FACULDADE DE DIREITO DE VITÓRIA
GRADUAÇÃO EM DIREITO

FERNANDA VITORIA COUTINHO SARTORI

A IMPLEMENTAÇÃO DA CRIPTOGRAFIA EM POLÍTICAS DE PRIVACIDADE E GOVERNANÇA PARA GARANTIR A PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES COMERCIAIS

VITÓRIA
2024

FERNANDA VITORIA COUTINHO SARTORI

A IMPLEMENTAÇÃO DA CRIPTOGRAFIA EM POLÍTICAS DE PRIVACIDADE E GOVERNANÇA PARA GARANTIR A PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES COMERCIAIS

Trabalho de Conclusão de Curso apresentado na Faculdade de Direito de Vitória, como requisito parcial para a conclusão do Curso de Direito.

Orientador: Prof.: Dr. Bruno Costa Teixeira

VITÓRIA

2024

AGRADECIMENTOS

Primeiramente, gostaria de agradecer a Deus pelas inúmeras oportunidades que me foram concedidas, por me permitir concluir este trabalho com muito foco e persistência.

Ao meu professor orientador, Bruno Costa Teixeira, que além de me transmitir um conhecimento técnico impecável, me deu todo o suporte necessário para que eu elaborasse um texto com as minhas próprias digitais. Serei sempre muito grata.

A minha mãe, Thaís, e ao meu pai, Wallace, agradeço a vocês por não medirem esforços e por me proporcionarem muito mais do que sempre havia sonhado. Espero que este trabalho seja apenas o início de uma caminhada profissional que os deixem muito orgulhosos.

Agradeço também aos meus avós e aos meus padrinhos, por estarem ao meu lado nessa jornada e por sempre torcerem por minhas conquistas.

A minha irmã, Maria Eduarda, e a minha prima, Maria Gabriela, por me trazerem mais leveza nos momentos mais delicados que vivenciei ao confeccionar meu trabalho de conclusão de curso.

Por fim, a minha grande amiga, Fernanda Penina, com quem dividi não só esse momento, mas toda a graduação. Obrigada por ter sido inspiração ao longo dos últimos cinco anos e, principalmente, por ter me transmitido tranquilidade nos momentos mais desafiadores.

A todos vocês, o meu muito obrigada.

RESUMO

Este trabalho tem como objetivo demonstrar como a criptografia pode ser implementada em políticas de privacidade e governança para garantir a proteção de dados pessoais nas relações comerciais. Para alcançar tal finalidade, é abordada a insuficiência do Direito para garantir a eficácia da norma jurídica no plano empírico, bem como a forma pela qual o meta-princípio *privacy by design* e a tecnologia se apresentam como elementos característicos de políticas de privacidade e governança, incentivadas pela Lei Geral de Proteção de Dados - LGPD. Também são demonstradas três possibilidades de implementação da criptografia, destacando a importância de decisões estratégicas no momento de eleger a melhor opção para o negócio desenvolvido, a partir das características de cada uma delas. Por fim, procura-se esclarecer os benefícios para as empresas e organizações que adotam a criptografia sob o ponto de vista econômico.

Palavras-chaves: Criptografia; Proteção de dados pessoais; Políticas de privacidade e governança; Lei Geral de Proteção de Dados - LGPD.

ABSTRACT

The present work aims to demonstrate how encryption can be implemented in privacy and governance policies to ensure the protection of personal data in commercial relations. To achieve this purpose, the insufficiency of the Law to guarantee the effectiveness of legal norms in the empirical sphere is discussed, as well as how the meta-principle of privacy by design and technology are characteristic elements of privacy and governance policies encouraged by the General Data Protection Law (LGPD). Also, are demonstrated three possibilities for implementing encryption, highlighting the importance of a strategic decision when choosing the best option for the business, considering the characteristics of each. Finally, the economic benefits for companies and organizations that adopt encryption are clarified.

Keywords: *Cryptography; Personal data protection; Privacy and governance policies; Brazilian General Data Protection Law.*

SUMÁRIO

APRESENTAÇÃO

O avanço e o desenvolvimento tecnológico ocasionaram importantes mudanças nas formas de organização social. O início da Era Moderna, com a descoberta de novos recursos, bem como sua ampliação em todas as esferas da sociedade, possibilitou o surgimento um novo contexto de fragilidade da privacidade individual, pela massificação de dados e de informações em extensas conexões de rede (MENDES, 2023, p. 14).

Essas mudanças acarretaram novas formas de acesso e de utilização de plataformas de redes sociais, bancos, serviços de transporte, comércio de produtos e mercadorias, entre outros. Diante desse contexto, o convívio em sociedade forçou o indivíduo a fornecer dados e informações pessoais como requisito para o acesso a esses recursos disponíveis (MENDES, 2023, p. 15).

Nesse contexto, a informação se tornou o novo elemento central para o desenvolvimento da economia. A velocidade e o fluxo de informações transmitidas permitiram a construção da chamada "sociedade de informação", em que são observados a desmaterialização e o deslocamento das informações para computadores, *pen drives*, bancos de dados e sistemas de rede (BIONI, 2016, p. 3).

Por sua vez, o acúmulo de informações por parte de empresas e suas plataformas de serviços e aplicações permitiu o avanço de ações publicitárias direcionadas, que acabaram por estabelecer uma relação ainda mais assimétrica entre o consumidor e o fornecedor, em razão da vulnerabilidade dos dados pessoais, podendo inclusive ser disponibilizados a terceiros (BIONI, 2016, p. 17).

A partir dessa perspectiva, aquele que disponibiliza informações pessoais, tanto na condição de consumidor, quanto em uma posição contratual, está sujeito à constante violação de sua privacidade, pela ineficácia dos recursos comumente utilizados no âmbito corporativo, em uma realidade em que os dados se tornaram mercadorias (SARTORI; BAHIA, 2019, p. 226).

Ciente das implicações experimentadas quanto à ausência de proteção de dados pessoais ou, no pior dos contextos, vazamento de dados, os legisladores brasileiros

criaram a Lei Geral de Proteção de Dados (LGPD), Lei número 13.709/2018 que, por sua vez, tem como objetivo "proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo” (BRASIL, 2024, on-line).

A Lei Geral de Proteção de Dados também contempla sanções para aqueles que infringem suas regras, podendo ser aplicadas advertências e multas que podem comprometer significativamente a situação econômica do infrator, além de incentivar políticas de privacidade e governança para garantir o cumprimento de suas disposições (BRASIL, 2018, on-line).

Contudo, é essencial que as empresas e plataformas que realizam tratamento de dados pessoais em seus sistemas, criem novas estratégias para reduzir os riscos, de modo a garantir a segurança digital.

Ante o exposto, questiona-se: como garantir a proteção de dados de modo eficiente, no seio das relações comerciais e empresariais, permitindo aos titulares o livre exercício da autonomia, do controle e do consentimento sobre seus dados pessoais, em perfeita consonância com a Lei Geral de Proteção de Dados - LGPD?

A partir da questão-problema levantada acima, neste trabalho procura-se verificar a hipótese no sentido de que a criptografia pode ser implementada como recurso para garantir a eficácia da norma jurídica, em especial aquelas relacionadas à proteção da privacidade e dos dados pessoais.

O método adequado para este trabalho é o hipotético-dedutivo (POPPER, 2013). Afinal, parte-se de uma questão-problema, "como garantir a proteção de dados pessoais nas relações comerciais" para, a partir dela, verificar uma hipótese no sentido de que: "a criptografia pode funcionar como importante instrumento para a segurança no tratamento de dados pessoais, devendo ser institucionalizada por meio de políticas de governança".

