REVISTA DE DIREITO | VIÇOSA | ISSN 2527-0389 | V.14 N.01 2020
DOI: doi.org/10.32361/2022140113764

A LGPD E A CONSTRUÇÃO DE UMA CULTURA DE PROTEÇÃO DE DADOS |
THE LGPD AND THE CONSTRUCTION OF A DATA PROTECTION CULTURE

LYS NUNES LUGATI
JULIANA EVANGELISTA DE ALMEIDA

RESUMO | O presente artigo traz uma análise da Lei Geral de Proteção de Dados (LGPD) e um levantamento das principais mudanças que a legislação propõe, a fim de compreender como foi feita sua adequação pelas empresas e os principais impactos percebidos. A ideia deste artigo é demonstrar que o principal propósito da Lei – a implementação de uma cultura de proteção de dados – foi ignorado, ao passo que houve o foco em promover uma rápida implementação da legislação com a finalidade precípua de não incorrer em sanções. Sendo assim, através de pesquisas qualitativas e quantitativas sobre o tema, o artigo buscou demonstrar a imprescindibilidade de um pensamento inovador e da criação de uma cultura de proteção de dados nas empresas, a fim de que se promova uma implementação e consolidação da legislação e de seus benefícios de forma contínua e duradoura.

PALAVRAS-CHAVE | LGPD. Proteção de dados. Empresas. Cultura. Tecnologia.

ABSTRACT | *This article presents an analysis of the General Data Protection Law (LGPD) and a survey of the main changes that the legislation proposes, in order to investigate how it has been implemented in companies and the impacts that have been perceived. The idea of this article is to show that the main purpose of the Law – the implementation of a data protection culture – was ignored, while there was a focus on promoting rapid implementation of legislation with the primary purpose of not incur sanctions. Thus, through qualitative and quantitative studies on the topic, the article sought to show the need for innovative thinking and for the creation of a culture of data protection in companies, in order to promote the implementation and consolidation of legislation and its benefits in a continuous and long-lasting way.*

KEYWORDS | *LGPD. Data Protection. Companies. Culture. Technology.*

1. INTRODUÇÃO

Dentro do contexto do *Big Data,* a sociedade passa pela datificação das coisas. Isso implica dizer que a cada dia mais dados transitam pela internet em velocidades e números exponenciais. Como Bioni (2020) defende, visualiza-se uma vigilância descentralizada, com múltiplos atores envolvidos no processamento de dados, sem a separação da vida *on-line* e *off-line*. Nessa perspectiva é que crescem as violações a diversos direitos fundamentais do titular de dados que vê a sua privacidade sendo constantemente violada.

Todo esse contexto de acentuado uso de tecnologias fez emergir a necessidade de legislações de proteção de dados que realmente abordassem o direito à proteção de dados e colocassem o titular como participante do processamento de dados, tendo em vista que se encontra em uma posição (hiper) vulnerável, conforme Bioni (2020) mesmo defende, e que precisa estar ciente do que acontece com seus dados, consentindo com isso.

O assunto de proteção de dados já era indiretamente tratado em legislações esparsas como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet. Contudo, não existia regulamentação que abordasse especificamente a problemática da proteção de dados, o que colocou em destaque a importância de se ter uma legislação específica sobre isso.

Nessa linha do tempo, outros países também implementavam suas leis. Assim, a União Europeia, que já tinha históricos de legislações como a Convenção 108 e a Diretiva 95/46, implementou uma legislação de proteção de dados extensiva e que regulamentou o tratamento de dados pelos seus signatários, qual seja, a *General Data Protection Regulation* (GDPR). A criação dessa legislação serviu como catalisador para outros países e dessa forma, o Brasil cria, em 2018, a Lei Geral de Proteção de Dados (LGPD).

A LGPD vinha sendo desenvolvida desde 2010 e insere o Brasil entre os países que têm legislações completas sobre proteção de dados. Seu texto,

seguindo a linha das legislações de dados mais atuais, como a *GDPR,* denota a importância dada ao consentimento, tendo em vista que o instituto é apresentado diversas vezes ao longo do texto, além de ser agora adjetivado como “livre”, “informado” e “inequívoco” e servir como orientação para várias outras normas apresentadas pela legislação.

Essa nova normativa exigiu, então, uma mudança no pensamento das organizações brasileiras, que precisaram adaptar todo seu processo de tratamento de dados a fim de não incorrerem em possíveis sanções, o que as levaram a buscar uma série de passos pré-determinados a fim de fazer essa adequação de forma rápida.

Contudo, a LGPD pretende uma mudança de pensamento duradoura, prezando por estabelecer uma cultura de proteção de dados no cenário brasileiro, o que tem sido ignorado, tendo em vista que o receio de sofrer sanções foi o principal motivo que levou as empresas a se adaptarem, e não o verdadeiro intuito da Lei, que é o de garantir a segurança dos dados e proteção de seus titulares a longo prazo.

