UNIVERSIDADE DO SUL DE SANTA CATARINA

HELOISA DOS SANTOS GOMES

LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): UMA ANÁLISE DOS IMPACTOS DA LEI NA CULTURA E TRATAMENTO DE DADOS NO BRASIL

Florianópolis

2019

HELOISA DOS SANTOS GOMES

LGPD:
UMA ANÁLISE DOS IMPACTOS DA LEI NA CULTURA E TRATAMENTO DE DADOS NO BRASIL

Trabalho de Estudo de Caso apresentado ao Curso de Tecnologia em Análise e Desenvolvimento de Sistemas da Universidade do Sul de Santa Catarina como requisito parcial à obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Prof. Maria Inés Castiñeira, Dra.

Prof. Vera R. Niedersberg Schuhmacher, Dra.

Florianópolis

2019

RESUMO

Dados são coletados e utilizados por todo tipo de empresa. A Lei Geral de Proteção de Dados trouxe à luz uma imensa parte dessas empresas que não são adeptas de métodos e técnicas de segurança da informação e terão que adaptar-se. Portanto essa nova lei terá um grande impacto em todos os tipos de negócio e em toda a sociedade.

Além das empresas, toda a sociedade sentirá o impacto dessa nova lei, o cidadão comum aos poucos irá conhecer seus novos direitos e todas as regras sobre como as empresas terão que comportar-se no que diz respeito à coleta e tratamento dos seus dados pessoais.

Palavras-chave: Lei Geral de Proteção de Dados. LGPD. Segurança de Dados.

SUMÁRIO

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados, tratada nesse artigo como LGPD, é uma lei brasileira que deve entrar em vigor em agosto de 2020. A referida lei altera a forma como as empresas brasileiras e estrangeiras coletam e tratam dados em território nacional (BRASIL, 2018).

1.1 PROBLEMÁTICA

As empresas brasileiras e estrangeiras que coletam e tratam dados no Brasil terão que adequar-se à nova lei - Lei nº 13.709/2018. Diante desse cenário, está sendo um grande desafio para as empresas comprometerem-se em não somente investir em tecnologias que ajudem no processo de segurança da informação, como também mudar sua cultura e o paradigma da coleta de dados não essenciais para o negócio.

Para os dados essenciais que serão coletados pelas empresas, como por exemplo, os dados indispensáveis para emissão de uma nota fiscal ou para a execução de um contrato, a lei exige que os dados tenham proteção contra invasão, também exige que os dados não sejam usados para outros fins além daquele para qual foram coletados (SERPRO, 2019).

As medidas que devem ser tomadas por todas as empresas e órgãos públicos vão desde garantir a segurança dos dados, quanto a pseudonimização ou anonimização dos dados para auxiliar na redução dos riscos para os titulares até outras que serão tratadas no decorrer deste artigo.

1.2 OBJETIVOS

A seguir são apresentados os objetivos deste trabalho.

1.2.1 Objetivo geral

Neste trabalho será apresentado um estudo da lei, seus aspectos e impactos nas empresas, órgãos públicos e na sociedade como um todo. Também abordará a importância dos dados e a transformação da economia na era digital e sua consequente dependência das bases de dados.

1.2.2 Objetivos específicos

São objetivos específicos deste trabalho:

- Apresentar de maneira simples para compreensão de um leigo, quais são as mudanças às quais as empresas precisarão adequar-se.
- Explanar sobre a importância da coleta e tratamento de dados pelas empresas e como algumas delas estavam tendo condutas consideradas inadequadas no tratamento de dados pessoais.
- Esclarecer sobre as possíveis sanções e como se dará a aplicação da lei.

1.3 JUSTIFICATIVA

Dados são coletados e utilizados por todo tipo de empresa, portanto essa nova lei terá um grande impacto em todos os tipos de negócio e em toda a sociedade. Assim, pode-se afirmar que o conhecimento da lei é necessário para as empresas evitarem sanções administrativas, judiciais e multas.

Também é de suma importância para o cidadão comum conhecer seus novos direitos e todas as regras sobre como as empresas terão que comportar-se no que diz respeito à coleta e tratamento dos seus dados pessoais.

1.4 MÉTODO

Para escrever este artigo foi utilizada a metodologia de pesquisa bibliográfica e documental.

O método de pesquisa documental é extremamente útil para a análise da lei, tema principal deste trabalho. “A análise documental busca identificar informações factuais nos documentos a partir de questões e hipóteses de interesse” (CAULLEY apud LÜDKE e ANDRE, 1986, p. 38).

Já a pesquisa bibliográfica, como destaca Gil (1994), possibilita um amplo alcance de informações, auxiliando na melhor definição do quadro conceitual que envolve o objeto de estudo proposto.

