pátrio em oferecer uma solução para o caso concreto. Tanto é que recentemente três decisões jurídicas determinando o bloqueio do aplicativo *WhatsApp* deram início a um debate mundial envolvendo as empresas de tecnologia, as autoridades, e os limites do uso da criptografia.

Em todos os casos (fevereiro e dezembro de 2015, março e julho 2016) envolvendo a empresa *WhatsApp* converteram na suspensão do serviço por um período determinado, além, de resultar na prisão preventiva do Vice-Presidente do *Facebook* em face da decisão proferida pelo juiz de Sergipe em fevereiro de 2015, em razão da recusa da empresa em encaminhar às autoridades policiais as mensagens de um narcotraficante, bem como a por descumprir ordens judiciais.

Nesse caso específico, por motivos de "ordem técnica" a divulgação do conteúdo das mensagens restou infrutífera, pois a única pessoa capaz de desbloquear a chave criptografia é o próprio usuário, e mesmo sob coação, a empresa não dispõe de qualquer mecanismo que venha a desbloquear os dados, ainda que por determinação judicial.

Não há dúvidas que nessa decisão o judiciário violou milhares de direitos individuais, além de ferir o direito e a liberdade de se comunicar no que se refere aos indivíduos que não estão no âmbito da jurisdição que envolve a polêmica decisão, asseverando assim, a insegurança que se encontra o poder judiciário brasileiro. A própria Agência Federal de Investigação – FBI, no intuito de quebrar a chave criptografada da empresa *Apple*, mediu todos os esforços possíveis, mas não demandou na prisão de ninguém, ou no bloqueio dos serviços de todos os usuários.

Pierre Lévy, estudioso da *Internet*, exalta o exercício da vigilância, ou também do Estado de vigilância[1] manuseada através da interceptação das comunicações criptografadas, bem como a resistência por parte dos entes estatais em face das tecnologias de liberdade:

> Os Estados vêem evidentemente na 'democratização' de poderosos instrumentos de criptografia um atentado à sua soberania e segurança. Por isso o governo dos Estados Unidos tentou impor com padrão um sistema de criptografia cuja chave seria conhecida por suas agências de informação. (...) Diversos governos, entre os quais o francês e o chinês, requerem autorização prévia (muito difícil de conseguir) para o uso das tecnologias de criptografia. A lei considera os milhares de franceses que usam o PGP sem autorização oficial possuem armas de guerra e poderiam atentar contra a segurança do Estado. (...)Observemos, enfim, para concluir esse assunto, que a proibição dos instrumentos de criptografia em um país não impede de forma alguma seu uso em toda parte pelo terrorismo e crime organizado, que, não se importando com uma ilegalidade, podem muito facilmente conseguir tais instrumentos, sobretudo através da rede (LEVY, 1999, p. 205-206).

Ainda, em sentido semelhante, Ruaro (2015) menciona que não é possível desconsiderar a importância dos sistemas de inteligência na preservação do bem-estar público e da própria segurança nacional. Todavia, prossegue a autora, tais atitudes não podem ferir a esfera privada dos indivíduos quando utilizadas indiscriminadamente pelo Estado. Até porque, "as novas tecnologias de vigilância, em especial aquelas referentes à interceptação de comunicações e dados, não se atém a uma jurisdição nacional, possuindo um alcance global ferindo direitos fundamentais de indivíduos que não têm, muitas vezes, relação com fatos a serem investigados em uma verdadeira subversão da ordem mundial" (RUARO, 2015).

Deste modo, atenta-se para os riscos incalculáveis que as TCI'S podem proporcionar à vida privada, quando tanto os indivíduos quanto o próprio ente Estatal estão na iminência de terem seus dados invadidos ou coletados não apenas na esfera nacional, mas em escala mundial, atingindo deslealmente direitos fundamentais, a exemplo do que aconteceu com as revelações de Edward Snowden.

Aliás, a própria legislação é omissa, pois tanto o Marco Civil da Internet quanto o anteprojeto de dados pessoais em tramitação ainda no Congresso Nacional não contemplam questões envolvendo a proteção de dados criptografados. Todavia, há de se levar em consideração, ainda, que o problema da criminalidade não vai ser estancado apenas com

[1] " O Estado de vigilância represente uma nova forma de organização do Estado. Ele adota parâmetros e tecnologias que utilizam as redes, em especial a internet no modelo vigente de protocolo Web, para promover o monitoramento e a coleta de dados, informações, comunicações e conteúdos, para atingir diferentes fins, em especial, o de estabelecer estratégias de segurança nacional". FORTES, Vinicius Borges. *O direito fundamental a privacidade*: uma proposta conceitual para regulamentação da proteção de dados pessoais na internet no Brasil. Tese de Doutorado, Rio de Janeiro: UNESA, 2015, 225p.

medidas de controle sobre os atos civis, como já antecipava Julian Assange (2013) "a vigilância de pessoas específicas não é a maior ameaça".