Ante o exposto, este artigo propõe uma análise dos requisitos estabelecidos pela LGPD, bem como um estudo de como as empresas têm se adaptado a isso, a fim de sugerir a importância de uma cultura de proteção de dados para as empresas, que seja baseada em uma cultura baseada em inovação, time com responsabilidades definidas, técnicas de segurança da informação e que permitam o repasse de informações de forma clara.

2. DA EVOLUÇÃO DAS LEGISLAÇÕES DE PROTEÇÃO DE DADOS NO ORDENAMENTO JURÍDICO

A discussão sobre o que hoje se conceituaria como privacidade se originou na medida em que as tecnologias se tornaram invasivas, dando margem à divulgação de informações da esfera privada do indivíduo. Com o *artigo “The right of privacy”,* de Warren e Brandeis, inaugura-se a discussão sobre o assunto, embora ainda sob uma perspectiva de privacidade que diz

respeito ao “direito a estar só”, expressão utilizada pelo jurista Thomas McIntyre em 1888, conforme indica Cancelier (2017).

Dessa forma, surge uma ideia do direito à privacidade que coaduna com a primeira geração de direitos fundamentais, com foco no direito à liberdade, em que o Estado assume postura de se abster de entrar nas relações individuais.

Conforme Doneda (2006) mesmo indica, o avanço das tecnologias e uma maior capacidade de processamento de informações faz emergir um novo delineado ao conceito, de forma que se cresce a democratização do interesse por uma tutela da privacidade e de seu exercício. Assim, se começa a falar em proteção de dados pessoais. Mendes (2014) indica que decisões que protegem os dados pessoais como uma extensão da personalidade do indivíduo e hábeis a receber proteção jurídica passam a ser vistas por volta de 1970.

A posição adotada pelas doutrinas é a assumida por Viktor Mayer-Scönberger. Ela demonstra que a regulamentação da proteção de dados pessoais percorreu quatro gerações distintas e, de acordo com Doneda (2011, p. 96), são “leis que partem de um cerne mais técnico e restrito para, por fim, ampliar as disposições e as técnicas referentes às tecnologias modernas”.

A primeira geração de leis tem como cenário o Estado Moderno. Através de uma postura autoritária, o Estado se utiliza de informações dos indivíduos para maior controle e, portanto, necessita de um grande volume de dados. O Estado é o destinatário de tais regulamentos.

Como exemplo, vê-se o *Privacy Act*, ato norte-americano de 1974. Essa primeira geração de leis, no entanto, percorre um longo caminho, que se estende até o implemento da *Bundesdatenschutzgesetz*, a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977. Nesse período, podem-se visualizar diversas leis acerca de proteção de dados na Alemanha, que nas palavras de Gasiola (2019):

> [...] são reações a projetos estatais para implementar bancos de dados centralizados sobre a população, em meio à euforia tecnológica que marcou o pós-guerra. O choque entre a recente lembrança (ou presença) dos governos autoritários e a iminência de tais projetos levou ao reconhecimento expresso da proteção de dados perante as pretensões públicas de aumentar seu poder informacional. O objetivo dessas leis era, acima de tudo, estabelecer limites e garantir a transparência na criação de bancos de dados.

Porém, entes privados passam também a tratar dados e, assim, nasce a necessidade de uma nova geração de leis. No contexto da segunda geração de leis, o usuário passa a participar do tratamento de dados em algumas fases, conforme aponta Bioni (2020).

Ato contínuo, cresce a preocupação em garantir a efetividade do direito à privacidade. Logo, não somente há a necessidade da cessão ou não de dados, mas há a cautela com o titular de dados, no momento em que ele passa a participar de todas as fases do tratamento, para que de fato este direito seja garantido de forma plena.

A quarta geração de dados, que prevalece até hoje, vem da urgência em garantir que todos os indivíduos sejam assegurados por essas regulamentações, tendo em vista que a terceira geração só abarca uma parcela de indivíduos. A ótica passa a ser em torno do usuário e há a cautela de que haja realmente uma proteção coletiva. Nas palavras de Doneda (2011, p. 98):

> Nestas leis procura-se enfocar o problema integral da informação, pois elas presumem que não se pode basear a tutela dos dados pessoais simplesmente na escolha individual – são necessários instrumentos que elevem o padrão coletivo de proteção.

Nessa mesma ideia é que se nota o crescimento da importância do requisito do consentimento, que ganha adjetivos como “livre, informado, inequívoco, explícito e/ou específico”, consoante Bioni (2020).

No ordenamento brasileiro, a proteção de dados é tratada desde 1988, na Constituição Federal de 1988 (CF/88), sendo visualizada através do direito de personalidade, à liberdade de expressão (art. 5º, IX) e direito à informação

(art. 5, XIV). Há também a consagração de outros direitos que abrangem a ideia, como o direito à inviolabilidade da vida privada e intimidade (art. 5º, X), o habeas data (art. 5º, LXXII) e a interceptação das comunicações telefônicas, telegráficas ou de dados (art. 5º, LXXII).