2 DADOS PESSOAIS E A ECONOMIA

Os avanços tecnológicos e a globalização trouxeram como consequência um grande fluxo de negócios, o aumento da troca de informações, e depois, o surgimento dos negócios digitais. Os negócios digitais, por sua vez fizeram com que as informações se tornassem cada vez mais importantes, dependendo assim, dos bancos de dados.

Uma reportagem publicada na renomada revista *The Economist* em 2017 chamou a atenção por seu título "O recurso mais valioso do mundo não é o petróleo, mas dados", que apesar de parecer sensacionalista, era realista.

Já em 2017, os dados eram tratados como "o óleo da era digital". Empresas como a *Alphabet*, *Amazon*, *Facebook*, e Microsoft foram citadas na matéria como as cinco empresas mais valiosas do mundo. Conforme destaca a reportagem (THE ECONOMIST, 2017, tradução nossa):

> Seus lucros estão aumentando: eles coletivamente acumularam mais de US $ 25 bilhões em lucro líquido no primeiro trimestre de 2017. A Amazon captura metade de todos os dólares gastos on-line nos Estados Unidos. Google e Facebook foram responsáveis por quase todo o crescimento da receita de publicidade digital na América no ano passado.

Considerando o ranking mundial em 2019, pouca coisa mudou. É interessante perceber como os dados seguem sendo o recurso mais valioso do mundo. A forma como os dados são usados para influenciar pessoas e gerar lucro, trouxe à tona algumas questões éticas que influenciaram diversos países a criar novas legislações que abraçassem a questão do direito à privacidade.

Em 2015, uma empresa chamada *Cambridge Analytica* acessou sem o consentimento, os dados de cinquenta milhões de pessoas nos Estados Unidos. Esses dados foram usados para construir um sistema que direcionava anúncios políticos personalizados, o que influenciou as eleições presidenciais (CADWALLADR, GRAHAM-HARRISON, 2018).

As mesmas empresas que lucram bilhões de dólares com dados, também são as principais protagonistas nos escândalos noticiados no mundo todo. Vazamento de dados e uso indevido das informações. Ainda assim, é evidente a importância da coleta e tratamento de dados. Empresas conseguem oferecer experiências personalizadas, desenvolvendo seu modelo de negócio baseado em dados.

Uma pesquisa do MIT (*MassachusetsInstituteof Technology*) destacou que apenas quatro movimentações de cartão de crédito são suficientes para identificar quem é o comprador, o que é extremamente preocupante. A mesma pesquisa, porém, aponta as excelentes melhorias amplamente conhecidas e utilizadas que são advindas da análise de dados (MONTJOYE et al.2015, tradução nossa).

> Novos campos, como ciências sociais computacionais contam com metadados para abordar questões cruciais, como combater a malária, estudar a disseminação de informações ou monitorar a pobreza. Os mesmos conjuntos de dados de metadados também são usados por organizações e governos. Por exemplo, a Netflix usa padrões de exibição para recomendar filmes, enquanto o Google usa dados de localização para fornecer informações de trânsito em tempo real, permitindo que os motoristas reduzam o consumo de combustível e o tempo gasto em viagens.

Fica claro então que os dados são valiosos para as empresas, porém esses dados muitas vezes são armazenados sem a devida segurança ou, num cenário muito pior, são negociados entre empresas para fins escusos.

O objetivo da LGPD é justamente legislar sobre a segurança e privacidade de dados; regulamentar e fiscalizar a forma como as empresas coletam, armazenam e utilizam os dados coletados.

Esse tema ganhou foco quando o Brasil demonstrou interesse em ingressar na OCDE – Organização para a Cooperação e Desenvolvimento Econômico. A relação entre o ingresso do país no que é chamado de “clube de países ricos e a criação da lei, é clara, pois a segurança dos dados é um dos requisitos. O site da entidade Organização para a Cooperação e Desenvolvimento Econômico (OCDE, 2019) destaca:

> O Brasil expressou oficialmente seu interesse em se tornar um membro em maio de 2017. Desde então, o país intensificou ainda mais sua cooperação com a OCDE, convergindo para os padrões da Organização e buscando ampliar sua participação nos diferentes órgãos da OCDE.

O mercado internacional vê com bons olhos países que tenham interesse pela proteção de dados dos seus cidadãos, o que pode facilitar as negociações entre as nações que já possuem leis específicas.

Não é apenas a Europa que possui legislação sobre tratamento de dados; comparado com os países vizinhos na América Latina, o Brasil também está atrasado. A Argentina possui leis específicas de proteção desde 1994, o Chile, desde 1999 (PAIXÃO, 2018).