No ano de 2014, a Assembleia das Nações Unidas (ONU) por meio da Resolução 169/66 aprovou o relatório em que analisa a aproximação entre o direito de expressão e de opinião e o direito à privacidade utilizando-se da criptografia e do anonimato na esfera digital. Este relatório foi realizado em parceria pelo Brasil e pela Alemanha e almeja que as entidades estatais reavaliem suas legislações, políticas e práticas com o intuito que seja incorporado a promoção e proteção do direito à privacidade e outros direitos humanos na era digital, o mais breve possível (ASSEMBLEIRA GERAL DAS NAÇÕES UNIDAS, 2014).

De acordo com o relator especial sobre a liberdade de opinião e de expressão da ONU, David Kaye, a criptografia e o anonimato nas comunicações merecem uma forte proteção para salvaguardar o direito dos indivíduos de exercer sua liberdade de opinião e expressão[2]. Ainda, prossegue: "há alguns que podem ver criptografia e anonimato como questões menores na amplitude da liberdade de expressão hoje, mas tendo visto que muito da nossa expressão, hoje, acontece no espaço digital, essas ferramentas de segurança devem ser encaradas como estando no coração da opinião e da expressão na era digital" (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2014).

Nesse entendimento, depara-se que o desejo do Estado por mais controle e monitoramento dos indivíduos resta fragilizado se observado importantes relatórios de âmbito internacional como é o caso da ONU e da própria Diretriz Europeia 2016/679, a qual é referência na inovação da proteção de dados pessoais. E assim como o Brasil, que se consagra como um Estado Democrático de Direito, por mais que não disponha especificamente no bojo do seu ordenamento jurídico quanto da tutela de dados criptografados, não pode ele vir a limitar o exercício de direitos fundamentais como é o caso da privacidade, mas sim contemplar o debate em torno da garantia da criptografia como mecanismo de proteção essencial na salvaguarda da proteção de dados e da privacidade.

Manuel Castells, importante sociólogo espanhol, da mesma forma reconhece que a necessidade de preservar os indivíduos contra eventuais intromissões do governo, que podem levar a uma situação de controle no tocante ao processamento de informações em rede. Segundo o autor "a última tentativa por parte dos governos para manter algum grau de controle sobre os fluxos de informação" e que é "uma grande ironia histórica que a tentativa de controlar a informação proibindo a distribuição da capacidade de encriptação deixe os

[2] Disponível em: https://nacoesunidas.org/criptografia-e-anonimato-sao-centrais-para-liberdade-de-opiniao-e-expressao-na-era-digital-diz-onu/. Acesso em 08 jul. 2016.

Estados – e a sociedade – indefesos perante os ataques efectuados a partir da periferia da rede (CASTELLS, 2004).

Diante deste cenário, verifica-se que assim como a privacidade evoluiu significativamente nos últimos anos em decorrência da crescente demanda das novas tecnologias, da mesma forma instrumentos para assegurar sua proteção foram conquistando mais destaque como é o uso da criptografia para proteger as informações. E o Estado não pode retroceder e vir a representar uma ameaça quanto às liberdades individuais, mas sim, acompanhar as transformações político-sociais, sem, contudo, comprometer o bem-estar e autonomia de seus cidadãos. E a lição de Doneda (2016), transcreve bem o cenário atual "transparência deve ser diretamente proporcional ao poder. Privacidade deve ser inversamente proporcional[3]", ou seja, quanto mais transparentes forem as ações desenvolvidas pelo Estado, mais transparente será a atuação dele; enquanto em sentido inverno, na privacidade, a parte mais frágil, no caso os cidadãos, é quem merece maior proteção em detrimento do poder estatal.

CONCLUSÕES

Conforme apresentado, o Direito à privacidade, consagrado na Constituição Federal no artigo 5º, inciso X, denota-se essencial para o desenvolvimento de uma sociedade livre, igualitária e democrática. Sem liberdade não se exerce a privacidade, por isso a necessidade em conceber e efetivar o direito à privacidade, que em conjunto com a proteção dos dados pessoais confere a posição de direito humano fundamental.