Não obstante, o Código de Defesa do Consumidor, em 1990, regulamenta a proteção de dados, de uma forma indireta. Isso ocorre porque o artigo 43 garante determinada proteção do titular de dados quando se vê diante de bancos de dados e cadastros, visto que deve ser comunicado sobre a abertura de cadastros, ficha, registro e dados pessoais e de consumo.

Mesmo assim, ainda é um direito à comunicação e apesar de garantir uma breve proteção ao titular de dados, ainda não diz respeito à proteção de dados de forma plena, até mesmo porque o consumidor não participa do processamento em todas suas fases.

Segundo Andrade e Moura (2019), a legislação consumerista ainda estava mais preocupada em regular os bancos de dados do que pensar sobre consentimento. Nas palavras dos autores:

> O presente artigo, entretanto, analisa a regra do CDC de forma mais crítica, pois se preocupa mais com a regulamentação dos Bancos de Dados do que com o consentimento prévio ao registro ou arquivamento dos mesmos, estando mais próxima das normas de primeira geração do que as de terceira. Ademais, a suposta autodeterminação informacional do consumidor resta ainda mais fragilizada a partir da Súmula no 404, do STJ, que adverte: "É dispensável o aviso de recebimento (AR) na carta de comunicação ao consumidor sobre a negativação de seu nome em bancos de dados e cadastros".

Para Mendes (2014), a lei 12.414/2011, "Lei do Cadastro Positivo" consolida uma evolução do conceito de autodeterminação informativa no ordenamento, pois trata o consentimento como requisito basilar. A Lei do Cadastro Positivo regulamenta a formação e consulta a bancos de dados que têm informações de adimplemento de pessoas naturais ou jurídicas para formar um histórico de crédito.

Há uma introdução do sistema *opt-in*[1] no ordenamento jurídico brasileiro, conforme diz Krieger (2019), pois o consentimento passa a ser fundamental, o que não era consagrado pelo Código de Defesa do Consumidor. Em 2019, a Lei Complementar nº 166/2019 regrediu ao sistema *opt-out*[2], pois há a inclusão de consumidores no banco de dados automaticamente, conforme afirma Bioni (2020).

Após um episódio de espionagem revelado por Edward Snowden, na Agência Nacional de Segurança dos Estados Unidos, envolvendo o Brasil, ganhou proeminência a regulamentação do Marco Civil da Internet. Sendo assim, a presidente Dilma, após o caso, adotou o regimento de urgência da lei, e aprovou o Marco num evento de governança multisetorial da internet (NetMundial) (ARAGÃO, 2020).

Na explicação de Bioni (2020), o Marco Civil da Internet se preocupou em garantir que não houvesse um retardo da inovação tecnológica no país ao se tentar regular o uso da internet por leis penais de forma restritiva e abordou a regulação do uso da Internet, com a garantia de direitos e garantias do cidadão no meio ambiente virtual.

Mesmo assim, apesar da menção ao consentimento adjetivado, não foi uma legislação que tratou especificamente da proteção de dados. Esta proteção só foi tratada de forma específica com a Lei Geral de Proteção de Dados, Lei 13.709, em 2018.

O Brasil carecia de uma legislação mais completa, principalmente em atenção ao artigo 46 da *General Data Protection Regulation* (GDPR), Lei de Proteção de Dados da União Europeia, que definiu que a transferência de dados só poderia ser feita a países que também tivesse leis que gerassem uma proteção adequada, vejamos:

1 De acordo com SENDPULSE (2020), "Opt-in é uma abordagem do Inbound Marketing em que um profissional de marketing digital solicita a permissão de um cliente em potencial para enviar determinado tipo e conteúdo sobre uma marca. Também é conhecido como marketing de permissão e pode ser opt-in único ou double opt-in".

2 De acordo com Davanzo (2015), "o sistema *opt-out* de envio é aquele onde o consumidor é inserido numa lista de "alvos" da empresa, recebe a publicidade eletronicamente e tem a possibilidade de ser excluído desse *mailing list* se assim requerer".

> Artigo 46º. Transferências sujeitas a garantias adequadas 1. Não tendo sido tomada qualquer decisão nos termos do artigo 45.o, n.o 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.

O Brasil passa a ter então uma legislação de proteção de dados que abrange especificamente o tratamento de dados, em meio ambiente virtual ou não, colocando uma série de princípios e garantias aos titulares e os envolvendo em todo o processamento. Isso já se pode ver no artigo 1º da LGPD:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Há diversas inovações trazidas pela Lei como, por exemplo, a responsabilização dos agentes frente ao tratamento de dados, a participação dos titulares desde a coleta até a transferência a terceiros, definições próprias para o processamento de dados e hipóteses em que este tratamento poderá ocorrer. Uma das maiores repercussões, contudo, é notada com a grande importância ao consentimento do usuário.

