FUNDAÇÃO PRESIDENTE ANTÔNIO CARLOS

FACULDADE DE DIREITO

2019

A ENCRIPTAÇÃO DE DADOS: O CONFLITO ENTRE EMPRESAS PRIVADAS E O ESTADO

Matheus Rodrigues Marques – matheusrodriguesmarques@yahoo.com.br

Alexandre Ribeiro da Silva - alexandreribeiroadv@gmail.com

RESUMO

O presente trabalho tem como objetivo questionar se a utilização por empresa de dados de encriptação é permitida em nosso ordenamento, como garantidora da privacidade dos usuários, ou se demonstra como ofensa ao direito à informação para fins de persecução penal pelo Estado. Tal tecnologia impossibilita a consulta por um terceiro que não seja o receptor e o emissor, gerando um conflito entre empresas privadas e as autoridades investigativas. O referencial teórico utilizado no presente estudo foi o artigo Direitos Humanos e Criptografia dos autores Wolfgang Schulz e Joris Van Hoboken. Esse trabalho utilizará como método de abordagem, o dialético, e como método investigativo, as súmulas, legislação, livros, revistas jurídicas etc.
Palavras-chave: Encriptação; Privacidade; Internet; Proteção; Segurança.

ABSTRACT

This paper aims to question whether the use of encryption data by a company is permitted in our system, as a guarantor of users' privacy, or demonstrates as an offense to the right to information for the purposes of criminal prosecution by the State. Such technology makes it impossible for a third party other than the receiver and the sender to consult, creating a conflict between private companies and investigative authorities. The theoretical framework used in this study was the article Human Rights and Cryptography by authors Wolfgang Schulz and Joris Van Hoboken. This work will use as a method of approach, the dialectic, and as an investigative method, the summary, legislation, books, legal magazines and etc.
Keywords: Encryption; Privacy; Internet; Protection; Safety.

INTRODUÇÃO

O presente trabalho tem como problema questionar se utilização por empresa de dados de encriptação é permitida em nosso ordenamento, como garantidora da privacidade dos usuários, ou se demonstra como ofensa ao direito à informação para fins de persecução penal pelo Estado.

Diante de tal fato, há um conflito entre as empresas privadas e o Estado sobre a possibilidade de fornecimento ou não dos dados encriptados, sendo que também há um debate dentro da própria legislação sobre o tema, pois não está bem definido na Lei.

Para tanto, no primeiro capítulo será abordado sobre a encriptação como forma de proteção dos dados pessoais, pois com tal método, as empresas e os usuários dos serviços possuem uma maior segurança para a navegação.

Posteriormente, no segundo capítulo, se analisará a regulamentação da encriptação em nosso ordenamento a partir do Marco Civil da Internet e da Lei Geral de Proteção de Dados ou LGPD.

Neste contexto, finalizar-se-á com uma análise crítica os conflitos entre empresas privadas e o Estado, pois em conformidade com a lei, as empresas citam que a privacidade é um direito de todos, ou seja, a criptografia é nesse caso lícito, uma vez que fornece tal garantia. Em contrapartida, o Estado e as autoridades investigativas são contrários a adoção de tal método, uma vez que está expresso na lei que mediante ordem judicial, as empresas são obrigadas a fornecerem os dados dos usuários, o que é impossível se tratando de alguns métodos de encriptação.

O referencial teórico utilizado no presente estudo foi o artigo direitos humanos e criptografia dos autores Wolfgang Schulz e Joris Van Hoboken. Esse trabalho utilizará como método de abordagem, o dialético, e como método investigativo, as Súmulas, legislação, livros, revistas jurídicas e etc.

1. A ENCRIPTAÇÃO DOS DADOS PESSOAIS

Atualmente, na sociedade contemporânea, a vida do cidadão comum é construída a partir do compartilhamento de dados. Neste sentido,

> "A participação e a inclusão nesse novo modelo de sociedade exigem dos indivíduos maior abertura de informações a seu respeito, como, por exemplo, na contratação de um determinado serviço que somente se concretiza a partir