Foi lançando um olhar para as leis vigentes internacionalmente, que o Brasil criou

a Lei nº 13.709/2018. A maior influência foi a *General Data Protection Regulation*, mais conhecida por sua sigla GDPR. A GDPR, por sua vez, utilizou como referência a ISO27000, também a Cobit e Itil como explica Marinho (2019) em seu artigo "A adequação da LGPD nas empresas":

> [...] a GDPR utilizou referências conhecidas e consolidadas, como a ISO27000, Cobit e Itil, para comentar as mais conhecidas. A LGPD é verdadeiramente baseada na GDPR e seu objetivo é o mesmo, apesar das mudanças que foram requeridas para ser aprovada no Brasil, com força de uma Lei, necessária para ser implementada e cobrada (tanto pelo aspecto de exigida, quanto de penalidade).

Criar uma regulamentação específica aproxima o Brasil dos países ricos pois ajuda a conseguir credibilidade internacional e consequentemente atrair investimentos.

3 PRINCIPAIS CONCEITOS

Para a compreensão da lei e dos textos que a ela se referem, é importante assimilar alguns conceitos, vamos a eles:

- Dados Pessoais

São informações relativas a uma pessoa identificada ou identificável. Uma pessoa identificável é aquela que pode ser identificada, seja por dados de identificação, dados de localização, identidade genética, etc.

- Dados Pessoais Sensíveis

São dados pessoais referentes à etnia ou origem racial, convicção religiosa, opinião política, filiação a sindicato ou a organização religiosa, filosófica ou política, dados referentes à saúde, vida sexual, dado genético ou biométrico.

Segundo Paludetto e Barbieri (2019), mentiras ou dados incorretos sobre uma pessoa também são dados pessoais, e o meio onde a informação está contida é irrelevante, isto é; informações em forma de texto, foto, vídeo, áudio ou qualquer outro meio possível se enquadra na nova lei.

- Dados Anonimizados

Um dado pessoal pode deixar de ser protegido pela lei caso seja anonimizado, com a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação direta ou indireta a um indivíduo". (art. 5º, III e XI).

- Processamento ou Tratamento de Dados

Essa é a definição mais abrangente de toda a lei, o processamento significa qualquer operação ou conjunto de operações efetuadas em dados pessoais, por meio de meios automatizados ou não, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, utilização divulgação por transmissão, disseminação ou de outra forma tornar disponível, alinhamento ou combinação, restrição apagamento ou destruição (BRASIL, 2018).

Exatamente por ter essa definição extremamente abrangente, todas as operações envolvendo dados de terceiros se enquadram na lei.

3.1 **PRINCIPIOS**

A Lei Geral de proteção de dados traz uma série de princípios nos quais todos devem se basear para realizar o tratamento de dados pessoais, são eles:

- Princípio da Finalidade:
- “Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”. (BRASIL, 2018). Ou seja, tanto a coleta quanto o tratamento dos dados precisa ser claro e explicado ao titular, que deve consentir esse processamento. Nenhum tratamento diferente do acordado poderá ser realizado.
- Princípio da Adequação:
- Esse princípio trata do contexto sob o qual o titular consentiu o tratamento dos dados, ou seja, a compatibilidade do tratamento de acordo com a finalidade informada ao titular.
- Princípio da Necessidade:
- Trata da limitação do tratamento e da coleta dos dados ao mínimo necessário para a finalidade. Ou seja, não será permitida a coleta de dados excessivos que não condizem com a finalidade.
- Princípio do Livre Acesso:
- Esse princípio garante aos titulares a consulta facilitada e gratuita sobre como seus dados estão sendo tratados, por quanto tempo e por qual finalidade.
- Princípio da Qualidade dos Dados:
- Esse princípio trata da exatidão dos dados, clareza sobre atualização e relevância de acordo com a necessidade e a finalidade para os quais os dados foram coletados.
- Princípio da transparência:
- Garante que as informações sejam claras, precisas e de fácil acesso pelos titulares dos dados.
- Princípio da segurança:

- Exige que os dados sejam armazenados de forma segura, utilizando técnicas diversas para que os dados pessoais não sejam indevidamente acessados.
- Princípio da Prevenção:
- Trata sobre a adoção de medidas para prevenir danos decorrentes do tratamento de dados pessoais.
- Princípio da não discriminação:
- Limita o tratamento de dados pessoais, impedindo o tratamento para fins discriminatórios, ilícitos ou abusivos.
- Princípio da responsabilização e prestação de contas:
- As empresas terão que demonstrar que adotaram as medidas eficazes para cumprir todas normas para proteger os dados pessoais e comprovar a eficácia dessas medidas adotadas.