Na primeira versão do anteprojeto da lei para proteção de dados colocada para consulta em 2010 o consentimento era colocado como a única hipótese em que para haver o tratamento de dados. Mas, apesar de o artigo 7º da LGPD prever outras hipóteses, Bioni (2020) entende que continua sendo o vetor principal. E isso fica evidente quando, por exemplo, este aparece 35 vezes ao longo do texto da Lei.

De acordo com Mendes (2014), pela ótica da LGPD, a validade do consentimento passa a se formar a partir dos pressupostos de que:

> [...] o titular deve emitir consentimento por sua livre e espontânea vontade; ii) o consentimento deve ser voltado a uma finalidade específica; iii) deve haver informação ao usuário sobre os objetivos da coleta, processamento e uso de dados e consequências sobre não consentir com o tratamento.

Depois de muitos debates acerca da data de entrada em vigor da legislação, principalmente frente à pandemia enfrentada pelo COVID-19, a Lei passou a vigorar, efetivamente, em 18 de agosto de 2020.

Sendo assim, com a introdução da Lei Geral de Proteção de Dados e a urgência em efetivá-la, principalmente frente às incertezas que foram geradas em virtude da data de sua entrada em vigor, começaram a serem adotadas uma série de medidas e passos prontos para adaptar o cotidiano das Empresas e escritórios ao que a Lei dispõe, para não incorrer em possíveis sanções.

Mas o que se pretende discutir é que para implementar a LGPD de forma efetiva na vivência do tratamento de dados, é fundamental repensar a Lei não só como uma legislação que possa trazer possíveis sanções e responsabilização dos envolvidos, mas como passo importante para garantir a segurança das organizações e dos titulares de dados, com possibilidade de resultados duradouros e que vão além de sua implementação.

Sendo assim, o que se defende é que, indo além da implementação que foi feita de forma rápida, se deve criar é uma mudança na cultura organizacional[3] das empresas, a fim de gerar uma cultura de proteção de dados, que ainda não foi consolidada.

Essa mudança deve focar, basilarmente, em quatro pilares, que são: estabelecimento de uma cultura inovativa; definição e consciência das responsabilidades de cada membro; técnicas de segurança da informação e técnicas que permitem o repasse de informações de forma clara aos titulares.

3 Para Armbrust, "Cultura organizacional (também chamada de cultura empresarial e corporativa) é o conceito que define a forma com que a organização conduz seus negócios e em como trata seus clientes e parceiros. E, nisso, envolve práticas, políticas e comportamentos que são reflexo da cultura".

3. REFLEXOS DA LGPD NAS EMPRESAS BRASILEIRAS E A CRIAÇÃO DE UMA CULTURA DE PROTEÇÃO DE DADOS

A LGPD revolucionou o cenário de proteção de dados no Brasil. Um tema antes quase não dito, passou a ser o foco de todas as empresas, que precisaram se adaptar rapidamente à legislação, que estabeleceu uma série de requisitos para o tratamento de dados.

A disseminação de dados, que acontece numa velocidade exponencial, agora precisa seguir uma série de normas que a Lei dispõe, e há a necessidade de bases legais que justifiquem o início do tratamento e quaisquer ações que envolvam os dados, bem como que os Controladores e Operadores mantenham o controle de tudo o que acontece, sabendo que podem ser cobrados pelo Usuário, que participa ativamente de todas as etapas desse processo, garantindo sua autodeterminação informativa.

Sendo assim, a LGPD impactou o ordenamento jurídico, ao passo que garantiu que o assunto começasse a ser visto como importante, coisa que já acontecia em outros países, como na União Europeia, com a General Data Protection Regulation (GDPR). Apesar de o assunto já fosse contemplado em legislações esparsas, como supramencionado, não havia nada específico e que conferisse tamanha importância à proteção de dados no Brasil.

Essa mentalidade precisava ser difundida, principalmente quando os titulares de dados começaram a se deparar com inúmeros casos de vazamento de dados por parte de grandes empresas e a terem seus direitos fundamentais violados, como por exemplo, com o caso recente da empresa norte-americana Cambridge Analytica (ENTENDA..., 2020).

Com uma data de vigência estabelecida para o início da Lei, surgem então inúmeros procedimentos prontos que permitem que as empresas tenham uma rápida adequação, a fim de não sofrer as sanções que a Lei propõe. Passa a ser uma corrida contra o tempo, para se adaptar antes de que as sanções possam ser aplicadas.

Nessa perspectiva, ganharam força algumas figuras, sobretudo a de profissionais da área, como os intitulados *Data Protection Officers* (DPO), e cresceu a procura por advogados da área do direito digital e proteção de dados pessoais.