> do fornecimento de dados pessoais ou, ainda, nas aplicações de um aparelho celular que só funciona a partir do perfil construído pela coleta de seus dados. É certo que atualmente as novas tecnologias como navegação em nuvem, internet das coisas, convergência e sincronicidade de multiplataformas e aparelhos auxiliam o avanço e a prática do uso da tecnologia e informação. Graças ao progresso tecnológico é possível acessar esses dados, seja por e-mail ou por rede social, em qualquer celular ou computador.
> Neste sentido, uma aplicação pertinente e concreta do Direito só será efetiva se considerar a realidade social a qual se está inserido, reconhecendo que essa realidade é fatalmente condicionada pelo desenvolvimento tecnológico vivenciado". (SILVA, 2017, p. 17)

Destarte, a proteção da privacidade contemporaneamente passa pela tutela sobre as manipulações dos dados pessoais. Assim, a tutela da privacidade deve passar por uma percepção pelos órgãos responsáveis que:

> - passamos de um mundo no qual as informações pessoais estavam substancialmente sob exclusive controle dos interessados para um mundo de informações divididas com uma pluralidade de sujeitos;
> - passamos de um mundo no qual a cessão das informações era, em grande parte dos casos, efeito das relações interpessoais, tanto que a forma corrente de violação da privacidade era a "fofoca", para um mundo no qual a coleta das informações ocorre através de transações abstratas;
> -passamos de um mundo no qual o único problema era o controle do fluxo de informações que saíam de dentro da esfera privada ao exterior, para um mundo no qual se torna cada vez mais importante o controle das informações que entram, como demonstra a crescente importância assumida pelo direito de não saber, pela atribuição aos indivíduos do poder de recusar interferências em sua esfera privada, como as derivadas da remessa de material publicitário e do marketing direito;
> Vivemos em um mundo no qual aumenta o valor agregado das informações pessoais, com uma mudança de paradigma, onde a referencia ao valor em si e de sua dignidade passou a secundário em relação à transformação da informação em mercadoria;
> - vivemos em um mundo no qual se começa a refletir conscientemente sobre o fato de que, até agora, as tecnologias da informação e da comunicação assumiram muito frequentemente as características de tecnologias sujas, aproximando-se muito mais do modelo das tecnologias industriais poluentes, tornando-se fundamental, portanto favorecer ou impor a introdução no ambiente informativo de tecnologias limpas;
> - vivemos em um mundo no qual as tecnológicas da informação e da comunicação contribuíram para tornar cada vez mais sutil a fronteira entre esfera pública e a esfera privada; e a possibilidade de construção livre da esfera privada e de desenvolvimento autônomo da personalidade passou a ser condições para determinar a efetividade e a amplitude da liberdade na esfera pública. (RODOTÁ, 2008, p.127)

Neste sentido,

> Essas novas interações intersubjetivas por meios digitais e a expansão global da internet permitem a manipulação de informações pessoais em grande escala. Surgiram empresas e instituições públicas capazes e dispostas a coletá-las, moldá-las e empregá-las na transformação do mundo e na geração de outros conhecimentos e bens a partir da utilização dos dados pessoais eletrônicos. (SILVA, 2017, p.4)

Uma das principais formas de proteger as informações e dados pessoais dos usuários é a utilização da tecnologia da encriptação.

A encriptação é uma chave secreta de dados dos usuários que codificam suas mensagens e conteúdos acessados por eles, com o objetivo principal de evitar que terceiros maliciosos utilizem ou saibam o que e porque a pessoa está navegando. Com isso, a criptografia é capaz de guardar seus dados e não mantê-los expostos para garantir uma acessibilidade com eficácia e segurança para todos os usuários.

É um tema de longa data no campo tecnológico, que se utiliza da matemática, da engenharia e da computação, e é normalmente definido como "a proteção da informação e computação mediante o uso de técnicas matemáticas".

Nas Diretrizes da OCDE, Encriptação e Criptografia são definidas da seguinte forma:

> "Encriptação" significa a transformação de dados pelo uso de criptografia para produzir dados ininteligíveis (dados encriptados) para garantir sua confidencialidade.
> "Criptografia" significa a disciplina que incorpora princípios, meios e métodos para a transformação de dados a fim de ocultar seu conteúdo informativo, estabelecer sua autenticidade, impedir a sua modificação não detectada, impedir o seu repúdio e/ou impedir o seu uso não autorizado. (SCHULZ e VAN HOBOKEN, 2016, p.11)

Com isso, é evidente que a criptografia é um instrumento fundamental para as empresas e para os usuários, por meio do qual através de códigos as pessoas têm sua intimidade e sua privacidade preservada, onde seus dados ficam armazenados e são utilizados apenas o necessário para cada caso, não havendo riscos de vazamentos a terceiros.