No que tange à insuficiência do Direito para efetivar a norma jurídica, adotou-se a perspectiva do autor Lawrence Lessig, desenvolvida em seu texto intitulado *New Chicago School*. Já em relação à utilização da tecnologia e do princípio *privacy by*

design, nortes em políticas de governança, levou-se em conta as análises contidas na obra "Proteção de Dados Pessoais - A função e os limites do consentimento" de Bruno Ricardo Bioni. Por fim, as abordagens dos autores Diego Machado e Danilo Doneda, no artigo "Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados" foram fundamentais para a compreensão de como a criptografia pode ser implementada no contexto aqui proposto.

Abordou-se, no primeiro capítulo, o caminho percorrido para a consolidação do direito fundamental à proteção de dados pessoais no ordenamento jurídico brasileiro. Já no segundo capítulo, buscou-se demonstrar três dilemas importantes: a insuficiência do Direito para o efetivo cumprimento das normas jurídicas, a importância da tecnologia e do meta-princípio *privacy by design*, além de como são característicos de políticas de privacidade e governança e, por fim, os tipos de criptografia mais utilizados para proteção de dados. O terceiro e último capítulo foi estruturado para verificar a relevância da implementação da criptografia em políticas de privacidade e governança, para a proteção de dados sob o ponto de vista do mercado.

1 DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Antes de adentrar na consolidação do direito fundamental à proteção de dados pessoais, há que abordar em que consistem os dados pessoais, bem como distingui-los das informações pessoais, a partir da análise das características elementares de cada um.

A necessidade de diferenciar os dados pessoais das informações pessoais é visualizada pelo fato de que ambos se sobrepõem em várias circunstâncias da vida cotidiana, pois representam um aspecto da realidade, porém, com peculiaridades específicas (DONEDA, 2011, p. 94).

A primeira distinção está no fato de que as informações pessoais possuem um vínculo objetivo com determinada pessoa. Esse vínculo, por sua vez, revela as ações ou as características atribuídas em conformidade com a lei - como por exemplo, nome e domicílio - ou informações provenientes de seus atos (seu consumo, manifestações, opiniões, outros) (DONEDA, 2011, p. 93).

De igual modo, a Convenção de Strasbourg de 1981 define a informação pessoal como “qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação” (UNIÃO EUROPEIA, 2018). Ou seja, sua caracterização é feita a partir do vínculo (objetivo) existente entre a pessoa e a informação.

Já o dado pessoal, para Raymond Wacks (1989, p. 25), é compreendido como uma informação em estado potencial, de modo que antes de sua transmissão, estaria relacionado com uma "pré-informação".

Para Bioni (2019, p. 54), os dados pessoais "são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação”.

Sob esse viés, enquanto o dado é interpretado de forma mais primitiva e fragmentada, a informação estaria posicionada para além da disposição contida no dado, mas sim no mundo empírico (DONEDA, 2011, p. 94).

Finalmente, a Lei Geral de Proteção de Dados (LGPD), número 13.709/2018, em seu artigo 5º, inciso I, define os dados pessoais como "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018).

Há que mencionar, ainda, a existência de uma outra categoria: os dados pessoais sensíveis que, nos termos do inciso II do mesmo artigo, são definidos como:

> [...]
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> [...]

Os dados pessoais consistem, então, em um conjunto de informações relacionadas a indivíduos identificados ou identificáveis e, que a distinção entre os dados pessoais e os dados pessoais sensíveis é realizada a partir do teor da informação pré-constituída e em função do contexto específico do processo de tratamento.

Outro ponto que merece destaque consiste na valorização da privacidade diante da fomentação da sociedade da informação. Danilo Doneda (2006, p. 14), entende a proteção de dados pessoais como forma de proporcionar ao indivíduo uma esfera privada própria:

> Algo paradoxalmente, a proteção da privacidade na sociedade da informação, tomada na sua forma de proteção de dados pessoais, avança sobre terrenos outrora impropóníveis e nos induz a pensá-la como um elemento que, antes de garantir o isolamento ou a tranqüilidade, serve a proporcionar ao indivíduo os meios necessários à construção e consolidação de uma esfera privada própria, dentro de um paradigma de vida em relação e sob o signo da solidariedade.

A sociedade da informação, potencializada pelo avanço tecnológico e pelo uso constante das redes sociais, culminou em um contexto em que as informações pessoais estão - a todo tempo - sendo disponibilizadas por seus titulares e tratadas por terceiros. E esse novo cenário acarreta o surgimento de um "novo Direito" (DONEDA, 2006, p. 15).

Para o autor, o novo direito mencionado é resultado de uma força expansionista que visa proteger e tutelar os dados pessoais, ressaltando a necessidade de que seja

amplamente visualizado e disseminado como um direito fundamental, a fim de efetivar, justamente, o direito à privacidade individual (DONEDA, 2006, p. 15).

Afinal, nas palavras de Caitlin Sampaio Mulholland (2018, p. 173), "a proteção de dados pessoais enquanto decorrência da cláusula geral de tutela da pessoa humana e do direito à privacidade é um requisito essencial da democracia".

Previamente à Emenda Constitucional número 115, a Constituição Federal de 1988 não fazia qualquer menção à proteção de dados como um direito fundamental autônomo.

Por essa razão, a proteção de dados individuais era visualizada, na realidade, como um direito fundamental implícito (MENDES, 2018). Os esforços para o reconhecimento deste direito se davam a partir da análise do artigo 5º, incisos XII e LXXII, da Constituição da República Federativa do Brasil de 1988 - CRFB/88, uma vez que previam a inviolabilidade do sigilo de correspondências, comunicações telegráficas, telefônicas e de dados, além do direito de interpor *habeas data* (SARLET, 2020, p. 183).

Insta salientar que, embora o direito fundamental à proteção de dados não fosse vislumbrado como um direito autônomo, os legisladores já observavam a necessidade de proteção de dados e o reconheciam como direito fundamental, motivo pelo qual, no ano de 2018, criaram a Lei Geral de Proteção de Dados - LGPD (SOUZA; ACHA, 2022, p. 677).

Apenas com a Emenda Constitucional número 115/2022, o direito à proteção de dados pessoais foi instituído de fato como um direito fundamental. Oportunidade em que também foi constitucionalizada a competência restritiva da União para legislar sobre dados pessoais e sua responsabilidade quanto à organização, fiscalização, proteção e tratamento (SOUZA; ACHA, 2022, p. 679).

Contudo, por força da Emenda Constitucional número 155/2022, o inciso LXXIX foi adicionado ao rol do artigo 5º da Constituição Federal, dispondo que: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

A partir do momento em que passou a compor o rol do artigo 5º, cessou o esforço doutrinário para considerar a proteção de dados como direito fundamental autônomo constitucionalizado, conforme pontuam Nicole Betta de Souza e Fernanda Rosa Acha (2022, p. 679):

> Apesar de a matéria já possuir regulação infraconstitucional há algum tempo, considerando a relevância do tema, o constituinte derivado achou pertinente a inclusão da proteção de dados de modo explícito na Carta Magna, passando-se a ter uma normatização completa, aumentando sua proteção jurídica e esvaindo qualquer debate a respeito do seu reconhecimento ou não como direito fundamental.

Dessa forma, não se encontram dificuldades ou obstáculos para alcançar a seguinte premissa: a proteção de dados individuais é um direito fundamental e, por essa razão, deve ser conhecida, obedecida e implementada por todos (PEDRA, 2012, p. 222), carecendo de tratamentos adequados e eficazes para seu gerenciamento, com base nas disposições previstas em sua lei regulamentadora, devendo o mundo corporativo adequar-se as suas diretrizes.