Assim, torna-se de extrema importância a criação de um time qualificado no assunto para guiar as decisões que a empresa tomará, como no que tange à criação de termos de consentimento, políticas de privacidade, termos de uso, distribuição de tarefas, bem como outras etapas necessárias para a que a organização esteja em consonância com as legislações atinentes.

Não obstante, a criação de um modelo eficiente para ser implementado nas organizações, trouxe a necessidade de conhecê-las a fundo, identificando todo seu cenário, mapeando os dados que são utilizados e coletados, os riscos que a permeiam, o modo como os colaboradores devem ser treinados, entre outros. Entender as empresas e dedicar um time adequado ao assunto é fundamental quando se fala em adequação às legislações de proteção de dados, de fato.

Contudo, há que se falar no assunto de uma forma mais profunda, considerando que a principal importância da chegada da LGPD se refere à criação de uma cultura sobre proteção de dados, ou seja, não basta que a empresa pareça adequada para a não incorrência em sanções: é necessário que a proteção de dados pessoais seja pensada em todas as ações dos membros do time.

Sendo assim, o assunto não cessou quando a LGPD entrou em vigor, em 2020, mas muito pelo contrário, a entrada em vigor passou a ser apenas o início de uma discussão sobre o que é proteção de dados pessoais. Indo ao contraponto do que se pensa, o assunto ainda não é de fato basilar ao cotidiano das empresas e vivências de seus colaboradores, por isso a necessidade de refletir sobre o verdadeiro intuito da legislação e como essa adequação deveria ser pensada.

O ano de 2021 foi marcado por uma série de ciberataques, apesar da marcante entrada da legislação em vigor. De acordo com a Psafe, mais de 600

milhões de dados foram vazados no país, com 44,5 milhões de tentativas de golpes virtuais de estelionato detectadas pelos sistemas do laboratório de cibersegurança e 4 milhões de bloqueios de “malware”, arquivos que são nocivos e podem invadir redes de empresas e permitir o sequestro de dados[4].

Por isso, a PwC trouxe a constatação de que 83% das empresas brasileiras visam aumentar os gastos com segurança digital neste ano, sendo que em 2020 os índices foram de apenas 55%[5].

Junto a isso, percebe-se também que a Autoridade Nacional de Proteção de Dados (ANPD) tem atuado para fiscalizar a aplicação da LGPD e, inclusive, pretende aplicar penalidades com efeito retroativo pelo descumprimento da Lei Geral de Proteção de Dados (LGPD) a partir da data de vigência das sanções, que foi em agosto de 2021[6].

Isso demonstra que, apesar da chegada da Lei, não houve realmente a implementação de uma cultura de proteção de dados no Brasil. Essa cultura ainda precisa, de fato, ser construída. O que houve, ao revés do pretendido, foi um equivocado entendimento de que a chegada da LGPD traria por si só a segurança dos dados pessoais e que bastaria que as empresas seguissem um plano pronto a fim de não incorrer em possíveis sanções.

Esse pensamento de que as legislações sobre proteção de dados devem permear todas as ações dos encarregados comumente se denomina de *privacy by design*, e é trazido pela própria legislação, como por exemplo, em seu artigo 46:

> 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.

4 KUCK, Daniel. Ano marcado por ciberataques eleva verba de proteção. Disponível em: https://www.lgpdbrasil.com.br/ano-marcado-por-ciberataques-eleva-verba-de-protecao/.

5 KUCK, Daniel. Ano marcado por ciberataques eleva verba de proteção. Disponível em: https://www.lgpdbrasil.com.br/ano-marcado-por-ciberataques-eleva-verba-de-protecao/.

6 LGPD BRASIL. Sanções por descumprimento da Lei devem ter efeito retroativo. Disponível em: https://www.lgpdbrasil.com.br/lgpd-sancoes-por-descumprimento-da-lei-devem-ter-efeito-retroativo/.

> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (BRASIL, 2018).

A importância da criação de um plano de conformidade à LGPD que seja duradouro e de fato aplicável é refletida nos próprios artigos da Lei, que destina seção específica sobre a criação de boas práticas e governança dentro das organizações, ressaltando que deve ser um enfoque a ser observado, como se pode ver com o artigo 50 da Lei:

> 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 (BRASIL, 2018).

Dessa forma, é importante pensar na ideia trazida por Livramento, Oliveira e Moraes (2015), que discorrem sobre a importância de se estabelecer uma cultura organizacional inovativa como uma forma de proteção para as empresas.

Nessa perspectiva, uma cultura organizacional inovativa seria aquela em que, conforme indicam Godoy e Peçanha (2009), por exemplo, tenha a existência de fatores concernentes à tolerância, ambiguidade e ao erro, à oferta de um trabalho desafiante e em equipe, com suporte das lideranças, com comunicação clara, coesão e reconhecimento de esforços.