A cada ano que se passa fica mais evidente a evolução da criptografia e a relevância da mesma no cenário digital mundial, pois são implantadas no intuito de garantir a segurança das informações e comunicações no âmbito pessoal, comercial e no setor público, uma vez que protegem o anonimato dos agentes de comunicação.

O uso da encriptação é um tema um tanto quanto polêmico, pois provoca debates em âmbito nacional e internacional entre países. Esses litígios ganharam os noticiários após Eduardo Snowden vazar informações para a mídia que os Estados Unidos estariam espionando outros países sem o consentimento dos mesmos, ou seja, algo gravíssimo e ilegal.

Com tal vazamento de informações, Eduardo Snowden disse ter alertado até então a Presidente Dilma Roussef que o seu celular e seus aplicativos nas redes estavam sendo monitorados o tempo inteiro, porém, a mesma não lhe deu a devida atenção quando ele a disse que deveria implementar o uso da criptografia em seus objetos eletrônicos no dia a dia. Com isso, vazaram informações e conteúdos sobre tudo o que a então Presidente se comunicava tanto em segredo de Estado quanto a sua própria intimidade.

Deste modo, estão sendo desenvolvidas e atualizadas novos formatos de criptografias, mais evoluídos e mais bem trabalhados, chamado criptografia de ponta a ponta, que consiste em um recurso de segurança que protege a intimidade e a privacidade dos usuários, tanto o remetente quanto o destinatário.

Com esse novo modelo, é impossível a invasão de hackers mal intencionados terem acessos a conteúdos exclusivos do usuário, até porque trata-se de um modelo amplamente eficaz e que gera tranquilidade e segurança para as pessoas.

A técnica de criptografia mais utilizada é entre o usuário da internet e o provedor de serviços específicos, por meio do qual são protegidos contra acessos não autorizados de terceiros. Com isso, ambos dependem um do outro para estabelecer esta relação de privacidade, pois o usuário não pode estabelecer a criptografia unilateralmente, apenas com os dois lados tendo anuência.

A criptografia dos metadados se dá pelas informações dos dados dos usuários e seus comportamentos diante dos meios de comunicação, o que é ameaçador para os usuários da internet de um contexto geral.

Através do referido metadado, os provedores de serviços sabem o que o usuário fez e faz em tempo real: o local, o site, o aplicativo, a duração de tempo em cada site, à comunicação com outras pessoas etc. Deste modo, fica evidente a ameaça com relação à segurança e a privacidade do usuário, pois podem ser rastreados geograficamente em tempo real.

Neste sentido, Schulz e Van Hoboken (2016, p.26) dispõem:

> “A disponibilidade de metadados, ou seja, as informações relativas aos dados de usuários e seus comportamentos de comunicação, podem representar uma ameaça particular aos usuários. Por metadados, neste contexto, nos referimos às informações que os provedores de serviços podem observar na prestação de serviços: quando; com que frequência; por quanto tempo; e com quem os usuários estão se comunicando. É possível inferir gráficos de comunicação, bem como padrões comportamentais detalhados de tais dados. Os metadados também podem ser usados para rastrear pessoas geograficamente e interferir na sua capacidade de se comunicarem anonimamente”.

Com isso, é perceptível que a encriptação é de suma importância para os usuários da Internet, uma que vez que o navegante terá a garantia da sua privacidade e a segurança para utilizá-la. Além disso, a encriptação permite diversos benefícios aos usuários, dentre eles e talvez o principal é a proteção de dados, que significa que todos os dados pessoais dos usuários e das empresas são confidenciais, ou seja, independente da transação ou do conteúdo, as partes não correm o risco de ter sua intimidade violada, pois a encriptação praticamente deixa impossível o acesso de terceiros ou hackers invadirem o seu sistema. Neste contexto,

> ”Técnicas criptográficas têm sido implantadas de maneira ampla por diversos atores, com o intuito de garantir proteção das informações e da comunicação no âmbito pessoal, comercial e no setor público. Técnicas criptográficas também são usadas para proteger o anonimato dos agentes de comunicação e, com isso, a privacidade em geral”. (SCHULZ e VAN HOBOKEN, 2016, p.11)

A afirmação acima demonstra a relevância da encriptação nos dias atuais, visto que é um excelente benefício tanto para os prestadores dos serviços quanto para os usuários do serviço, uma vez que garantem a privacidade e a segurança nas transações e na utilização de aplicativos.