3.2 NOVOS PAPÉIS E SUAS RESPONSABILIDADES

Com a lei, surgiram novos agentes responsáveis pelo tratamento de dados nas empresas: o operador e o controlador.

A lei define em seu artigo 5º que o controlador é uma pessoa física ou jurídica de direito público ou privado responsável pela tomada de decisão sobre o tratamento de dados pessoais numa determinada empresa. Já o operador é a pessoa física ou jurídica, de direito público ou privado, que é responsável pela realização dos tratamentos de dados pessoais conforme as decisões do controlador.

A diferença entre o controlador e o operador é o poder de decisão. Enquanto o controlador possui mais responsabilidades e precisa estar atento a qualquer mudança da lei, além de entender todo o fluxo de coleta e tratamento de dados pessoais de uma determinada empresa para tomar as decisões sobre os processos, o operador precisa apenas cumprir as ordens do controlador.

Como explica Ventura (2019) em seu artigo “LGPD: Eu sou um operador ou um controlador de dados?”:

> [...] controladores serão as empresas de setores da economia que lidam diretamente com o consumidor. É o caso dos bancos, supermercados, seguradoras e outros. Já as empresas que terceirizam esse tipo de relacionamento, caso das empresas de *contact centers*, elas se apresentam como operadoras de dados.

A forma de se posicionar no mercado definirá a estratégia que será usada em cada empresa. A gestão transparente dos dados poderá ser um diferencial em breve. “Você vai saber exatamente como coletar e tratar esses dados para sua atividade, é uma forma de criar segurança jurídica para as empresas”. (GONÇALVES apud MARRONE, 2019).

Além do controlador e do operador, a lei define o papel do encarregado; conforme cito: “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)” (BRASIL, 2018).

O encarregado deverá ser uma pessoa natural, porém pode ser um papel atribuído a alguém da própria equipe, ou terceirizado.

Assim como aconteceu na Europa, com essa nova realidade à qual as empresas precisam se adaptar, nasceu a demanda por especialistas.

No Brasil, além de já possuirmos profissionais certificados para trabalhar nas empresas que atendem o mercado europeu, agora há um crescente número de cursos a fim de preparar os profissionais que serão os especialistas nas empresas. Essas certificações não exige uma formação acadêmica específica, mas os empresários irão procurar por profissionais de tecnologia com conhecimento na lei.

O movimento foi intenso na Europa e fez surgir um novo mercado, de acordo com Soprana (2018), o conceito de DPO (Data Protection Officer) como serviço é bastante presente e consiste na criação de empresas especializadas em prestar consultoria para adequação à lei. A tendência é que o Brasil siga esse mesmo modelo.

Fazendo uma análise dos princípios e tendo claros os principais conceitos e dos novos papéis que estarão intimamente ligados à aplicação da lei, podemos traçar o passo a passo que as empresas terão que realizar para adequarem-se.

4 PASSO A PASSO PARA ADEQUAÇÃO

A combinação entre dois principais passos, conhecer a lei e revisar processos, levará o empresário a encontrar o caminho para adequação.

Começando com um mapeamento sobre qual setor da empresa utiliza quais dados, por que esses dados são utilizados e por quanto tempo ficam armazenados.

Em seguida identificar se esses dados são transferidos entre as pessoas, de que forma ocorre essa transmissão e quais pessoas tem acesso.

Com esses passos iniciais será possível determinar a quais riscos a empresa está vulnerável. É necessário fazer esse levantamento, pois as ações podem variar dependendo do ramo de atuação da empresa e os dados por ela tratados. “Para uma pequena padaria, por exemplo, não vai ser tão desafiador quanto para uma startup que faz uso de big data”. (MARTINS apud CHAVES, 2019).

Para ajudar a identificar esses pontos e o definir o quão crítico é cada caso, é aconselhável a criação de um time multidisciplinar. O trabalho em conjunto de uma pessoa do setor jurídico, uma pessoa da área de T.I. que tenha pleno domínio sobre segurança da informação, uma pessoa da área de *compliance*[1]; lembrando que todas essas pessoas podem ser funcionários internos ou terceirizados.

Caso a empresa opte por terceirizar, o ideal é possuir pelo menos uma pessoa interna que será o líder do projeto; essa pessoa precisa ter aptidão técnica e conhecimento do projeto, além de ter autonomia para interagir com os terceirizados sobre as propostas de soluções para a adequação à lei.

Após essa definição inicial, a necessidade é de mapeamento. A revisão de todos os contratos que a empresa possui, isso porque a lei determina que a responsabilidade é compartilhada. Isso significa que todas as empresas que compartilham dados precisam estar adequadas, e cada empresa precisa se certificar de que as demais empresas com as quais se relaciona estão tratando os dados de acordo com as novas regras.

