A RESPONSABILIDADE DAS EMPRESAS EM FACE À LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Stéfany Barrueco
Discente do Curso de Direito da Faculdade da Alta Paulista (FAP)
Juliana Ortiz Minichiello Palu
Docente do Curso de Direito da Faculdade da Alta Paulista (FAP) - Tupã

Com os avanços tecnológicos, os dados pessoais se tornaram um ativo de importância intangível, pois a sociedade está cada vez mais conectada, e, assim, as informações pessoais passam a ter valor único para as empresas, onde segurança e confidencialidade geram alto valor para a carga informacional. Desta forma, surge a seguinte questão: qual a responsabilidade legal das empresas da proteção de dados de seus clientes em face a LGPD? Resolver esse dilema é o objeto deste trabalho.

A Lei Geral de Proteção de Dados, ou LGPD, ainda Lei nº 13.709 de 14 de agosto de 2018, define-se como um conjunto de regras jurídicas para coleta, armazenamento e manipulação de dados por quaisquer organizações públicas, privadas e por pessoas físicas, após um minucioso processo de criação.

A LGPD abarca, em seus intentos, a regulamentação, e fiscalização da utilização dos dados recolhidos, tratados e armazenados por estas pessoas, trazendo ao titular dos dados maior segurança no tocante à privacidade

Em seu artigo 5º, temos que os dados são denominados como

pessoais sensíveis sendo que o primeiro é o que consegue identificar ou tornar uma pessoa identificável e o segundo aqueles que versam sobre a religião, filosofia, política e orientação sexual, dado genético, quando vinculado a uma pessoa natural.

A LGPD tende a causar grande impacto em território nacional, visto que milhões de empresas e pessoas físicas, a fim de desenvolverem suas atividades econômicas, tratam dados pessoais e, por consequência disso deverão a elas se adequarem.

A LGPD, em seus artigos 42 a 45, estabelece as regras relativas à responsabilidade civil dos agentes de processamento de dados pessoais, trazendo à tona o debate sobre a natureza da obrigação de indenizar, se subjetivamente - fundada na inexistência de dever de conduta imposto no agente de tratamento - ou objetivamente - com base no risco da atividade desenvolvida.

A LGPD é considerada - especialmente pelos profissionais do Direito Digital - um marco muito importante para a defesa da privacidade no Brasil, impactando os mais diversos setores e organizações. Dada a sua relevância e por se tratar de uma lei relativamente nova, é importante que alguns aspectos sejam estudados com maior profundidade.

Com toda uma nova regulamentação, faz-se também necessário entender os conceitos a ela atrelados, os bens jurídicos sobre os quais a lei exerce tutela, quem são os responsáveis e quem tem competência para regulamentar, fiscalizar e aplicar sanções, caso seja constatado o seu descumprimento.

A pesquisa também se baseou em textos doutrinários e

legislativos, principalmente na própria Lei Geral de Proteção de Dados Pessoais, Lei n. 13.709 de 14 de agosto de 2018.

A Lei Geral de Proteção de Dados, mais conhecida como LGPD, foi instituída pela Lei n. 13.709, de 14 de agosto de 2018 e entrou em vigor em agosto de 2020, com o objetivo de promover a proteção dos dados pessoais, devendo ser respeitada por pessoas físicas e pessoas jurídicas de direito público ou privado que com dados pessoais obtenha proveito econômico.

A proteção de dados se baseia nos fundamentos trazidos pela própria LGPD, em seu artigo 2º, conforme destacado a seguir:

> A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;
> e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018).

Dessa forma, a LGPD apresenta regras sobre a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, aumentando sua proteção e impondo penalidades significativas em caso de seu descumprimento.

Para entender mais claramente, a LGPD garante o direito constitucional à privacidade, pois com os avanços tecnológicos, em

muitas situações, esses direitos acabam sendo violados em ataques a bancos de dados digitais e outras informações.

Sobre o direito à privacidade, Maciel (2019, p. 7) diz que:

> Em 1824, a Constituição do Império reconhecia um certo direito à privacidade, ao proteger o "segredo da carta" e a "inviolabilidade da casa". No entanto, naquele momento, a privacidade estava submetida a um conceito mais lastreado na propriedade, ou seja, a carta magna protegia o meio físico e não o conteúdo em si. Por isso, vê-se apenas referência ao sigilo da correspondência e à inviolabilidade do domicílio. Perceba-se que não há uma proteção da privacidade por si só, pelo seu conteúdo ou por um aspecto mais subjetivo. O que se protegia ali era a invasão, o ato de romper barreiras físicas.