2. A ENCRIPTAÇÃO NA REGULAMENTAÇÃO BRASILEIRA

Com objetivo de tutelar a utilização destes dados pelo usuário e a privacidade, primeiramente foi promulgado o Marco Civil da Internet, também conhecido como a Constituição da Internet Brasileira, que é uma lei que garante aos usuários da rede uma maior segurança com relação à utilização da internet por usuários comuns e empresas. A mencionada Lei 12.965 de 23 de junho de 2014 tem como prioridade levar a todos as garantias, direitos e deveres das partes. Ou ainda,

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> I - o reconhecimento da escala mundial da rede;
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> III - a pluralidade e a diversidade;
> IV - a abertura e a colaboração;
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VI - a finalidade social da rede.

Assim, o ambiente de inovação com a nova lei surgiu para disciplinar as empresas operadoras de produtos ou serviços associados à internet e os usuários dos serviços. A criação dessa lei específica teve um embasamento em três fundamentos que logo mais viraram redações na legislação, que são: privacidade, neutralidade da rede e fiscalização dos acessos.

O princípio da privacidade, na web, é a garantia que os usuários possuem de que seus dados pessoais serão preservados, ou seja, não terão sua intimidade revelada ou descoberta por terceiros. Neste sentido:

> "O princípio da privacidade nada mais é do que a garantia de inviolabilidade das comunicações dos usuários. Nesse sentido, a Lei do Marco Civil atribui o dever de sigilo de suas informações ao provedor do recurso de internet.
> A quebra de tal garantia somente pode acontecer por meio de ordem judicial, quando forem imprescindíveis para a elucidação de ações ilícitas, bem como na tentativa de identificação dos seus responsáveis.
> Além disso, vale ressaltar que as empresas estrangeiras que pretendem atuar no país também deverão se adaptar às diretrizes do ordenamento jurídico brasileiro, o qual envolve não somente o Marco Civil da Internet, mas todas as legislações que cuidam desses direitos". (CRUZ, 2017)

O princípio da neutralidade significa que a navegação não pode ser diferenciada em outras regiões ou em outros sites, independente de lugar, hora ou site acessado, a velocidade da Internet continuará sempre a mesma, sem a distinção de velocidade pela empresa fornecedora da rede. Neste sentido:

> "Esse princípio tem a função de coibir ações abusivas praticadas pelas empresas na prestação do serviço de internet e telefonia, por exemplo limitando que os seus clientes acessassem alguns sites ou serviços.
> Antes, os usuários esbarravam numa série de critérios para a utilização de cada tipo de conteúdo — a sua origem e o destino do que estavam consumindo. Basicamente, a pessoa adquiria um plano de dados "X", mas se quisesse ter acesso ao Facebook, por exemplo, deveria comprar um pacote adicional, específico para tal finalidade.
> Um dos objetivos da lei foi justamente proporcionar um tratamento igualitário entre os consumidores, gerando conformidade com as suas expectativas de volume e velocidade de dados". (CRUZ, 2017)

E, por fim, o princípio da fiscalização dos acessos consiste em que a empresa fornecedora do serviço é obrigada a armazenar os dados de conexão e registro durante o período de 1 ano do usuário da rede. Neste sentido:

> "Tem-se a regulamentação do processo de armazenamento dos registros de dados de conexão. Trata-se de uma responsabilidade da empresa provedora do serviço cujo prazo mínimo da obrigação é de 1 ano. Caso necessário, as autoridades podem exigir de um provedor alguns dados cadastrais que

> qualifiquem os seus usuários, como nome completo, estado civil, profissão, filiação, endereço". (CRUZ, 2017)

A criação da lei do Marco Civil, com o paradigma dos princípios apontados, foi de extrema importância, pois abre precedentes para debates acerca de até onde chega à tutela ao princípio da privacidade de acordo com a norma.

Isto porque a neutralidade exige a indistinção do tratamento do conteúdo, o que de certo modo já preserva a inviolabilidade dos dados trafegada pelos operadores de conexão e de conteúdo.