2 A INTERSECÇÃO ENTRE DIREITO, PRIVACIDADE E CRIPTOGRAFIA

2.1 A INSUFICIÊNCIA DO DIREITO PARA ASSEGURAR O CUMPRIMENTO DA NORMA JURÍDICA A PARTIR DA ANÁLISE DAS FORÇAS REGULATÓRIAS PROPOSTAS POR LAWRENCE LESSIG

Superado o reconhecimento constitucional quanto à proteção de dados pessoais, há que se demonstrar como o Direito, por si só, se apresenta insuficiente para efetivar normas, valores e princípios presentes em um ordenamento jurídico. Para legitimar tal premissa, serão analisados os estudos do autor norte americano Lawrence Lessig, referência acadêmica em assuntos que versam sobre a regulação da internet (COLNAGO, 2016, p. 18).

Seu trabalho desenvolvido no *New Chicago School* busca compreender o comportamento dos seres humanos, inclusive sob o prisma individual, a partir das "forças" restritivas e incidentes no ordenamento jurídico, sendo elas: o Direito, as Normas Sociais, o Mercado e a Arquitetura (COLNAGO, 2016, p. 20).

O Direito (*Law*), primeira força regulamentadora proposta por Lessig, é visualizado a partir do exercício do monopólio estatal que, por sua vez, restringe o comportamento humano a partir da aplicação de sanções (COLNAGO, 2016, p. 25).

O autor também compreende que o Direito, por si só, não consegue efetivar os valores jurídicos que tem como objetivo e, por essa insuficiência, nasce a necessidade de viabilizar a incidência das demais forças reguladoras, conforme pode-se visualizar:

> As ameaças aos valores implícitos no Direito – ameaças decorrentes de mudanças na Arquitetura em código – são somente exemplos específicos de uma questão geral maior: a de que além do Direito, outros fatores também viabilizam valores jurídicos, e o Direito sozinho não consegue garanti-los. Se nosso objetivo é um mundo constituído por esses valores, então são esses outros reguladores – código, mas também costumes e o Mercado – que devem ser abordados. O Ciberespaço torna claro não somente como essa interação ocorre, mas também a urgência em compreender como influenciá-la (LESSIG, 1999b, p. 546).

Além disso, o Direito não se encontra em sincronia com os acontecimentos da sociedade globalizada, tornando o paradigma jurídico moderno insuficiente para atender todas as contingências sociais (MOREIRA, 2007, p.179).

Enquanto as normas jurídicas são positivadas pelo Direito, as Normas Sociais - segunda força regulamentadora - são constituídas pelos costumes enraizados de acordo com a cultura de cada localidade (LESSIG, 1998a, p. 673). Dessa forma, as normas sociais servirão como balizas do comportamento para pessoas socialmente integradas (LEONARDI, 2012, p. 160).

Mayer-Schoenberger (2008, p. 716), professor de governança e regulamentação da internet na Universidade de Oxford, desenvolveu os estudos de Lessig no sentido de que as normas sociais variam de cultura para cultura, mas que todas possuem comportamentos que são e não são aceitos, sendo este um ponto em comum entre todas elas.

Por outro lado, o Mercado - terceira força regulamentadora prevista pelo autor - segue a lógica básica do preço em decorrência da escassez (COLNAGO, 2016, p. 27). Para Lessig (1998a, p. 673), o Mercado não deve atuar de forma totalmente autônoma e deliberada, sobre ele, devem incidir limites que impeçam a conversão de uma sociedade de pessoas para uma sociedade de mercado.

As constantes intervenções do poder público no âmbito mercadológico influenciam diretamente no comportamento das pessoas, ainda que possam impedir o fluxo natural da economia. Um exemplo prático dessa força é a extrafiscalidade existente em alguns tributos, ou até mesmo a existência de políticas públicas que visam aumentar ou reduzir certos tipos de comportamentos, por vezes enraizados culturalmente em uma sociedade (COLNAGO, 2016, p. 30).

A última força regulamentadora prevista por Lessig é a Arquitetura, isto é, a forma "pela qual os objetos do mundo são apresentados aos sentidos humanos, compreendendo não somente as criações naturais, como também as artificiais" (CONALGO, 2016, p. 31).

Lawrence Lessig (1998a, p. 663) entende que a própria infraestrutura de uma região pode atuar de forma restritiva no comportamento humano, uma vez que pode influenciar no tempo para chegar em determinados lugares, ou até mesmo impossibilitar a circulação de pessoas entre dois espaços pela presença de grandes obstáculos.

Ainda que a força da Arquitetura seja mais palpável ao senso humano no que tange à construções civis e a urbanização, Lessig ampliou seus estudos sobre as forças regulatórias, especialmente incidentes no ambiente digital.

Ainda que já reconhecido o fato de que os desenvolvedores controlam toda a arquitetura da rede (SCHEWIK, 2010, pp. 293;313), Lawrence Lessig visualizava que a internet, na sua forma original, permitia a liberdade perfeita, por ser um lugar irregulável. Em suas palavras:

> Comportamentos, se controlados, eram regidos por costumes da rede. O arquiteto impediu qualquer controle além disso. Por quê? A [...] irregulabilidade da rede original se baseava numa funcionalidade daquela rede. A identidade, a localização, não eram auto- autenticáveis. Eu descrevi como o fato de ser uma criança não é auto-autenticável. Isso significa que é relativamente difícil rastrear quem é determinada pessoa; o que significa que é relativamente difícil regular como as pessoas se comportam (LESSIG, 2000, p. 9).

Atribui-se essa característica irregulável exclusivamente à arquitetura construída para as redes à época. No entanto, três princípios foram considerados fundamentais para a configuração da internet nos moldes atuais, sendo eles, em livre tradução: o princípio ponta a ponta, código aberto e acesso livre (COLNAGO, 2016, p. 39).

O princípio ponta-a-ponta, defendido pelo autor, é concebido como um facilitador de trocas de informações e dados entre os usuários, impossibilitando que em seu curso sofra qualquer discriminação pela rede (LESSIG, 2000b, p. 10).

Já o código aberto, nas palavras de Sérgio Amadeu (2004, p.12), significa uma espécie de "modelo colaborativo que envolve programadores da empresa e todos

aqueles interessados no desenvolvimento daquele software, inclusive voluntários espalhados pelo mundo".

A facilidade de compartilhamento disponibilizada por esse princípio guarda forte relação com o princípio do "acesso livre" que, por sua vez, garante que a informação publicada seja gratuita para todos os usuários (LESSIG, 2000b, p. 12).

No entanto, se a rede - em sua forma original - era irregulável pela arquitetura utilizada pelos programadores e desenvolvedores no período em que teve início, é plenamente possível que sejam construídas novas arquiteturas voltadas para a proteção de direitos e garantias fundamentais, já que a evolução do comércio acarretou o surgimento de novas camadas de código (COLNAGO, 2016, p. 42).

As alterações ocorridas no espaço virtual, culminaram na existência de um contexto inovador, em que foram deslocados os valores consagrados pelo Direito para os desenvolvedores e programadores no ato de construção de seus códigos, permitindo e garantindo a sobrevivência das premissas contidas no ordenamento jurídico (LESSIG, 1999b, p. 541).