No Brasil, a legislação que visa garantir a proteção de dados não surgiu de forma aleatória, tendo como impulso o Marco Civil da Internet, dando início a uma gama de novas palavras que passaram a fazer parte do vocabulário das questões jurídicas relacionadas aos sistemas de proteção de dados. O Marco Civil da Internet inaugurou uma nova era no Brasil.

> Foi com o Marco Civil da Internet que o Brasil passou a constar em seu sistema jurídico a palavra "privacidade". Embora curioso, esse fato nada inova, já que "vida privada", no frigir dos ovos, possui o mesmo sentido. Com o MCI entrando em vigor em 2014, a internet no Brasil passou a ser mais bem disciplinada, prevendo como princípios a proteção da privacidade e dos dados pessoais (art. 3º), bem como garantindo aos usuários, dentre outros, os seguintes direitos (art. 7º):
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante

> consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação;
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet.
> X - Exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; (MACIEL, 2019, p. 13).

Essa necessidade de regulamentação de proteção de dados não é exclusividade brasileira. Nos países europeus, já é uma realidade, pois também contam com uma legislação específica para tratar de questões relacionadas à proteção de dados e informações, a GDPR. Este novo perfil de legislação visa garantir a integridade dos dados e a personalidade de cada indivíduo, utilizando um sistema regulatório muito semelhante ao europeu.

A LGPD se aplica a todas as operações de processamento de dados pessoais realizadas no Brasil com a finalidade de oferta de bens, serviços ou processamento de dados de pessoas físicas localizadas no próprio país.

Do ponto de vista econômico, os dados importam na medida em que podem ser convertidos em informações necessárias ou úteis para a atividade econômica. Consequentemente, os dados precisam ser processados para que possam gerar valor. Só para se ter uma dimensão do risco para os usuários, o professor especialista Martin Hilbert

afirma que com 150 “curtidas”, certos algoritmos podem saber mais sobre uma pessoa do que seu companheiro e que, com 250 “curtidas”, algoritmos podem saber mais sobre uma pessoa do que ele mesmo. (FRAZÃO, TEPEDINO e OLIVA, 2019)

Os dados pessoais têm sido utilizados por governos e grandes atores econômicos para criar o que se chama de espelho unidirecional, permitindo que tais agentes saibam tudo sobre os cidadãos, enquanto nada sabem sobre os primeiros. Tudo isso acontece por meio de monitoramento e vigilância constante sobre cada passo da vida das pessoas, o que leva a um verdadeiro capitalismo de vigilância, cuja principal consequência é a constituição de uma sociedade de vigilância. (PASQUALEOS, 2015 apud TEPEDINO, 2019, p. 10)

Portanto não há como entender o advento da Lei Geral de Proteção de Dados – LGPD a não ser no contexto descrito, que destaca seu importante papel no reforço da autonomia informacional dos dados titulares de dados e o necessário e devido controle que eles precisam exercer sobre essas informações, a fim de se frear as adversidades que permitiram consolidar o atual estágio da economia baseada em dados.

A LGPD não se restringe ao ambiente virtual, mas a todos os meios pelos quais os dados podem ser coletados e utilizados. No entanto, também não há dúvidas de que é no ambiente virtual que se concentram as maiores preocupações e os maiores desafios da proteção de dados.

Segundo Frazão, Tepedino e Oliva (2019), o mais preocupante é que tudo isso é feito a partir de uma série de relatos que podem até parecer irrelevantes para o cidadão comum, como suas

buscas na internet, tempo gasto em redes sociais, pesquisas sobre determinados assuntos, músicas e locais de sua escolha, entre outros. É com base nesse conhecimento, posteriormente convertido em novos dados, que a inteligência artificial atua para formular um componente crítico da própria inteligência. Muito mais do que um problema de privacidade, no sentido do direito à privacidade ou a ser deixado em paz, a proteção de dados, nesse contexto, é um fundamento para a preservação da individualidade, da liberdade e da própria democracia.

Para a aplicação dessa lei, é importante analisar o conceito de dados pessoais. Segundo a LGPD (2018), considera-se dado pessoal a informação relacionada à pessoa natural, identificada ou identificável.