Já o princípio da fiscalização dos acessos, garante que a empresa somente armazene determinado dado, a saber, os registros ou de conexão ou de acesso a depender do serviço ofertado, por um prazo mínimo.

Portanto, com a cumulação dos três princípios a empresa prestadora de serviços não terá acesso a outros dados privados, como o próprio conteúdo dos pacotes de dados. Aliás, isso está expresso no marco Civil:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. (grifos nossos).

De acordo com o advogado especialista em direito empresarial Paulo Cesar Busnardo Junior**,** sócio do escritório PN&BA - Peregrino Neto & Beltrami Advogados, o Marco Civil da Internet é claro ao garantir o direito à privacidade aos usuários da rede, onde o mesmo diz:

> "Tais dados e informações são objetos de proteção por sigilo legal, especialmente por parte dos provedores de serviços de internet. Estes dados somente poderão ser disponibilizados por ordem judicial, como regra geral, salvo algumas exceções legais como o consentimento livre, expresso e informado do próprio usuário." (BUSNARDO JÚNIOR, 2015)

Sendo assim, é perceptível que as empresas não disponibilizam dados dos seus usuários, até porque estariam violando a proteção de dados e a privacidade, presentes no art.3°, incisos II e III:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> **II - proteção da privacidade;**
> **III - proteção dos dados pessoais, na forma da lei;**
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (grifos nossos)

E com vistas às garantias estipuladas e às demandas do próprio mercado, as empresas cada vez mais têm se aperfeiçoado em técnicas para não fornecer dados de seus usuários, a fim de manter a integridade e a intimidade dos mesmos, para que possam ter uma navegação tranquila e com sua privacidade guarnecida na forma da lei, como no caso da encriptação de dados que é o objeto de análise do presente estudo.

Não por menos, foi formalizada no próprio regulamento do Marco Civil da Internet (Decreto nº 8.771/2016), em seu art. 13, IV, a encriptação como diretriz sobre padrões de segurança da informação:

> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
> (…) IV – o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, **como encriptação ou medidas de proteção equivalentes**. (grifos nossos)

Em síntese, a utilização de criptografia foi acolhida pelo Marco Civil como diretriz de segurança da informação.

E balizando esta previsão, também foi aprovada a Lei geral de proteção de dados (LGPD), lei 13.709/2018, que é a legislação que regula a proteção dos dados pessoais dos usuários de aplicativos e navegações de internet.

A legislação é relativa à privacidade e proteção de dados e está fortemente interligada a proteção dos direitos humanos, pois garante a todos o direito ao princípio da segurança. Esse princípio sugere que sejam tomadas medidas de segurança adequadas para garantir a proteção de dados pessoais contra o acesso ilegal de terceiros aos destinatários pretendidos. É o que está previsto no artigo 46 da lei:

> Art. 46. Os agentes de tratamento **devem adotar medidas de segurança**, **técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados** e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> § 1º **A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo**, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. **(grifos nossos)**

Diante disso, abre-se espaço para o método da criptografia legal, pois há uma lei que visa proteger os direitos dos usuários, das empresas ou de qualquer outro prestador de serviços que estejam interligados no mundo digital.

Mas, ao mesmo tempo, cria-se uma precedente no parágrafo 1º do art 46 da LGPD que determina que a "autoridade nacional" deverá dispor sobre os padrões técnicos mínimos para a aplicabilidade da tecnologia da criptografia.

No presente ano de 2019, foi editada a Lei nº 13.853 que trata da criação a Autoridade Nacional de Proteção de Dados e dá outras providências. Mas apesar da criação do órgão responsável pela difusão e regulamentação das tecnologias a serem adotadas para a criptografia, a lei se cala nesse sentido, deixando a questão ainda em aberto.

E agrava-se ao fato de que a encriptação não é bem aceita por autoridades, uma vez que a utilização desta tecnologia, em tese, inviabiliza o acesso às informações criptografadas tecnicamente, ainda que mediante ordens judiciais.