E a partir dessa dinâmica de intersecção entre os códigos jurídicos e os códigos de programação, Cláudio Colnago (2016, p. 46) concluiu:

> Daí se fazer necessário, como proposto alhures, “[...] o estudos interdisciplinar das intersecções possíveis entre Direito e tecnologia, entre os códigos jurídicos e os códigos de programação” (COLNAGO, 2013a, p. 160), de forma a viabilizar a influência dos direitos fundamentais na formatação do código enquanto Arquitetura, numa abordagem multidisciplinar que rejeite soluções unilaterais, numa busca por soluções equilibradas entre direitos fundamentais e eficiência/sustentabilidade econômica (BROWN, MARSDEN, 2013, p. 160).

Inclusive, Lessig (2006, p. 79) afirma: "os programadores são cada vez mais legisladores. Eles determinam quais os padrões que a Internet seguirá; se a privacidade será ou não protegida; o grau de anonimato permitido".

Destaca-se, ainda, os ensinamentos de John Greenleaf (1998, p. 13), quando alega que "somente uns poucos aspectos do ciberespaço, como os aspectos de biologia humana com os quais interage, são impenetráveis ao Direito".

Diante desse contexto, verifica-se a grande relevância das forças regulatórias de Lessig, em especial a força da Arquitetura, para cumprir as diretrizes e imposições do ordenamento jurídico, especialmente no que tange ao espaço digital, pelas possibilidades inerentes à atividade dos programadores e desenvolvedores por meio da conexão de códigos.

2.2 A UTILIZAÇÃO DE TECNOLOGIAS FUNDADAS NO META-PRINCÍPIO DO *PRIVACY BY DESIGN* COMO FORMA DE EFETIVAR POLÍTICAS DE PRIVACIDADE E GOVERNANÇA

Partindo do pressuposto que os recursos tecnológicos têm a potência de proteger direitos da personalidade, muitas vezes com mais eficiência do que a legislação, conforme debruçado no tópico anterior, há que se demonstrar como a tecnologia, em especial a criptografia, pode ser utilizada como política de governança prevista na Lei Geral de Proteção de Dados - LGPD (Lei número 13.709/2018).

Para isso, serão abordados alguns dos estudos de Bruno Ricardo Bioni, autor brasileiro e especialista em proteção e privacidade de dados, principalmente aqueles consolidados em sua obra "Proteção de Dados Pessoais - A função e os limites do consentimento".

Para o autor, os modelos de negócios, principalmente aqueles com maior foco na publicidade direcionada, consolidam uma estrutura industrial voltada ao tráfego de informações para elaboração de perfis precisos de potenciais consumidores para adesão de determinados produtos ou serviços (BIONI, 2019, p.141).

Ainda que esse comportamento ocorra de forma reiterada por muitas empresas, existe um aparente descaso normativo quanto à forma de operacionalização da manifestação de consentimento, razão pela qual o mercado se autorregulou, fazendo surgir as políticas de privacidade, com a finalidade de legitimar qualquer tratamento de dados pessoais (BIONI, 2019, p. 166).

Paralelamente ao surgimento das políticas de privacidade, nasceu também o meta-princípio *privacy by design (privacidade desde a concepção),* pensado originalmente nos anos 1990, pela autora canadense Ann Cavoukian (2010, on-line).

Bruno Bioni (2016, p. 171) define o meta-princípio *privacy by design* como a "ideia de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviços" e ainda atribui o dever de que a proteção seja acompanhada por tecnologias de controle.

Isso significa que a privacidade deve ser arquitetada desde a sua concepção, ou seja, todo projeto deve ser desenvolvido pensando na proteção de dados em todas as suas fases, inclusive iniciais.

O autor propõe a utilização das *Privacy Enhancing Technologies (PETs),* em tradução literal, tecnologias que reforçam ou melhoram a privacidade. As PETs abarcam, em suas palavras, "toda e qualquer tecnologia que seja amigável e facilitadora à privacidade" (BIONI, 2019, p. 171), sendo concebidas pelo próprio princípio *privacy by design*.

E ainda pondera:

> Veja-se, por exemplo, a criptografia que assegura a confidencialidade das comunicações. Ou, ainda, a anonimização dos dados pessoais que quebra ou pelo menos dificulta o vínculo de identificação entre um dado e o sujeito ao qual ele está atrelado (subcapítulo 2.2.2), bem como mecanismos de navegação anônima que impedem o rastreamento do usuário. Em todos esses exemplos, a arquitetura dos sistemas de informação é um instrumento hábil para proteger os dados pessoais do cidadão.

Assim, Bioni (2019, p. 171) observa viabilidade em tais tecnologias - como a criptografia e a anonimização - por garantirem que os titulares poderão reaver o controle de seus dados e, consequentemente, exercer livremente o consentimento, permitindo que desempenhem um papel multifacetado e emancipador no processo de captação e mineração de dados pessoais.

Em sua perspectiva, trata-se de uma projeção de ambientes, afinal, o titular deve ser reconhecido como sujeito vulnerável inserido em uma arquitetura de vulnerabilidade. Apenas com a transformação da arquitetura de rede, de modo a permitir o exercício do livre consentimento e controle de dados é que de fato o drama da proteção de dados será superado (BIONI, 2019, p. 199).

Ao propor uma arquitetura permissiva e favorável ao titular, os estudos de Bruno Bioni guardam íntima relação com os pensamentos de Lawrence Lessig, uma vez que ambos reconhecem que o código é o recurso mais atrativo para efetivar uma norma jurídica dentro de uma perspectiva arquitetônica.

Diante da ausência de uma rígida legislação preventiva, a adoção de tecnologia pelos programadores e desenvolvedores - em conformidade com o meta princípio ora analisado - e, mais especificamente, o uso da criptografia como forma de assegurar a confidencialidade dos dados, em nada mais consiste do que a utilização de uma política de privacidade segura e eficiente.

E políticas de privacidade são, inclusive, permitidas e incentivadas pela Lei Geral de Proteção de Dados. A Seção II da Lei número 13.709/2018, intitulada como "Das boas práticas e da governança", permite que os agentes de tratamento formulem regras, criem padrões, estabeleçam procedimentos e regimes de processamento de dados que mitiguem riscos de vazamento, levando em consideração as especificidades dos dados coletados, é o que dispõe o artigo 50 e seu parágrafo 1º:

> [...]
>
> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
>
> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

[...]

Para nortear a implementação de políticas de governança para proteção de dados individuais, o Ministério da Gestão e da Inovação em Serviços Públicos, em parceria com outros órgãos do governo, confeccionou e disponibilizou um guia descrevendo o passo a passo para elaboração de programas de privacidade e segurança da informação (PPSI) (BRASIL, 2024).

A instalação do programa foi dividida em três etapas: 1) Iniciação e Planejamento; 2) Construção e Execução e 3) Monitoramento. A fase de iniciação e planejamento contempla várias subdivisões, como por exemplo, indicação do encarregado, alinhamento com as expectativas da administração, criação de uma estrutura organizacional e de inventário contendo dados pessoais (BRASIL, 2024).

Por outro lado, a fase de construção e execução vincula-se aos procedimentos de elaboração de políticas e práticas para proteção da privacidade, análises de viabilidade de cultura e segurança de dados, além da confecção de relatórios e adequações de cláusulas contratuais (BRASIL, 2024).

Por fim, o monitoramento, última etapa de implementação, busca a análise dos resultados obtidos e a observação contínua sobre a conformidade com a LGPD. Extrai-se que, em todas as fases e suas ramificações, estão presentes diferentes tecnologias e inteligências para o aperfeiçoamento de gestão e resultados (BRASIL, 2024).