Sendo assim, há a criação de um ambiente propício à conversa e ao desenvolvimento de habilidades da equipe, em que os membros se sentem parte da organização e à vontade para o diálogo, o que consequentemente encoraja ideias inovadoras. Como diz Silva *et al*. (2014):

> Pesquisas sugerem que o sucesso de empresas que são altamente inovadoras está ancorado em uma cultura voltada para inovação, a qual disponibilizará ambiente com recursos físicos, financeiros e humanos para apoiar um clima de inovação.

Portanto, na concepção de Livramento, Oliveira e Moraes (2015), a implementação de uma cultura organizacional inovativa seria o principal meio de proteção, haja vista que se criam empresas resilientes, aptas a enfrentar mudanças e rupturas, sem que isso interfira de forma significativa em seus resultados. Conforme Sheffi (2007):

> Empresas resilientes são aquelas que investem na habilidade de retomar rapidamente suas atividades planejadas após passarem por uma ruptura e ainda garantem que seus clientes sejam minimamente afetados por tal episódio.

Nessa linha de pensamento, a BS65000, um "Guia para Organizações Resilientes" criado pela *British Standards Institution*, em 2014, define Resiliência Organizacional como a habilidade que as empresas têm de se antecipar, se preparar, responder e se adaptar tanto às mudanças repentinas quanto àquelas que ocorrem de forma gradual, ou seja, são adaptáveis, competitivas, ágeis e fortes (BSI GROUP, 2014a).

Trazendo a noção de cultura organizacional inovativa para a implementação da Lei Geral de Proteção de Dados, é notória a sua importância, ao se pensar que, caso o cenário brasileiro contasse com mais empresas resilientes, o impacto gerado pela necessidade de adaptação à Lei seria fortemente reduzido, haja vista que teríamos empresas preparadas a se adaptar a mudanças.

Ademais, Lobato (2013) defende que um modelo resiliente de organização tem pilares como descentralização, redução de níveis hierárquicos, compartilhamento de responsabilidades e estrutura de poder dinâmica. Há, assim, um sistema de comunicação eficiente e um compartilhamento de valores pela empresa.

Utilizando-se da ideia do autor é perceptível que as vantagens de empresas resilientes, como a consciência dos seus membros de suas responsabilidades e o compartilhamento de ideias, seria um importante fator quanto à implementação de uma cultura de proteção de dados.

Importante pensar que o primeiro passo a ser dado na implementação de legislação é conhecer a empresa como um todo, principalmente quais seriam as suas maiores dificuldades a serem enfrentadas, com cada membro tendo responsabilidade de qual papel terá nesse processo de implementação.

Há de se ter, então, um intenso processo de autoconhecimento e um time que entenda a importância de suas ações no decorrer da adequação. E essas seriam vantagens que empresas resilientes apresentam, o que descomplicaria esse primeiro passo.

Não obstante, Ferreira (2020) indica que é preciso ir além e promover a revisão de todos os mecanismos de segurança da informação que envolvam dados pessoais, até mesmo para garantir a rastreabilidade no caso de vazamentos e incidentes.

O conceito de segurança da informação está relacionado a práticas que visam assegurar a proteção de um conjunto de informações, dando enfoque ao valor que possuem, através de quatro pilares básicos: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

As empresas deverão, então, contar com as melhores práticas de segurança de informação, de forma urgente, haja vista que a não implementação dessas práticas é um aspecto arriscado, conforme Ferreira (2020).

Ademais, novas técnicas devem ser implementadas no dia a dia da empresa para garantir que as informações sejam transmitidas de forma transparente e clara aos usuários de dados, sabendo que a qualquer momento essas informações podem ser requisitadas pelo titular dos dados.

Além de linguagem clara e termos compreensíveis disponibilizados nos canais de comunicação externos, técnicas, como a de *Legal Design*, têm ganhado importância, garantindo que as normas sejam transmitidas de forma

simples aos usuários. Isso gera confiabilidade nos usuários e garante que estes saibam de seus direitos de forma adequada, como é o intuito da Lei.

Portanto, a implementação de uma cultura organizacional inovativa com um time que tenha a consciência de suas responsabilidades e importância da Lei, saiba empregar técnicas aprimoradas de segurança da informação e ter o cuidado em se buscar novas técnicas que permitam o repasse de informações de forma clara aos titulares de dados, é essencial para que, então, se tenha uma adequação à legislação de proteção de dados de forma plena e duradoura, exatamente como a LGPD pretende.

4. CONCLUSÃO

Dessa forma, este artigo demonstrou que a implementação da LGPD deve se basear em uma mudança na cultura organizacional das empresas, com a criação de uma cultura de proteção de dados, fundamentada em alguns pilares que permitam essa mudança.