Entretanto, há de se ressaltar que a efetivação do direito à privacidade não significa apenas positivá-lo perante a ordem jurídica, mas sim, priorizá-lo em detrimento as garantias inerentes ao ser humano, sem supostamente ser visto como um empecilho à segurança pública dos entes Estatais. Por isso a necessidade em reavaliar a atuação por parte do Estado diante de medidas e de controle que limitam cada vez mais as liberdades individuais, cujo pressuposto deve ser garantido no âmbito do Estado Democrático de Direito.

Tanto o Marco Civil da Internet como o Anteprojeto de Dados Pessoais (ainda em tramitação) representam um avanço normativo no tocante aos direitos relativos à *Internet*,

[3] Frase destacada em um evento promovido pela Associação Brasileira da Propriedade Intelectual (ABPI) em 29 de janeiro, o primeiro após a abertura da consulta pública, Danilo Doneda, coordenador geral de estudos e monitoramento de mercado da Secretaria Nacional do Consumidor do Ministério da Justiça. Disponível em: http://ibidem.org.br/v-seminario-do-cgi-discute-a-protecao-a-privacidade-e-aos-dados-pessoais-no-brasil/. Acesso em: 08 jul. 2016.

entretanto ainda, de um modo geral não abarcam explicitamente e de maneira segura questões que envolvam a integridade da tutela de informações pessoais. É nesse sentido que Diretriz Europeia 2016/679 merece ser incorporada na salvaguarda da privacidade, proteção e tratamento de dados pessoais.

Nesse cenário, apesar das incongruências e omissões por parte da legislação brasileira no tocante a privacidade e a proteção de dados pessoais, como ocorreu nos anos de 2015 e 2016 com o bloqueio do *WhatsApp* e a prisão do vice-presidente do *Facebook*, faz-se importante ressaltar que o uso da tecnologia baseada na criptografia além de possuir uma regulamentação específica na esfera internacional, também é contemplado por importantes relatórios, como o da ONU. Em razão disso, verifica-se o uso da encriptação de mensagens como artifício tecnológico capaz de assegurar a integridade e confidencialidade das mensagens transmitidas, dispondo assim de segurança em todo ambiente computacional, inclusive de eventuais intervenções por parte do Estado ou de terceiros, que se apropriam de informações indiscriminadamente, desrespeitando o direito à privacidade dos cidadãos.

Sob essa ótica, verifica-se que há um longo caminho a ser percorrido pelo Estado, pois quanto maior for o avanço das tecnologias, maior poderá ser a violação da privacidade e consequentemente de dados pessoais. Há um antagonismo entre avanço tecnológico e privacidade que não pode perdurar, por isso a necessidade em positivar e ampliar leis que regulamentam a proteção de dados pessoais. A Diretriz Europeia é exemplo a ser praticado em termos de regulamentação, que juntamente com técnicas criptográficas, podem resolver boa parte das lacunas jurídicas que envolvam a violação a privacidade e os dados pessoais.

É de suma importância para um Estado Democrático de Direito, como é o Brasil, desenvolver um sistema resiliente a qualquer tipo de violação ou ataque as liberdades individuais, pois a privacidade, e outras medidas igualmente importantes para a preservação da intimidade e da vida privada dos titulares das informações, não podem ser condenadas frente aos avanços tecnológicos. A proteção não pode ser vista como inimiga de inovação, mas sim como a salvaguarda tanto pelo respeito à liberdade de informação como pela preservação de importantes princípios fundamentais do Estado Democráticos de Direito.

REFERÊNCIAS

ALEIXO, Gabriel; RADU, Roxana. *Blockchain* e o futuro da governança. ITS Rio. Nov. 17, 2015. Disponível em: http://www.diplomacy.edu/blog/blockchain-and-future-governance. Acesso em 01 jul. 2016.

ALONSO, Félix Ruiz. Pessoa, intimidade e o direito à privacidade. In: MARTINS, Ives Gandra; PEREIRA JÚNIOR, Antônio Jorge (coordenadores). *Direito à privacidade*. São Paulo: Centro de Extensão Universitária, 2005, pp. 11-35.

ALMEIDA, Coriolano; CRESPO, Marcelo. *A proteção aos dados pessoais no ordenamento jurídico brasileiro e o anteprojeto do Ministério da Justiça*. Disponível em: http://www.migalhas.com.br/DireitoDigital/105,MI220187,81042-A+protecao+aos+dados+pessoais+no+ordenamento+juridico+brasileiro+e+o. Acesso em 07 jul. 2016.