De modo conclusivo, reforçam a importância que a disponibilização de dados seja clara, eficiente e acessível (BRASIL, 2024). Destaca-se que, conforme exposto no guia, a "capacitação e treinamento devem ser oferecidos para que uma cultura de Privacidade desde a Concepção (*privacy by design*) seja instituída".

Tal cenário apresentado permite concluir de modo cristalino que a tecnologia adequada ao *privacy by design* é quase uma característica intrínseca de programas de governança e privacidade, podendo e devendo ser implementada, de modo a facilitar o acesso, controle e, principalmente, a segurança de dados.

2.3 O *DESIGN* DA IMPLEMENTAÇÃO DA CRIPTOGRAFIA PELOS AGENTES DE TRATAMENTOS NA PERSPECTIVA DE DIEGO MACHADO E DANILO DONEDA

Finalmente, neste tópico busca-se demonstrar como de fato a criptografia pode ser implementada garantindo a autonomia, o consentimento e o controle do titular. As possibilidades que serão demonstradas foram extraídas da obra "Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados" de autoria de Diego Machado e Danilo Doneda (2018), não descartando, claro, a contribuição da legislação e de outros autores para melhor abordagem da temática sob análise.

O artigo 5º da Lei Geral de Proteção de Dados - LGPD prevê conceitos importantes no que tange a proteção e o tratamento de dados e, dentre eles, há que destacar os incisos VI, VII e VIII, IX, os quais dispõem que:

> [...]
>
> Art. 5º Para os fins desta Lei, considera-se:
>
> [...]
>
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX - agentes de tratamento: o controlador e o operador;
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
>
> [...]

Foram então criadas três figuras importantes que serão responsáveis pela adequação do tratamento, sendo eles: o controlador, a quem compete a tomada de decisões, o operador que realiza o tratamento de dados em nome do controlador e, por fim, o encarregado que atuará como uma via de comunicação entre o controlador e o titular do dado. O controlador e o operador são chamados de agentes de tratamento.

Em contrapartida, o termo tratamento diz respeito às operações nas quais os agentes terão que lidar diretamente com os dados pessoais sob sua responsabilidade. Esses conceitos são de suma importância para viabilizar a implementação de tecnologias no procedimento de coleta, armazenagem, distribuição, controle e outros.

A importância da criptografia vem sendo amplamente reconhecida, tendo em vista que, para muitos, já é considerada "parte do mundo dos negócios e da rotina das pessoas" (TOTVS, 2024), além de ser implementada em diversas políticas públicas do governo brasileiro (DONEDA; MACHADO, 2018, p. 114).

A criptografia consiste na ciência que tem como finalidade esconder o significado de determinadas mensagens, garantindo a confidencialidade da informação submetida à cifragem (DONEDA; MACHADO, 2018, p. 101). Esse processo transforma um texto simples em uma cifra por meio de algoritmos matemáticos, tornando o conteúdo acessível apenas por meio das “chaves" (TOTVS, 2024).

Muitas técnicas de criptografia podem ser implementadas diante de um objetivo claro de proteção de informações. No entanto, a criptografia ponta a ponta, abordada pelos autores Danilo Doneda e Diego Machado (2018, p. 114), é o modelo mais utilizado para garantir a proteção de dados pessoais.

Para os autores, a criptografia ponta a ponta busca "reduzir a ameaça de pontos intermediários ou ataques internos que operam o serviço e desfrutam de acesso privilegiado", buscando alcançar a confidencialidade para além do acesso de estranhos, mas também em relação aos próprios agentes (DONEDA; MACHADO, 2018, p. 115). Contudo, a predileção pela criptografia ponta a ponta não descarta a possibilidade da sua implementação de outras formas.

Considerando-se que a informação trafega de um computador a outro, a criptografia é pensada também sobre dois aspectos: a criptografia em trânsito (*encryption in transit*) e a criptografia em repouso *(encryption at rest)* (DONEDA; MACHADO, 2018, p. 117). Ambas precisam ser implementadas conjuntamente para afastar qualquer possibilidade de violações.

A criptografia em repouso consiste na cifragem de informações que já estão armazenadas em determinado servidor, computador, HD, *pen drive* e outros (DONEDA; MACHADO, 2018, p. 117). Ainda, para os autores, a criptografia em repouso pode se dar sob duas perspectivas, tanto pelo usuário *(client side)* quanto do servidor *(server side encyption)* (2018, p. 117).

Sob o prisma do usuário, a criptografia estará presente exclusivamente no local de sua posse em que o dado estará armazenado, enquanto na criptografia sob o prisma do servidor, a cifragem ocorra de forma remota, estando presente em servidores em localidade diversas, como ocorre nas redes de internet (DONEDA; MACHADO, 2018, p. 117).

Há que destacar, ainda, que a utilização da criptografia pelos servidores não descarta a possibilidade que o usuário se resguarde de qualquer potencial violação, cifrando seus dados pessoais antes de disponibilizá-lo ao servidor (DONEDA; MACHADO, 2018, p. 117).

Tecidos esses esclarecimentos, os autores concluem que a criptografia de dados pessoais poderia ser realizada em três formatos distintos, sendo eles:

> [...] (i) comunicação intermediada por provedor de aplicação de internet, em que o teor das mensagens e dados só pode ser acessado pelo(s) usuário(s) que possui(em) a chave criptográfica pertinente; (ii) dados de usuários armazenados e procesados em servidores ou bases de dados de ente responsável, ou terceiro a ele interligado, encriptados por iniciativa ou determinação do próprio provedor de serviço, que pode acessar a chave de decriptação; e (iii) informações cifradas por ato do usuário e armazenadas e processadas em servidores ou bases de dados de provedor de serviço de computação em nuvem, o qual não tem acesso à correspondente chave criptográfica (2018, p. 118).

A comunicação intermediada por provedor de aplicação de internet, primeira situação descrita, trata da cifragem no âmbito do sigilo das comunicações (DONEDA; MACHADO, 2018, p. 118). Esta hipótese retrata o caso da cifragem da informação, em que apenas os interlocutores teriam as chaves duplas para decriptar e acessar seu teor.

Para Frederico Meinberg Ceroy (2014, on-line), presidente do Instituto Brasileiro de Direito Digital[1], provedor de internet "é um termo que descreve qualquer empresa, organização ou grupo que forneça um conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet".

Ainda que qualquer empresa possa ser considerada provedora de internet, essa técnica demonstra-se mais interessante para aquelas que estão inseridas em um contexto de comunicação, tendo em vista que apenas os interlocutores terão acesso ao conteúdo das mensagens, dispensando a necessidade dos agentes de tratamento para assegurar a inexistência de violações aos direitos da personalidade.

Um perfeito exemplo desse tipo de criptografia é visualizado cotidianamente pelos usuários do aplicativo *WhatsApp*[2]*.* No ano de 2016, a plataforma adotou a criptografia ponta a ponta para garantir a segurança da comunicação de seus usuários, sendo criptografadas mensagens, áudios, fotos e vídeos (WHATSAPP, 2024, on-line).

A segunda hipótese prevista pelos autores é a possibilidade de que os dados armazenados em servidores ou bases de dados sejam encriptados e decriptados pelo próprio provedor de serviço. Isso significa que, por iniciativa do provedor, o dado será cifrado, possuindo autonomia para acessá-los quando conveniente.

Ou seja, nesse caso, ocorrerá a criptografia em repouso, ficando a critério do controlador e do operador a adoção da técnica como medida de segurança (DONEDA; MACHADO, 2018, p. 118).