A importância dessa mudança reside no fato de que o imediatismo em se adequar à legislação retirou o cerne da legislação, que era o de que as empresas reformulassem suas técnicas de segurança e a maneira como trazem as informações aos titulares de dados, que passa a ser o foco do tratamento de dados.

Ao invés disso, as sanções trazidas pela Lei atraíram os olhares dos encarregados da adequação, com foco apenas em uma adequação que pudesse ser feita de forma rápida. O passo a passo para a adequação se tornou um modelo pronto e a Lei foi enxergada sob seu aspecto negativo.

Por isso, buscou-se entender como as disposições trazidas pela Lei proporcionam duradouros aspectos positivos às organizações, principalmente ao estabelecer uma mudança em suas culturas organizacionais, tendo em vista que o primeiro passo rumo a uma implementação adequada seria o autoconhecimento das organizações quanto a todos seus procedimentos e seu time.

Para que a LGPD traga aquilo que propõe, portanto, há de se focar no estabelecimento de uma cultura organizacional inovativa, num time que tenha conhecimento da sua importância individual e coletiva e na busca pelas melhores técnicas de segurança e de apresentação de informações aos titulares.

Com o foco adequado, vê-se que a Lei Geral de Proteção de Dados torna-se um importante instrumento para reformular a visão que se tinha sobre proteção de dados no Brasil e que a longo prazo será hábil a trazer diversos impactos positivos, principalmente para as empresas que aproveitarem das mudanças normativas para se reinventarem.

REFERÊNCIAS

ANDRADE, Diego de Calasans Melo; MOURA, Plínio Rebouças de. O direito de consentimento prévio do titular para o tratamento de dados pessoais no ciberespaço. **Revista de Direito, Governança e Novas Tecnologias**, Goiânia, v.5, n.1, p.110-133, Jan/jun. de 2019.

ARAGÃO, Alexandre. Dilma sanciona Marco Civil na abertura do NETMundial. **Folha.** Disponível em: https://www1.folha.uol.com.br/tec/2014/04/1444200-dilma-sanciona-marco-civil-na-abertura-do-netmundial.shtml. Acesso em: 01 maio 2020.

ARMBRUST, Gabrielle. Cultura Organizacional: o que é, importância, tipos e exemplos. *In*: **GUPY**, 16 out. 2020. Disponível em: https://www.gupy.io/blog/cultura-organizacional. Acesso em: 01 nov. 2020.

BASTOS, Athena. **Legal Design: a técnica do Design Thinking aplicada ao Direito**. Disponível em: https://blog.sajadv.com.br/legal-design/. Acesso em: 18 out. 2020.

BIONI, B. R. **Xeque-Mate: o tripé de proteção aos dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. GPoPAI/USP, 2015. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em: 06 mar. 2020.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Lei 13709, de 14 de agosto de 2018. **Diário Oficial da União.** Brasília, 2018.

BSI GROUP. (Inglaterra) (Org.). **BS 65000 - Guidance for Organizational Resilience.** 2014a. Disponível em: http://shop.bsigroup.com/ProductDetail/?pid=000000000030258792. Acesso em: 04 nov. 2020.

BSI GROUP (Inglaterra) (Org.). **Organizational Resilience Standard Published**. 2014b. Disponível em: http://www.bsigroup.com/en-GB/aboutbsi/media-centre/press-releases/2014/November-2014/Organizationalresilience-standard published/#.VVKUOPlViko. Acesso em: 04 nov. 2020.

CANCELIER, Mikhail Vieira de Lorenzi; CRISTO, Camila Kohn de; MAFRA, Gabriela**. Evasão de informações privadas: proteção à privacidade nos casos de pornografia de vingança**. 2017. Disponível em: https://egov.ufsc.br/portal/conteudo/evas%C3%A3o-de-informa%C3%A7%C3%B5es-privadas-prote%C3%A7%C3%A3o-%C3%A0-privacidade-nos-casos-de-pornografia-de-vingan%C3%A7. Acesso em: 13 mar. 2020.

DAVANZO, Danilo. E-mail marketing: sistema opt-in e opt-out de envio*. In:* **Revista JusBrasil.** 15 de julho de 2015. Disponível em: https://danilodavanzo.jusbrasil.com.br/artigos/208357821/e-mail-marketing-sistema-opt-in-e-opt-out-de-envio. Acesso em: 13 abr. 2020.

DISPÕE sobre a proteção de dados pessoais, a privacidade e dá outras providências". **Cultura Digital.** Disponível em: http://culturadigital.br/dadospessoais/files/2010/11/PL-Protecao-de-Dados.pdf. Acesso em: 20 maio 2020.

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

DONEDA, Danilo. Princípios da proteção de dados pessoais. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de (Coords.). **Direito & Internet III** – Tomo I: Marco Civil da Internet (Lei n.12.965/2014). São Paulo: Quartier Latin, 2015, p.373.