Todos os contratos revisados, é o momento de implantar os processos que farão com que a lei seja cumprida, ou seja, adequar os processos da empresa para atender aos direitos do usuário. A equipe multidisciplinar tem muita importância nessa adequação,

[1] *Compliance trata de certificar-se que a empresa está agindo de acordo com a lei e com possíveis órgãos regulamentadores, garantindo a transparência da empresa e de seus processos.*

pois o entendimento da lei e também o conhecimento de técnicas para construir um ambiente seguro são os principais alicerces para essa estruturação.

Analisando cada um dos direitos do consumidor é possível identificar se a empresa já está adequada, caso não esteja, inicia-se a definição de como realizará a adequação. Por exemplo: É raro uma empresa possuir um processo de portabilidade de dados, porém, a portabilidade de dados é um direito do consumidor previsto pela lei. Portanto, não apenas criar uma forma de realizar essa portabilidade fará com que uma empresa esteja adequada, mas criar uma forma de portabilidade que seja segura, rápida e simples, como destaca o artigo 11, parágrafo 4°, inciso, I da Lei n 13.709/18. Será necessário garantir que só quem vai conseguir exportar os dados é o próprio usuário, também que a exportação seja realizada dentro do prazo previsto no seu SLA (*Service Level Agreement*), que esse prazo seja razoável, e, por fim, garantir que os dados exportados sejam entregues ao usuário de uma forma simples, que ele consiga importar em outras plataformas ou que ele consiga abrir o arquivo e conferir os dados que estão contidos nele.

Outro ponto importante, é a definição de como serão realizados os avisos caso haja alguma ocorrência de falha de segurança e vazamento de dados. A lei, em seu artigo 46, especifica que o dono do dado tem o direito de ser avisado sobre qualquer ocorrência. Portanto, será necessário criar um sistema de monitoramento e também um canal de comunicação efetivo com os usuários.

Já existem no mercado alguns seguros para proteger as empresas em situações de vazamentos ou roubo de dados; o que indica que provavelmente esse item da lei já tem sido fortemente avaliado e levado em consideração, principalmente por ser o que vai entregar as falhas das empresas que não estão adequadas, gerando multas de valores consideráveis.

Dentro dos itens regulatórios que todas as empresas terão que atender, aquele que é tecnicamente mais complexo é o Direito de Esquecimento. Existe um antagonismo, se por um lado o cliente tem o direito de pedir para ser esquecido (leia-se: ter seus dados esquecidos pela empresa), por outro lado, cada ramo tem outras leis às quais precisa atender; por exemplo, uma transação financeira, dependendo da sua natureza, precisa ter seus dados disponíveis para uma eventual auditoria num prazo de até 15 anos.

É necessário então analisar os requisitos regulatórios de cada mercado, pois eles variam muito, e definir uma forma de atender a regulamentação de armazenamento dos dados para fins de auditoria fiscal, por exemplo, e também atender a lei geral de proteção

de dados. Montar uma estratégia técnica que equilibre a ambas necessidades. Não é uma “receita de bolo”, cada caso precisa ser estudado.

Um outro complicador para atender a lei, é que não basta a empresa apagar os dados internamente; será necessário mapear todos os fornecedores que tiveram acesso àqueles dados e eles precisam ser apagados em toda a cadeia.

4.1 SEGURANÇA DA INFORMAÇÃO

No que diz respeito à segurança da informação, é primordial que as empresas comecem a tomar decisões de maneira que contemple as boas práticas que muito comumente são negligenciadas.

Para isso, a atenção precisa estar voltada à alguns elementos, como:

- Segmentação das permissões de acesso

É muito comum que em empresas muitas pessoas tenham acesso à integralidade dos dados, mesmo que esses dados não sejam pertinentes para a execução da atividade desses funcionários. Também é comum que esses dados possam ser coletados pelos funcionários e tratados em um computador local ou em uma rede não segura. Uma boa parte dos possíveis problemas de segurança da informação já pode ser resolvido caso a empresa faça uma boa limitação de permissões e acessos às informações.

- Testes de penetração e vulnerabilidade

Executar testes de vulnerabilidade em todos os sistemas utilizados pela empresa e no ambiente de rede. Com esses testes, é possível saber os riscos e tomar as devidas providências. Existem empresas especializadas na realização desses testes. É fortemente recomendado que se faça testes de penetração, por melhor que sejam os profissionais de TI de uma empresa, dificilmente haverá um ambiente cem por cento seguro.