A última situação retratada pelos autores ocorrerá quando o usuário, por sua iniciativa, fornecer o dado já encriptado para os servidores. Antes da informação chegar para o tratamento de dados pelo provedor, a informação já estará cifrada, motivo pelo qual os agentes de tratamento não terão acesso ao teor do dado disponibilizado (DONEDA; MACHADO, 2018, p. 118).

---

[1] Disponível em: https://jus.com.br/artigos/31938. Acesso em: 10 out. 2024.

[2] Disponível em: https://whatsapp.com. Acesso em: 03 out. 2024.

Dessa forma, a distinção entre as hipóteses estabelecidas é se o provedor terá ou não acesso às chaves para decriptar a informação/dado que armazena (SPINDLER; SCHMECHEL, 2016, p. 171).

Tendo em vista que a última das hipóteses mencionadas prevê o desconhecimento do teor do dado disponibilizado pelo provedor, surgiram muitos questionamentos se essa metodologia se confundiria com a anonimização de dados e, por essa razão, esse pensamento deve ser desmistificado.

Os autores compreendem que a partir da força e da extensão do algoritmo de cifragem, juntamente com a segurança do gerenciamento de chaves, a criptografia impossibilita que a cifra seja vinculada a um indivíduo específico, impossibilitando uma interpretação equivocada de que, na prática, ocorreria uma anonimização.

Mesmo que a criptografia seja segura, o controlador não se encontra desonerado de atuar buscando maiores níveis de segurança (DONEDA; MACHADO, 2018, p. 121).

A implementação das hipóteses mencionadas no mundo corporativo irá depender do tipo de atividade desenvolvida e a forma como ela se desenvolve, tendo em vista que alguns modelos poderão ser melhores que outros para garantir a segurança em casos específicos.

Nessa perspectiva, as políticas de privacidade e governança são imprescindíveis, uma vez que a elaboração do *design,* de forma prévia à implementação da estratégia eleita para o contexto delimitado, permitirá o alcance de uma segurança digital muito mais eficaz.

3 OS ATRATIVOS DA IMPLEMENTAÇÃO DE MEDIDAS EFICAZES PARA A PROTEÇÃO DE DADOS PESSOAIS SOB O PONTO DE VISTA DO MERCADO

Superadas as questões quanto à relevância e às possibilidades oriundas da criptografia, deve-se demonstrar os atrativos da sua implementação sob o ponto de vista do mercado, uma vez que as empresas e organizações precisam visualizar de forma concreta os impactos de determinadas estratégias nos contextos em que estão inseridas a partir da análise de casos relevantes.

Antes das eleições de 2016, a *Cambridge Analytica*, empresa de análise de dados e consultoria política, estava auxiliando membros responsáveis pela campanha do candidato Donald Trump nos Estados Unidos. Com a intenção de traçar perfis de potenciais candidatos e estratégias de campanha, a empresa disponibilizou um aplicativo de teste na plataforma do *Facebook*[3], conhecido como *"This is your digital life"* (essa é sua vida digital), impulsionando milhares de usuários a fazer o teste disponibilizado (NEWS, 2018, on-line*).*

Além da plataforma obter os dados informados, também foram coletados dados dos amigos dos usuários que realizaram a pesquisa, totalizando uma coleta de dados de aproximadamente 87 milhões de usuários em todo o mundo (BRASIL, 2022). Os dados incluíam informações sobre a identidade (nome, profissão e endereço), suas preferências, hábitos e suas redes de contatos (NEWS, 2018, on-line*)*.

O caso somente veio a público porque um dos analistas responsáveis pela implementação do projeto, Christopher Wylie, revelou um dossiê contendo evidências robustas sobre a utilização dos dados coletados para auxiliar a candidatura de Donald Trump (NEWS, 2018, on-line*).*

A coleta, a utilização e comercialização foram fatores determinantes para que o *Federal Trade Comission* (FTC) condenasse o *Facebook* a pagar uma multa de U$5 bilhões de dólares pelas violações cometidas (CANALTECH, 2019, *online*). A plataforma também foi multada em R$ 6,6 milhões de reais pela Secretaria Nacional

[3] Disponível em: www.facebook.com. Acesso em: 03 out. 2024.

do Consumidor (Senacon) pelos dados dos brasileiros que foram violados (BRASIL, 2022).

A repercussão do caso reduziu consideravelmente a credibilidade de ambas as empresas, refletindo cristalinamente na redução de aproximadamente U$35 bilhões de dólares do valor comercial da rede social na bolsa de valores dos Estados Unidos em apenas dois dias após a publicidade do ocorrido (NEWS, 2018, on-line*)*.

Outro caso de grande impacto foram os vazamentos de dados pela rede de hotelaria *Marriott International.* Após uma investigação, foi identificada a ocorrência de um acesso não autorizado que copiou e criptografou dados pessoais de clientes da *Starwoods*, cadeias de hotéis que operam com as bandeiras *W Hotels, Sheraton, Le Méridien* e *Four Points*, localizados por todo o mundo (GLOBO, 2018, *online).*

Aproximadamente 500 milhões de usuários tiveram seus dados violados e, segundo a própria *Marriott*, os dados de aproximadamente 327 milhões de hóspedes guardam semelhança entre eles (GLOBO, 2018, *online)*. A situação se alarmou pelo fato de que boa parte dos dados eram nomes, endereços, número de passaporte e cartões de crédito, além de datas de *check-in* e *check-out* no hotel (GUARDIAN, 2018, on-line*).*

Em razão da violação ao Regulamento de Proteção de Dados da União Europeia (GDPR) a *Information Commissioner's Office,* autoridade de proteção de dados no Reino Unido, aplicou uma multa de £14,4 milhões de libras pagas pela rede *Marriott* (VISEU, 2020, on-line)*.*

A ocorrência de situações semelhantes sensibiliza consideravelmente a relação de confiabilidade entre o cliente e a empresa, tendo em vista que os dados acessados por terceiros colocam os titulares em uma situação de vulnerabilidade e insegurança em todas as suas dimensões, especialmente no âmbito pessoal, privado e digital.

Afinal, uma pesquisa realizada pela PwC (*PricewaterhouseCoopers*), empresa prestadora de serviços de consultoria e auditoria, confirmou que para 90% dos

consumidores brasileiros a proteção de dados pessoais é um dos fatores mais importantes para que as empresas conquistem sua confiança (PWC, 2024, on-line).

Ainda que ambos os casos retratados tenham ocorrido fora do país, o Brasil ocupa o 6º lugar no ranking internacional de países que mais sofrem com vazamento de dados pessoais, contabilizando aproximadamente 24,2 milhões de perfis que tiveram informações vazadas, seja por ataques cibernéticos ou por brechas em sistemas apenas no ano de 2021 (ISTO É, 2021, *online*).

A ausência de uma política de privacidade robusta em navegadores, sites, plataformas e redes acaba proporcionando um cenário de insegurança digital e, por essa razão, as empresas que se preocupam em implementar políticas de privacidade ocupam uma posição diferenciada em relação aos seus concorrentes.

Fora que, o impacto econômico de um vazamento de dados pode comprometer significativamente a saúde financeira da empresa. O IBM (*International Business Machines Corporation*), empresa voltada para o mercado de informática, divulgou que, no ano de 2023, o custo médio global de uma violação de dados foi de U$ 4,45 milhões de dólares (IBM, 2023, on-line).

Ao desfocar da análise sobre a relação empresa-consumidor, há também que demonstrar os desdobramentos da proteção de dados no âmbito das relações entre as próprias empresas e organizações, como aconteceu com a *Global Payments.*

No ano de 2012, a empresa americana prestadora de serviços financeiros, *Global Payments,* foi retirada da relação de provedores seguros fornecida pela Visa - multinacional de serviços financeiros - em razão de uma invasão que supostamente teria afetado 1,5 milhões de cartões de crédito emitidos pela instituição financeira (GLOBO, 2012, on-line).