ENTENDA o escândalo de uso político de dados que derrubou o valor do Facebook e o colocou na mira de autoridades". **G1.** 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: 20 out. 2020.

FERREIRA, F. **LGPD: por que você não pode mais esperar para se adaptar**, 2020. Disponível em: https://lozinskyconsultoria.com.br/estrategia-e-gestao-de-ti/lgpd-por-que-voce-naopode-mais-esperar-para-se-adaptar/. Acesso em: 24 jan. 2020.

GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha.** Disponível em:

https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 10 mar. 2020.

GODOY, R.S.P.; PEÇANHA, D.L.N. Cultura Organizacional e processos de inovação: um estudo psicossociológico em empresa de base tecnológica. **Boletim Academia Paulista de Psicologia**, São Paulo, Ano XXIX nº01/09, p.142-163, maio 2009.

KUCK, Daniel. **Ano marcado por ciberataques eleva verba de proteção**. Disponível em: https://www.lgpdbrasil.com.br/ano-marcado-por-ciberataques-eleva-verba-de-protecao/. Acesso em: 15 jan. 2022.

KRIEGER, Maria Victoria Antunes. **A análise do instituto do consentimento frente à lei geral de proteção de dados do brasil (lei nº 13.709/18)**. Trabalho de Conclusão de Curso (graduação) – Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, 2019. Data da publicação: 05 de dezembro de 2019. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/203290/TCC.pdf?sequence=1&isAllowed=y. Acesso em: 20 mar. 2020.

LGPD BRASIL. **Sanções por descumprimento da Lei devem ter efeito retroativo**. Disponível em: https://www.lgpdbrasil.com.br/lgpd-sancoes-por-descumprimento-da-lei-devem-ter-efeito-retroativo/. Acesso em: 15 jan. 2022.

LIVRAMENTO, T. F. S.; OLIVEIRA, E. A. de A. Q.; MORAES, M. B. de. Empresas resilientes: o desafio de estabelecer uma cultura inovativa como fator de proteção. **Latin American Journal of Business Management**, Taubaté, v. 6, n. 2, p. 237-255, jan. /jun. 2015.

LOBATO, D.M. **Gestão Resiliente: um modelo eficaz para a cultura empresarial brasileira contemporânea**. São Paulo: Atlas, 2013.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. Série IDP: linha de pesquisa.

SENDPULSE. **O que é Opt In?.** Disponível em: https://sendpulse.com/br/support/glossary/opt-in. Acesso em: 02 nov. 2020.

SHEFFI, Y. **The resilient enterprise:** overcoming vulnerability for competitive advantage. Massachusetts: MIT Press, 2007.

SILVA, M. A. C. et al. Cultura Inovativa e Formação de Ambiente Inovador. *In*: **XVII SEMEAD Seminários em Administração**, ISSN 2177-3866. São Paulo: out. 2014.

TOTVS. **O que é DPO e qual a importância desse profissional?**. Disponível em: https://www.totvs.com/blog/negocios/o-que-e-dpo/#:~:text=A%20Lei%20Geral%20de%20Prote%C3%A7%C3%A3o,clientes%20quanto%20da

%20pr%C3%B3pria%20organiza%C3%A7%C3%A3o. Acesso em: 19 out. 2020.

UGGERI, Karollyne. Compliance Digital: os benefícios da implementação. *In*: *Revista Migalhas,* 01 mar. 2018. Disponível em: https://migalhas.uol.com.br/depeso/275349/compliance-digital---os-beneficios-da-implementacao. Acesso em: 19 out. 2020.

VENTURA, Leonardo Henrique de Carvalho. Privacy by Design e Compliance na LGPD. *In*: *Revista Jus*, 11 out. 2018. Disponível em: https://jus.com.br/artigos/69585/privacy-by-design-e-compliance-na-lgpd. Acesso em: 21 out. 2020.

SUBMETIDO | *SUBMITTED* | 15/01/2022
APROVADO | *APPROVED* | 16/05/2022

REVISÃO DE LÍNGUA | *LANGUAGE REVIEW* | Maria Carolina Ferreira Reis

SOBRE AS AUTORAS | *ABOUT THE AUTHORS*

LYS NUNES LUGATI

Pós-graduanda em Advocacia Contratual e Responsabilidade Civil pela Escola Brasileira de Direito. Bacharela em Direito pela Universidade Federal de Ouro Preto. Pesquisadora em Direito Digital. Analista Jurídico da Gerencianet S.A. E-mail: nuneslys@gmail.com.

JULIANA EVANGELISTA DE ALMEIDA

Doutora e Mestra em Direito Privado pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas). Especialista em Direito Civil pela PUC Minas. Bacharela em Direito pela PUC Minas. Professora do curso de Direito da Universidade Federal de Ouro Preto. Pesquisadora em Direito Digital. E-mail: juliana.almeida@ufop.edu.br.