- Monitoramento de acessos ao sistema

Diversos serviços de computação na nuvem possuem ferramentas de monitoramento de acesso, muitas vezes esses serviços estão desligados ou são subestimados; utilizar essas ferramentas disponíveis facilitará o entendimento do cenário da empresa e ajudará na tomada de decisão de possíveis providências. Implementar alarmes automatizados que avisem sobre acessos indevidos ou tentativas de acesso também é uma boa forma de se precaver de ataques. É necessário estar atento o tempo todo.

Trabalhar com banco de dados criptografados, discos criptografados, software de criptografia, etc., garante que, mesmo que haja uma invasão, os dados coletados não serão legíveis. Essa prática se tornará cada vez mais comum, principalmente quando se tratar de dados sensíveis, isso fará com que a chance de um vazamento ou uma interceptação dos dados causar um transtorno considerável será significativamente reduzido. Conforme esclarecido pelo presidente do Instituto Goiano de Direito Digital, Rafael Fernandes Maciel:

> No juízo de gravidade a autoridade também analisará eventuais medidas técnicas adequadas que tornem os dados pessoais ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los. É o caso, por exemplo, de se criptografar os dados pessoais, sobretudo senhas, de forma que um vazamento em nada poderá acarretar danos, já que os dados serão inúteis a quem acessar.

- Ter certeza da legalidade da origem dos dados

Não bastam os elementos técnicos, é preciso se certificar que os dados que estão sendo tratados na empresa não tenham sido adquiridos de maneira indevida. Guardar o aceite de uso dos dados feito pelo usuário ou cliente também é primordial para garantir que a empresa está agindo em acordo com a lei.

Estabelecendo essas políticas, a empresa estará resguardada, pois demonstrará o comprometimento em aplicar as boas práticas de segurança da informação; ainda assim, certamente haverá que observar todos os critérios com regularidade e realizar adaptações conforme pontos de vulnerabilidade forem identificados.

5 OS NOVOS DIREITOS DOS TITULARES DOS DADOS

A Lei Geral de Proteção de Dados Pessoais possui 5 artigos que tratam dos direitos do titular dos dados. Os titulares dos dados, podem ser apenas pessoas naturais, portanto não fazem parte do escopo da lei as pessoas jurídicas. Os direitos dos titulares estão intimamente relacionados aos deveres das empresas e às formas de adequação citadas anteriormente.

O primeiro artigo que trata dos direitos, o artigo 17, fala sobre os direitos fundamentais de liberdade, intimidade e privacidade. De modo geral, é disso que se trata toda a LGPD. De acordo com Pinheiro, 2019, essa garantia reflete a própria Constituição Federal e o Código Civil:

> É possível relacionar essa garantia da pessoa natural à titularidade de seus dados à inviolabilidade de sua vida privada, pontuada por meio do art. 5°, X11, da Constituição Federal e do art. 21 do Código Civil, haja vista que as informações pessoais da pessoa fazem parte de sua privacidade, ainda mais no contexto digital.

O artigo 18 determina as solicitações que o titular dos dados pode fazer ao controlador; são elas:

- Confirmação da existência do tratamento de dados.
- Acesso aos dados armazenados pelo controlador.
- Correção dos dados que estejam desatualizados, incompletos ou inexatos.
- Anonimização ou eliminação dos dados que tenham sido coletados excessivamente, ou que tenham sido tratados em desconformidade com a lei.
- Portabilidade dos dados a outro fornecedor.
- Eliminação dos dados pessoais tratados, exceto nas hipóteses já previstas no artigo 16.
- Revelação de todas as entidades públicas ou privadas com as quais os dados foram compartilhados.
- Informações sobre a possibilidade de não fornecer consentimento para o tratamento de seus dados e as possíveis consequências.
- Revogação do consentimento concedido anteriormente.

É esperado que o cidadão brasileiro demore um tempo para se familiarizar com esses conceitos e direitos que estão sendo adquiridos com a vigência dessa lei. Assim como diversos direitos pouco conhecidos da população, é comum que apenas uma parcela das pessoas exija um tratamento adequado e saiba reconhecer quando há uma contravenção envolvendo seus dados. Já as empresas, precisam reconhecer seus deveres imediatamente para tomar todas as medidas necessárias para adequação e evitar as multas.

A aplicabilidade da lei, no longo prazo, mudará conceitos e a cultura do brasileiro, que ficará mais exigente quanto ao tratamento dos seus dados e sua privacidade.

6 TERMO DE CONSENTIMENTO E TERMO DE COMPROMISSO

Para que uma empresa possa realizar o tratamento dos dados de uma pessoa, será necessário o consentimento da mesma, como já citado anteriormente, a forma de conceder a permissão de tratamento dos dados deve ser clara e pertinente para o negócio. Coleta e tratamento de dados que não possuem relação com a natureza do negócio já será considerada uma infração.