3. A ENCRIPTAÇÃO X DIREITO À INFORMAÇÃO PÚBLICA

No Marco Civil da Internet, em seu artigo 23 da Lei 12.965, o legislador garantiu que se necessário, haveria como obter informações sigilosas dos usuários e teriam que ser fornecidas pelas empresas após ser conseguida uma ordem judicial, a

qual a mesma deveria conter a anuência do juiz para conseguir os registros de conexões ou registros de acessos e aplicações da internet, conforme disposto a seguir:

> Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

Em consonância com tal artigo, percebe-se que desta forma, a empresa seria obrigada a fornecer tais dados requeridos a pedido da justiça no caso de o juiz julgar necessária e relevante tais informações para o prosseguimento da investigação. Diante do disposto, a empresa estaria colaborando de forma investigativa com as autoridades que aplicam tal ato, sendo que, com tais dados fornecidos, é mais fácil encontrar irregularidades e encontrar as pessoas em casos de quebra da lei, ou seja, em casos de práticas de crimes.

Porém, os responsáveis pelos tratamentos de dados alegam que a utilização de encriptação de ponta a ponta não permite a "quebra" do sigilo do conteúdo, uma vez que pela própria tecnologia somente o emissor e o receptor teriam acesso. Sendo assim, as empresas não se enxergam obrigadas a fornecer os dados pessoais de seus usuários as autoridades investigativas, uma vez que, seu comprometimento na realidade é com o seu usuário e com o bem estar do mesmo, para atrair novos contingentes de pessoas, e que cada vez mais vem agradando aos usuários o fato de não ter como ser exposto mediante os meios tecnológicos.

Exemplo recente deste conflito entre autoridades e empresas é o caso do aplicativo whatsApp que foi alvo de quatro decisões de bloqueio no Brasil, devido aos empresários ou responsáveis pelas empresas no país terem se negado a prestar informações mediante ordem judicial, fator previsto na legislação vigente, sendo que, três delas que foram levadas a cabo, por não entregar conteúdo de comunicações de investigados em inquéritos e processos penais. Durante tal período em que houve esses bloqueios, o aplicativo citado ficou "fora do ar" no país, ou seja, o aplicativo não funcionava, estava bloqueado por não cumprir as ordens judiciais requeridas pelas autoridades brasileiras.

O serviço de mensagens alega nos casos que a impossibilidade se deve à adoção do método da criptografia de ponta a ponta, ou seja, nem o WhatsApp tem conhecimento sobre o que os seus usuários estão se comunicando, apenas sabem que existem a comunicação, porém sem acesso ao conteúdo do diálogo.

Outro exemplo presente no marco teórico foi que, em março de 2016 o juiz da Vara Criminal de Lagarto (SE), Marcel Maia Montalvão, decretou a prisão de Diego Jorge Dzodan, vice-presidente do Facebook na América Latina, motivada pelo descumprimento da ordem judicial em um processo envolvendo tráfico de drogas interestadual, no qual a Polícia Federal solicitou ao Juízo a quebra do sigilo de mensagens trocadas pelo WhatsApp.

Mesmo diante de tal fato, foi negado o pedido para entregarem o conteúdo da comunicação entre os usuários, onde foi afirmado que não era possível a obtenção de tal fato devido modelo adotado de criptografia do aplicativo. E no dia seguinte, o desembargador plantonista Ruy Pinheiro da Silva, do Tribunal de Justiça do Estado de Sergipe, concedeu *habeas corpus* ao mesmo.

Desde o momento em que implementou a chamada "criptografia de ponta a ponta", a empresa tem reiterado a impossibilidade técnica de cumprir ordens judiciais de interceptação, o que sucinta a algumas autoridades a necessidade de se criar plataformas e tecnologias de encriptação que permitam acesso às autoridades

Contra a tal implementação do método da criptografia, as autoridades investigativas insistem em expressar que a encriptação não poderia ser lícito, uma vez que não segue a legislação vigente no Brasil, gerando diversos conflitos, como dispõe a Juíza Daniela Souza:

> "Qualquer empresa que se instale no País fornecendo determinado serviço, deverá estar apta a cumprir as decisões judiciais que, porventura, recaiam sobre esta, sob pena de cancelamento do próprio serviço, […]. A falta ou a negativa de informação por parte da empresa, deixando de atender a uma determinação judicial, impede aos órgãos de persecução de apurarem os ilícitos e alcançarem os autores dos crimes praticados, constituindo-se a recusa no fornecimento dos dados mera estratégia da empresa a fim de procrastinar e até descumprir a ordem judicial, sob o pálio de impossibilidades técnicas" (Marco teórico).