ASSANGE, Julian. *Cypherphunks:* Liberdade e o futuro da internet. Tradução Cristina Yamagami. São Paulo: Boitempo, Editorial, 2013.

BOFF, Salete Oro; DIAS, Felipe de Veiga Dias. *Direito à privacidade online*: um sonho virtual ou uma realidade constitucionalmente possível?. In: ADOLFO, Luiz Gonzaga Silva (coord.). Direitos Fundamentais na Sociedade da Informação. Florianópolis: UFSC/GEDAI, 2012.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 01 jul. 2016.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 06 jul. 2016.

CAMPUZANO TOMÉ, Hermínia. *Vida privada y datos personales:* su protección jurídica frente a la Sociedad de la Información. Madrid: Tecnos, 2000.

CASTELLS. Manuel, *A Galáxia Internet* – Reflexões sobre Internet, Negócios e Sociedade, Fundação Calouste Gulbenkian, 2004.

CELLA; José Renato; ROSA, Luana Aparecida. *Controle social e necessidade de proteção de dados pessoais*. Revista Democracia Digital e Governo Eletrônico (ISSN 2175-9391), n° 9, p. 158-171, 2013, p. 158-171.

CERT.BR, CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. *Cartilha de Segurança para Internet*. Disponível em: <http://cartilha.cert.br/criptografia/>. Acesso em 07 de jul. 2016.

CONSELHO DA EUROPA. *Convenção no 108 para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal*. Estrasburgo. 28 de janeiro de 1981. Disponível em <http://www.apdt.org/guia/L/Ldados/108.htm>. Acesso em: 06 jul. 2016.

DELEUZE, Gilles. *Controle e Devir*. In: Conversações. Trad. de Peter Pál Pelbart. São Paulo: Editora 34, 1992.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006.

FOUCAULT, Michel. *Vigiar e punir*: nascimento da prisão. Tradução de Raquel Ramalhete. Petrópolis: Vozes: 1987.

FORTES, V. B. *O direito fundamental a privacidade***:** uma proposta conceitual para regulamentação da proteção de dados pessoais na internet no Brasil. Tese de Doutorado, Rio de Janeiro: UNESA, 2015, 225p.

FRANÇA, Waldizar Borges de Araújo. *Criptografia*. Universidade Católica de Brasília, 2005, Distrito Federal.

GARCÍA, Clemente García. *El derecho a la intimidad y dignidad em la doctrina del Tribunal Constitucional*. Murcia: Universidad de Murcia, Servicio de Publicaciones, 2003, 151-154.

LÉVY, Pierre. *Cybercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LIMBERGER. Têmis. *O direito a intimidade na era da informação*: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

LORENZETTI. Ricardo Luis. *Fundamentos do direito privado*. São Paulo: Revista dos Tribunais, 1988.

RODOTÀ, S. *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro, Renovar, 2008, p.

RODOTÁ. Stefano. *Tecnologia e diritti*, in: Giuristi e legislatori. GROSSI, Paolo (cur), Milano. Giuffrè, 1997.

RUARO. Regina. *Privacidade e autodeterminação informativa obstáculos ao estado de vigilância?* Arquivo Jurídico – ISSN 2317-918X – Teresina-PI – v. 2 – n. 1, 2015, p. 41-60.

SIMSON Garfinkel. Web Security, *Privacy & Commerce*. O'Reilly, 2nd edition, january, 2002.

SOUTO, Bruno Guedes. *Transmissão de dados esteganografados e criptografados no cabeçalho de pacotes TCP/IP*. Trabalho de conclusão de curso. Brasília, 2008, Distrito Federal.

SOUZA, Sérgio Ricardo de. *Controle judicial dos limites constitucionais à liberdade de imprensa*. Rio de Janeiro: Lumen Juris, 2008.

SOUZA, Douglas Delgado de. *Criptografia Quântica com Estados Comprimidos da Luz*. 2011.Dissertação de Mestrado, Universidade Estadual de Campinas.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 32ª ed. São Paulo: Malheiros, 2009.

VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação, efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Porto Alegre: Sergio Antonio Fabris Editor, 2007, p. 40-44.

WARREN e BRANDEIS, *"The right to privacy"*.Harvard *law review.* Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 09 jul. 2016.

WEINGARTNER NETO Jayme. *Honra, privacidade e liberdade de imprensa*: uma justificação penal. Porto Alegre: Livraria do Advogado, 2002.
WESTIN, A. F. *Privacy and Freedom*. New York. Altheneum, 1967.