O consentimento, considerado a grande solução para o tratamento dos dados pessoais, deve ter na verdade um cuidado muito grande por parte do controlador, pois deve obedecer a algumas regras. Os requisitos principais, são os já destacados neste artigo, como por exemplo a finalidade, não se deve solicitar consentimento para coletar um dado que foge do mínimo necessário para a realização da transação.

Muitos consentimentos são genéricos, não especificam a finalidade, outros utilizam as *checkbox* que já são pré marcadas e podem induzir o titular dos dados a consentir acesso aos seus dados erroneamente. Em todos esses casos, o consentimento poderá ser anulado. A forma correta, como prevê a lei, especifica que o consentimento precisa ser uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (artigo 5, inciso XII).

Ao solicitar a autorização de forma correta, o controlador também deve assegurar-se de que possui forma de garantir e provar, caso necessário, que agiu de acordo com a lei; isso porque, cabe a ele o ônus da prova.

Existem, claro, outras formas legais de realizar o tratamento de dados pessoais, todas elas especificadas na lei, no seu artigo 7. O consentimento é apenas uma das formas, as demais são:

- Para cumprimento de obrigação legal pelo controlador (como já mencionado anteriormente).
- Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.
- Para a realização de estudos por órgãos de pesquisa, garantida, sempre que possível a anonimização dos dados pessoais.

- Quando necessário para execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.
- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral.
- Para a proteção da vida ou da incolumidade física do titular ou de terceiro.
- Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.
- Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
- Para a proteção do crédito.

7 MULTAS E SANÇÕES APLICADAS EM CASO DE NÃO CUMPRIMENTO DA LEI

A LGPD é inspirada na GDPR, que por sua vez possui um histórico de multas de altíssimo valor; já para a nova lei, estão previstas consequências das mais brandas às mais rígidas, algumas, com valor estipulado sobre o faturamento da empresa; outras, cujo prejuízo não é possível estimar.

A advertência, na qual constará um prazo para adequação é a punição mais branda. Outra punição é a multa de 2% (dois por cento) do último faturamento anual da empresa, com limite em R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

Outras punições como publicização da infração após devida confirmação da ocorrência, bloqueio e/ou eliminação dos dados pessoais a que se refere a infração até a sua regulamentação, são mais incalculáveis; pois podem causar um grande transtorno e fazer com que a reputação da empresa seja colocada em xeque.

Perder a confiança do consumidor, nesses casos envolvendo o tratamento de dados pessoais, pode facilmente levar uma grande empresa a falência, uma vez que sem a confiança do público, não haverá clientela, e, há que se considerar que os clientes prejudicados também poderão entrar com ação indenizatórias pelo vazamento dos seus dados.

Também é importante atentar-se ao fato de que o inciso segundo da lei, define um teto por infração, mas como bem observa Maciel, em uma mesma denúncia podem ser apuradas diversas infrações:

> Por exemplo, um incidente de vazamento de dados em que, no decorrer do procedimento, seja apurado que também havia um tratamento de dados pessoais excessivo ou desproporcional. Poderá haver uma infração pelo incidente e outra pela ilicitude do tratamento. Ainda, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

Como já citado anteriormente, uma empresa que fizer o que está dentro do seu alcance para evitar um vazamento de dados, por exemplo, poderá ter sua pena abrandada, assim como uma empresa que claramente agir de má fé, poderá ter sua pena

agravada. Essas definições também constam na lei e merecem ser consideradas. A lei define as formas de avaliar a gradação das sanções, são elas:

I. A gravidade e a natureza das infrações e dos direitos pessoais afetados.
II. A boa-fé do infrator.
III. A vantagem auferida ou pretendida pelo infrator.
IV. A condição econômica do infrator.
V. A reincidência.
VI. O grau do dano.
VII. A cooperação do infrator.
VIII. A adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei.
IX. A adoção de política de boas práticas e governança.
X. A pronta adoção de medidas corretivas.
XI. A proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Com essas possibilidades devidamente mapeadas pela aplicabilidade da nova lei, é possível perceber que são diversos os fatores que podem influenciar o valor da multa que será aplicado no caso de uma contravenção. Portanto, buscar todos os mecanismos técnicos possíveis para adequação à lei, além de trazer adequação da empresa, também pode ajudar a garantir uma pena mais branda no caso de algum vazamento de dado.