Apesar da insatisfação o posicionamento da juíza não é totalmente correto. De fato há que discutir a viabilidade de se cumprir ordem legal, mas a criptografia tem guarida tanto no Marco Civil da Internet como na Lei Geral de proteção de Dados pessoais como já exposto no capítulo anterior.

Com isso, apresentou-se um conflito muito grande, pois de acordo com o Marco Civil da Internet, após ordem judicial, as empresas têm a obrigação de fornecer os dados pretendidos pela autoridade investigativa, o que está previsto em seus artigos, porém não foi atendida por suposta impossibilidade tecnológica. O professor Danilo Doneda, sobre o tema, aduz que:

> De fato, a impossibilidade de atender a tais pedidos leva a discussão para outro patamar, ao questionar se os serviços de mensagens devem ser arquitetados para permitir o acesso ao seu conteúdo por autoridades, pela introdução de uma espécie de "grampo digital". E a solução que mais frequentemente é vislumbrada para isto é uma espécie de “chave-mestra” (ou porta dos fundos - backdoor), uma ferramenta que torne compreensível ao seu detentor qualquer comunicação em um sistema criptografado. (DONEDA, 2017, n.p).

Como solução ao dilema as autoridades contrariadas exigem a adoção de uma tecnologia “grampeável” por entrega de uma “chave –mestra” capaz de descriptografar os conteúdos quando assim exigíveis pela autoridade investigadora. Mas sobre a possiblidade aventada, novamente esclarece o professor Doneda

> “A solução das backdoors, que à primeira vista pode parecer razoável, infelizmente contrasta diretamente com a experiência acumulada em segurança da informação, que indica que a implementação de uma chave-mestra inexoravelmente diminui drasticamente a segurança de um sistema criptográfico. Em outras palavras, simplesmente não é possível implementar uma backdoor e manter a segurança que a criptografia tinha anteriormente, tornando-a mais vulnerável à intromissão de terceiros no conteúdo das comunicações e fragilizando as utilizações que necessitem de maior segurança”. (DONEDA, 2017, n.p).

Ou seja, a partir de criada uma descriptação viável, a própria criptografia cai por terra, uma vez que não há como se garantir a inacessibilidade da chave mestra, colocando em risco todos os dados privados de quem se utiliza a tecnologia.

Diante disso, há um conflito muito grande entre o Estado e as empresas privadas, pois se usarem tal criptografia, nem mesmo com ordem judicial, as autoridades investigativas terão acessos ao conteúdo desse meio de comunicação, mas abrindo a tecnologia a possiblidades de descriptar acaba-se com o próprio propósito da mesma.

Por outro lado, ao se utilizar de criptografia, as pessoas se comunicam com uma maior segurança, sabendo que não estão expostas e vulneráveis nos meios de comunicação, o que preserva os princípios do Marco Civil da Internet ou Constituição da Internet Brasileira.

Diante disso, o então Ministro da Justiça Alexandre de Moraes declarou intenções de trazer um projeto de lei que regularia aplicativos de mensagens que utilizam criptografia e o Supremo Tribunal Federal convocou audiências públicas para entender as complexidades técnicas dessa tecnologia. Tal iniciativa ainda não rendeu frutos e a questão permanece em aberto.

Neste contexto, é possível a afirmação que as Empresas e o Estado estão em um litígio interminável, uma vez que a própria legislação é omissa com relação a encriptação. Porém, a mesma defende a proteção à privacidade dos dados, o que abre um precedente para a utilização da criptografia, pois o principal objetivo de tal método é a preservação da privacidade e maior segurança para as empresas prestadoras de serviços e os usuários que contratam e utilizam de tais serviços.

Além disso, é comprovada a importância da criptografia, pois preserva a inviolabilidade dos direitos dos usuários da Internet em um contexto geral, gerando uma satisfação de quem está navegando e utilizando de tal serviço. A confidencialidade neste caso é algo de sumo importância entre as empresas fornecedoras dos serviços e o destinatário final.

CONCLUSÃO

O presente estudo foi realizado através de análise sobre os conceitos de encriptação e os marcos legais no Brasil sobre o tema que buscaram explanar a contradição entre a natureza de proteção do sigilo dos dados em contrapartida à necessidade das autoridades de acessarem o conteúdo destes dados em determinados casos.