Fica evidente, portanto, que o contexto de violações de dados pessoais, além de afetar a reputação da marca, também pode acarretar a suspensão ou até mesmo no

encerramento de negócios, já que inexistem vantagens para a manutenção de parcerias comerciais que poderiam descredibilizar uma das partes.

Ainda que os benefícios e a necessidade de adequação pareçam ser óbvios, segundo a pesquisa realizada pelo Grupo Daryus no ano de 2022, cerca de 80% das empresas ainda não se adequaram às diretrizes da Lei Geral de Proteção de Dados (CANALTECH, 2022, on-line).

Esse fato se dá pela existência de uma legislação mais permissiva e menos rígida quanto à obrigatoriedade de adoção de medidas preventivas para proteção de dados pessoais, instaurando uma realidade em que a preocupação com dados pessoais seja optativa para aqueles que os coletam e armazenam.

Diante do crescimento exponencial do uso da tecnologia somado ao contexto de descaso presente por boa parte das empresas brasileiras, o deputado Amom Mandel apresentou o Projeto de Lei número 2.517/2024, cuja finalidade é estabelecer novas diretrizes para a proteção de dados pessoais no meio digital, reforçando as previsões atinentes à Lei Geral de Proteção de Dados. O projeto ainda precisa ser aprovado pela Câmara e pelo Senado (BRASIL, 2024).

Tal cenário apresentado permite concluir que a preocupação com a adoção de políticas de privacidade e governança eficazes podem gerar grande impacto em um mundo corporativo. A reputação, a credibilidade e a construção de relações de confiança são fatores determinantes para o reconhecimento de um diferencial em meio a constantes violações de dados pessoais, além de evitar penalidades financeiras significativas.

CONSIDERAÇÕES FINAIS

O principal objetivo deste trabalho foi abordar como a criptografia pode ser implementada nas relações comerciais para garantir a proteção de dados pessoais, possibilitando o exercício de maior controle pelos titulares e demonstrando sua importância sob o ponto de vista econômico.

Para alcançar tal premissa, foram abordados os pensamentos do autor Lawrence Lessig desenvolvidos no *New Chicago School.* Ao propor a existência de quatro forças regulatórias - o Direito, as Normas Sociais, o Mercado e a Arquitetura - incidentes sobre o comportamento humano, posicionou a força da Arquitetura de forma privilegiada no que cerne à efetivação da norma jurídica, reconhecendo que o Direito, por si só,é insuficiente para garantir o cumprimento de suas próprias premissas.

Partindo do pressuposto que o Direito carece de outros recursos para permitir a eficácia de suas diretrizes, foi demonstrado como as tecnologias e, especialmente, a criptografia surgem para suprir essa necessidade, devendo ser implementadas e arquitetadas em políticas de privacidade e governança instituídas com base no meta princípio *privacy by design* o que é, inclusive, objeto de incentivo da Lei Geral de Proteção de Dados - LGPD.

Em seguida, foi apresentado o conceito de criptografia e narrada suas possibilidades, destacando quais os melhores métodos para atender determinadas finalidades e atividades desempenhadas por empresas e organizações. Dentre elas, foram destacadas três formas de utilização da criptografia, ocorrendo quando: i) apenas os interlocutores possuem as chaves para acessar e decriptar o teor da informação, ficando o provedor de internet limitado a função de intermediador; ii) o próprio provedor do serviço faz a encriptação do dado; e iii) o titular já disponibiliza seus dados criptografados.

Realizadas tais intersecções, foram elencados dados e casos relevantes como o da *Cambridge Analytica* e a *Marriott International,* com a finalidade de demonstrar os impactos dos vazamentos de dados no ponto de vista do mercado, especialmente no

que tange à descredibilidade e à ruptura de relações de confiança entre clientes, usuários e/ou consumidores. Destacou-se também o caso da *Global Payments* de modo a constatar que ausência de políticas de privacidade robustas podem acarretar a suspensão de contratos e encerramento de parcerias e negócios.

Foram apresentadas estatísticas que comprovam que muitas empresas brasileiras ainda não se adequaram as diretrizes previstas na Lei Geral de Proteção de Dados - LGPD e que, em resposta a esse cenário, tramita o Projeto de Lei número 2.517/2024, para enrijecer as diretrizes para proteção de dados no ciberespaço, de forma a equilibrar a legislação com o avanço tecnológico.

Todas as abordagens elaboradas foram idealizadas para permitir o alcance da seguinte premissa: a problemática da proteção de dados somente será superada com a adoção de tecnologia para garantir a eficácia da norma jurídica e, no presente caso, que a criptografia pode ser implementada como técnica eficiente nas relações comerciais, incluindo os titulares nos processos de tratamento e assumindo um papel diferenciado e inovador na perspectiva de mercado.

REFERÊNCIAS

BBC. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 07 out. 2024

BIONI, Bruno. **Proteção de dados pessoais:** a função e os limites do consentimento. Cidade: Forense, 2019.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**.
_____. **Guia de Programa de Governança de Privacidade. Brasília**, DF: Governo Digital, 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_programa_governanca_privacidade.pdf. Acesso em: 07 out. 2024.
_____. **Lei no 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei no 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República; 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 05 jun. 2024.
_____. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Facebook é condenado a pagar R$ 6,6 mi por vazar dados de usuários**. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/facebook-e-condenado-a-pagar-r-6-6-mi-por-vazar-dados-de-usuarios#:~:text=dados%20de%20usuários-,Facebook%20é%20condenado%20a%20pagar%20R%24%206%2C6%20mi,por%20vazar%20dados%20de%20usuários&text=Bras%C3%ADlia%2C%2023%2F08%2F2022,de%20dados%20de%20usuários%20brasileiros. Acesso em: 07 out. 2024
_____. MINISTÉRIO DO ESPORTE. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd.
_____. **Projeto de Lei nº 2.517/2024**. Estabelece diretrizes para a proteção da privacidade dos cidadãos em meio virtual, reforçando a Lei Geral de Proteção de Dados Pessoais (LGPD) e ampliando as competências da Autoridade Nacional de Proteção de Dados (ANPD). Brasília: Câmara dos Deputados, 2024. Disponivel em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2442707#:~:text=PL%202517%2F2024%20Inteiro%20teor,Projeto%20de%20Lei&text=Estabelece%20diretrizes%20para%20a%20proteção,Proteção%20de%20Dados%20(ANPD). Acesso em: 07 out. 2024

CANALTECH. **Facebook é condenado a pagar US$ 5 bilhões por caso Cambridge Analytica**. 2019. Disponível em: https://canaltech.com.br/redes-sociais/facebook-e-condenado-a-pagar-us-5-bilhoes-por-caso-cambridge-analytica-144841/. Acesso em: 07 out. 2024

CAVOUKIAN, Ann. Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph. D. **Identity in the Information Society**, v. 3, n. 2, p. 247-251, 2010.

CEROY, Frederico Meinberg. Os conceitos de provedores no Marco Civil da Internet. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 19, n. 4093, 15 set. 2014. Disponível em: https://jus.com.br/artigos/31938. Acesso em: 03 out. 2024.

COLNAGO, Cláudio Oliveira Santos. **Liberdade de expressão na internet: desafios regulatórios e parâmetros de interpretação**. 2016. 208 f. Tese

(Doutorado em Direitos e Garantias Fundamentais) - Programa de Pós-Graduação em Direitos e Garantias Fundamentais, Faculdade de Direito de Vitória, Vitória, 2016.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, dez. 2011.