8 CONCLUSÃO

A mudança de cultura, assim como a adequação às normas que uma nova lei apresenta, não acontece de uma hora para outra. Haverá ainda um período onde as empresas, principalmente as pequenas, não terão conhecimento das boas práticas para tratamento de dados, assim como os donos dos dados não terão ciência de que existe uma lei que os protege. É absolutamente natural que isso ocorra, o tempo e os exemplos (de empresas que serão multadas por não se adequarem) farão o trabalho de popularizar essa nova realidade.

Ambos os lados saem ganhando, empresas e titulares de dados: As empresas com uma nova experiência em segurança da informação, na coleta e tratamento de dados de forma responsável; já os titulares de dados ganham com a garantia de que suas informações serão tratadas com respeito e de forma adequada. Claro que é necessário considerar que nesse novo cenário, apenas um lado tem o ônus de investir tempo e recursos financeiros, comprando tecnologia e contratando pessoas, para conseguir manter-se dentro da lei.

A adaptação das empresas que possuem seus negócios pautados em dados são as que devem estar mais preocupadas em investir em formas de garantir a segurança e o tratamento adequado dos dados.

Ainda é cedo para saber como essa novidade será recebida pela população em geral. Há poucos livros sobre esse tema, todo o trabalho de previsão a respeito das consequências, multas, negócios gerados e negócios fechados são baseados na experiência europeia.

Aos titulares dos dados, resta esperar e ficar atento à todas as empresas que solicitam dados. Às empresas, resta investir o máximo possível para cumprir o que a lei determina, criando novos hábitos e boas práticas.

9 REFERÊNCIAS

BRASIL. Câmara dos Deputados. Centro de documentação e Informação.**Lei Geral de Proteção de Dados Pessoais**. Brasília, 14 ago. 2018. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156212-pl.html. Acessado em: 08 Nov. 2019.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian.** Londres, p. 0-1. 17 mar. 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 08 nov. 2019.

GIL, A. C. **Como elaborar projetos de pesquisa**. 3. ed. São Paulo: Atlas, 1994.

GONÇALVES, MARRONE. **A LGPD Chegou: sua empresa está preparada para a regulação?** 2018. Disponível em <https://www.consumidormoderno.com.br/2019/04/25/lgpd-chegou-sua-empresa-esta-preparada-para-regulacao/>. Acessado em 03 abril 2020.

LÜDKE, M.; ANDRÉ, M.E.D.A. **Pesquisaem educação:** abordagens qualitativas. São Paulo, EPU, 1986.
MACIEL, Rafael. Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18 . RM Digital Education. Edição do Kindle.

MARINHO, Fernando. **A adequação da LGPD nas empresas.** 2019. Disponível em: https://www.linkedin.com/pulse/adequa%C3%A7%C3%A3o-da-lgpd-nas-empresas-fernando-marinho/. Acesso em: 01 maio 2019.

MARTINS, Danylo; CHAVES Luiz Fernando. **Pequeno empreendedor deve revisar processos.**18 nov. 2019. Disponível em: <https://www.daniel-ip.com/wp-content/uploads/2019/12/mat%C3%A9ria-Valor_.pdf>. Acesso em 21 abril 2020.

MONTJOYE, Yves-alexandre de et al. **Unique in the shopping mall: On the reidentifiability of credit card metadata**. **Science**, Washington, Dc, v. 347, n. 6221, p.536-539, 30 jan. 2015. Disponível em: https://science.sciencemag.org/content/347/6221/536. Acesso em: 12 Nov. 2019.

OECD. **Brasil: Uma cooperação mutuamente benéfica**. Disponível em http://www.oecd.org/latin-america/countries/brazil/brasil.htm. Acesso em 11 Nov. 2019.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais Comentários à Lei n. 13.709/2018 LGPD** (Locais do Kindle 1075-1080). Saraiva Educação. Edição do Kindle.

PAIXÃO, Pedro. **Proteção de Dados na América Latina. 2018. Disponível em:** https://cio.com.br/protecao-de-dados-na-america-latina/. Acesso em: 21 Nov. 2019.
SERPRO. **Os 10 princípios para um efetivo tratamento de dados, segundo a Lei Geral de Proteção de Dados Pessoais**. Disponível em https://www.serpro.gov.br/lgpd/menu/arquivos/os-10-principios-para-um-efetivo-tratamento-de-dados/view. Acessado em 21 Nov. 2019

THE ECONOMIST. **O recurso mais valioso do mundo não é mais petróleo, mas dados: Regulando os gigantes da Internet**. **The Economist.** Londres,06 maio 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 08 nov. 2019.

SOPRANA, Paula. **Cresce demanda por especialistas em privacidade.** 16 set. 2018**.** Disponível em **<**https://www1.folha.uol.com.br/mercado/2018/09/cresce-demanda-por-especialistas-em-privacidade.shtml>. Acesso em 11 abril 2020.