A encriptação tem em sua essência o princípio da privacidade dos usuários da Internet, o que é de suma importância para as partes em qualquer relação do mundo online. Com isso, foi-se criado um conflito, no qual as empresas privadas são favoráveis à adoção da criptografia, pois assim garante a segurança para os usuários e também para a própria empresa prestadora do serviço, e o Estado, representado pelas autoridades investigativas, que relutam contra a encriptação, uma vez que alguns modelos de criptografia são impossíveis de descobrir os dados pessoais e os conteúdos da comunicação entre os usuários, desse modo não auxiliando nas investigações conforme previsto na Lei anteriormente citada.

Buscou-se evidenciar a relevância na aplicação do método em questão, sendo possível o deferimento da encriptação baseando que a mesma oferece garantias principiológicas para os usuários e empresas que utilizam a Internet de forma geral, uma vez que estabelece um elo maior de segurança para ambas as partes. Diante disso, a regulamentação da LGPD será de suma importância para cessar os conflitos existentes entre o Estado e as Empresas privadas quanto à criptografia.

Sendo assim, a encriptação não pode ser impedida de ser utilizada, visto que o seu uso traz enormes benefícios a todos os usuários de aplicativos e dos meios de comunicação. Com isso, o Estado não pode ter acesso a uma "chave mestra", que teria o intuito de quebrar a encriptação, uma vez que perderia o sentido da criptografia, que é ser inviolável para garantir a privacidade e a segurança dos usuários.

BIBLIOGRAFIA

ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação, Vol, 3, dezembro de 2017. Disponível em: Revista Brasileira de Políticas Públicas. Acesso em: 25 de out. 2019.

BUSNARDO JÚNIOR, Paulo César. Privacidade é um dos temas mais polêmicos do Marco Civil da Internet, 12 de abril de 2015. Disponível em: https://www.migalhas.com.br/Quentes/17,MI218759,31047-Privacidade+e+um+dos+pontos+mais+polemicos+do+marco+civil+da+internet. Acesso em: 10 de out. 2019.

CRUZ, Carlos Henrique. Marco Civil da Internet: o que é e o que muda para o seu negócio, 27 de fevereiro de 2017. Disponível em: https://chcadvocacia.adv.br/blog/marco-civil-da-internet/#Principio_da_neutralidade_da_rede-. Acesso em: 15 de out. 2019.

DONEDA, Danilo. A regulação da criptografia e o bloqueio do WhatsApp, 30 de maio de 2017. Disponível em: <https://www.conjur.com.br/2017-mai-30/danilo-doneda-regulacao-criptografia-bloqueio-whatsapp>. Acesso em: 17 de out. 2019.

PLANALTO, Marco Civil da Internet, Lei 12.965 de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm-. Acesso em: 23 de out. 2019.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCHULZ, Wolfgang e VAN HOBOKEN, Joris. Direitos Humanos e Criptografia Publicado em 2016 pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura, 7, place de Fontenoy, 75352 Paris 07 SP, França, traduzido por Instituto de Tecnologia e Sociedade do Rio. Disponível em: http://www.unesco.org/open-access/terms-use-ccbysa-en. Acesso em: 08 de out. 2019.

SCORSIM, Ericson Meister. A questão da criptografia do WhatsApp: julgamento do caso pelo STF sob a perspectiva da segurança das comunicações, 06 de junho de 2017. Disponível em:
https://www.migalhas.com.br/dePeso/16,MI259918,71043-
A+questao+da+criptografia+do+WhatsApp+julgamento+do+caso+pelo+STF+sob-.
Acesso em : 18 de out. 2019.

SILVA, Alexandre Ribeiro da. A Proteção de Dados no Brasil: a tutela do direito à privacidade na sociedade da informação. Juiz de Fora: UFJF, 2017. Disponível em: <https://repositorio.ufjf.br/jspui/handle/ufjf/5374>. Acesso em: 12 out. 2019.

TEIXEIRA, Tarcísio e SABO, Paulo Henrique e SABO, Isabela Cristina,
WhatsApp e a Criptografia Ponto a ponto: tendência jurídica e o conflito privacidade vs. Interesse, Belo Horizonte: UFMG, dezembro de 2017. Acesso em: 27 de out. 2019.