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

DE SOUZA, Nicolle Bêtta; ACHA, Fernanda Rosa. A proteção de dados como direito fundamental: uma análise a partir da emenda constitucional 115/2022. **Revista Ibero- Americana de Humanidades, Ciências e Educação - Rease**, São Paulo, v. 8, n. 9, p. 666-684, set. 2022.

G1. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 07 out. 2024.

GREENLEAF, Graham. An Endnote On Regulating Cyberspace: Architecture vs Law? **University of New South Wales Law Journal.** Volume 21, Number 2 'Electronic Commerce: Legal Issues For The Information Age'; (1998). Disponível em http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2188160 Acesso em: 07 out. 2024

ISTOÉ. **Segurança de dados: Brasil é o 6º país com mais vazamentos, diz pesquisa.** 2022. Disponível em: https://istoedinheiro.com.br/seguranca-de-dados-brasil-e-o-6o-pais-com-mais-vazamentos-diz-pesquisa/. Acesso em: 07 out. 2024

LEONARDI, Marcel. **Internet e regulação**: o bom exemplo do Marco Civil da Internet. 2012. Disponível em <http://leonardi.adv.br/2012/04/internet-e-regulacao-o-bom-exemplo- do-marco-civil-da-internet/>. Acesso em: 07 out. 2024

LESSIG, Lawrence. **Architecting for control.** Cambridge, 2000. Disponível em:https://cyber.law.harvard.edu/works/lessig/camkey.pdf Acesso em: 07 out. 2024
_____. **Code 2.0**. New York: Basic Books, 2006, 410p.

_____. **Cyberspace's constitution.** Berlin, 2000. Disponível em: https://cyber.law.harvard.edu/works/lessig/AmAcd1.pdf. Acesso em: 07 out. 2024
_____. The New Chicago School. **The Journal of Legal Studies**, vol. XXVII, Jun 1998A, p. 661-691.

MACHADO, Diego; DONEDA, Danilo. Direito ao anonimato na internet: fundamentos e contornos dogmáticos de sua proteção no direito brasileiro (Right to Anonymity on the Internet: Foundations and Legal Outlines for Its Protection in the Brazilian Law). **Revista de Direito Civil Contemporâneo**, v. 23, p. 95-140, 2018.

MAYER-SCHOENBERGER, Viktor. Demystifying Lessig. **Wisconsin Law Review**, vol. 4, out. 2008, p. 713-746.

MENDES, Hugo Rocha. A proteção de dados pessoais: diálogo entre o CDC e a Lei Geral de Proteção de Dados. **Estudos Sobre o Direito Civil**, Goiânia, p. 13-19, 2023. Disponível em: https://unigoias.com.br/wp-content/uploads/E-book-Estudos-sobre-o- Direito-Civil-2023-1.pdf#page=19. Acesso em: 05 jun. 2024.

MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, v. 12, n. 39, p. 185-216, dez. 2018.

MOREIRA, Nelson Camatta. A Função Simbólica Dos Direitos Fundamentais. **Revista de Direitos e Garantias Fundamentais**, nº 2, p. 163-192, 13 ago. 2007.

MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, *[S. l.]*, v. 19, n. 3, p. 159–180, 2018. DOI: 10.18759/rdgf.v19i3.1603. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 9 out. 2024.

O GLOBO. **Vazamento de dados pode ter afetado até 500 milhões de hóspedes do grupo Marriott**. 2018. Disponível em: https://oglobo.globo.com/economia/vazamento-de-dados-pode-ter-afetado-ate-500-milhoes-de-hospedes-do-grupo-marriott-23270767. Acesso em: 07 out. 2024.

O GLOBO. **Visa tira Global Payments da relação de provedores seguros.** 2012. Disponível em: https://oglobo.globo.com/economia/visa-tira-global-payments-da-relacao-de-provedores-seguros-4474834. Acesso em: 07 out. 2024.

PEDRA, A. S. A. O Tribunal Constitucional e o exercício da função legislativa stricto sensu para a efetivação dos direitos fundamentais em decorrência de uma omissão legislativa inconstitucional. **Revista de Direitos e Garantias Fundamentais**, *[S. l.]*, n. 11, p. 221–256, 2012. DOI: 10.18759/rdgf.v0i11.161. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/161. Acesso em: 9 out. 2024.

POPPER, Karl. **A lógica da pesquisa científica**. São Paulo, Cultrix, 2013.

PWC. **90% dos consumidores brasileiros afirma que a proteção dos seus dados pessoais é um dos fatores mais importantes para as empresas conquistem a sua confiança.** 2024. Disponível em: https://www.pwc.com.br/pt/sala-de-imprensa/release/90-dos-consumidores-brasileiros-afirma-que-a-protecao-dos-seus-dados-pessoais-e-um-dos-fatores-mais-importantes.html#:~:text=Temas%20atuais-,PwC%3A%2090%25%20dos%20consumidores%20brasileiros%20afirma%20que%20a%20proteção%20dos,empresas%20conquistem%20a%20sua%20confiança. Acesso em: 07 out. 2024.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, v. 14, n. 42, p. 179-218, jun. 2020.

SARTORI, E. C. M.; BAHIA, C. J. A. Big Brother is watching you: da distopia orwelliana ao direito fundamental à proteção de dados pessoais. **Revista de Direitos e Garantias Fundamentais**, *[S. l.]*, v. 20, n. 3, p. 225–248, 2019. DOI: 10.18759/rdgf.v20i3.1785. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1785. Acesso em: 9 out. 2024.

SCHEWIK, Barbara van. **Internet architecture and innovation**. Cambridge: The MIT Press, 2010, 7361p. (*Kindle Edition*).

SILVEIRA, Sérgio Amadeu da. **Software livre:** a luta pela liberdade do conhecimento. Cidade: São Paulo, 2004.

SPINDLER, Gerald; SCHMECHEL, Philipp.Personal data and encryption in the European General Data Protection Regulation. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, v. 7, p. 171, 2016.

THE GUARDIAN. **Marriott hotels:** data of 500m guests may have been exposed. 2018. Disponível em: https://www.theguardian.com/world/2018/nov/30/marriott-hotels-data-of-500m-guests-may-have-been-exposed#:~:text=Personal%20data%20including%20credit%20card,Westin%2C%20Le%20Méridien%20and%20Sheraton. Acesso em: 07 out. 2024.

TOTVS. **Criptografia: o que é e para que serve essa tecnologia?**. 2024. Disponível em: https://www.totvs.com/blog/gestao-para-assinatura-de-documentos/criptografia/. Acesso em: 07 out. 2024.

UNIÃO EUROPEIA. Conselho Europeu. **Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal**. Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em: 10 out. 2024.

VISEU. **Autoridade de Dados do Reino Unido multa a rede hoteleira Marriot por falha na segurança não detectada em operação de M&A.** 2020. Disponível em: https://viseu.com.br/noticias/digital/autoridade-de-dados-do-reino-unido-multa-a-rede-hoteleira-marriot-por-falha-na-seguranca-nao-detectada-em-operacao-de-ma/. Acesso em: 07 out. 2024.

WACKS, Raymond. **Personal information**. Oxford: **Clarendon Press**, 1989.

WHATSAPP. **Como usar as transmissões no WhatsApp**. 2024. Disponível em: https://faq.whatsapp.com/820124435853543/?locale=pt_BR. Acesso em: 07 out. 2024.