A definição de dados pessoais é a delimitação essencial para a proteção das informações do indivíduo, justamente, porque demarca o domínio desse direito. Esse direito pode ser mais restrito, onde limita a interpretação dos operadores do direito, ou mais amplo, permitindo a análise sob novas perspectivas. Tal análise pode ser feita uma vez que a lei se refere a "pessoa física identificada" e a "identificável", onde perfis podem ser traçados e identificados a partir de um padrão de atuação do indivíduo.

Conforme apresentado por Bernardo Menicucci Grossi, para a Comissão Especial de Proteção de Dados" da OAB de Minas Gerais: "Considera-se dado pessoal aquele que está vinculado à projeção, extensão ou dimensão de determinada pessoa, tanto em sua esfera, bem como em sua esfera relacional. (GROSSI, 2020)

O objetivo básico da Lei 13.709/2018 é regular o tratamento de dados pessoais pelos coletores de informações sobre pessoas físicas, digitalmente ou não. A captura desses dados deve seguir um

protocolo linear para a legalização de seu uso, aplicacional ou privado, com foco nestas etapas para pessoas físicas, jurídicas, públicas em meios digitais.

Conforme enumerado no artigo 5.º da referida lei, define-se como pessoal toda e qualquer informação que os dados possam conduzir à identificação da pessoa singular, ou seja, dados como nome completo, e-mail, telefone, Carteira de Identidade (RG), Cadastro de Pessoa Física (CPF) e endereço, conta bancária, além de dados indiretos, como endereços IP, geolocalização de dispositivos móveis e outros identificadores. eletrônica (BRASIL, 2018, online).

O inciso II do referido artigo define dados sensíveis como dados passíveis de uso indevido para fins discriminatórios e lesivos ao cidadão, como o acesso a informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de natureza religiosa, filosófica ou política, dados relativos à saúde ou vida sexual, dados genéticos ou biométricos quando vinculados a um pessoa ; tais informações requerem maior proteção, pois tratam de assuntos extremamente particulares e requerem o consentimento específico do titular (BRASIL, 2018, online).

Segundo Patrícia Pinheiro, os dados sensíveis merecem tratamento especial, pois em algumas situações sua utilização é imprescindível, mas deve-se garantir o cuidado, o respeito e a segurança com tais informações, haja vista que sua violação pode resultar em sua natureza, ou por suas características, a tomar riscos significativos em relação aos direitos e liberdades fundamentais da pessoa (PINHEIRO, 2018).

Seguindo a análise do artigo 5, o inciso III trata dos dados anonimizados. Esta categoria é assim denominada quando um dado pessoal deixa de estar diretamente relacionado com uma pessoa que não permite ser identificada, tendo em conta a utilização de meios para o seu tratamento. Um exemplo é em relação aos inquéritos censitários, onde os dados pessoais do entrevistado são coligidos com outros e tornam-se estatísticas; esses dados (BRASIL, 2018, online) estão fora da proteção da LGPD.

O conceito de dado pessoal sensível também é abordado no inciso II do artigo 5º da LGPD (2018):

> dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de cunho religioso, filosófico ou natureza política, dados relativos à saúde ou vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa física.

Para classificar um dado pessoal como sensível, ele deve estar presente na lista exaustiva, prevista na LGPD. Alguns dados, por mais sensíveis que sejam, só serão considerados sensíveis se estiverem incluídos nessa lista.

Entre os agentes de tratamento, temos a figura do encarregado que é o profissional que possui um nível de conhecimento jurídico e informático, em que a sua principal responsabilidade é observar, avaliar e organizar a gestão do tratamento de dados pessoais de uma determinada empresa ou entidade pública, para que se adapte ao sistema defendido pela lei. (LIMA, 2019)

A relação jurídica estabelecida entre os agentes de tratamento de dados na LGPD deve se pautar pelo princípio da boa-fé, objetiva o

que determina que todos os envolvidos colaboram entre si, para o devido cumprimento da Lei Geral de Proteção de Dados Pessoais.

No que diz respeito à responsabilidade, determina a lei que os agentes de tratamento - controlador e o operador são responsáveis pela promoção da adequação à LGPD e o encarregado, por sua vez, responde, de acordo com as regras do Direito do Trabalho, caso seja empregado, ou dos Direitos Civil e Empresarial, caso seja empresa contratada para essa finalidade. No entanto, tal responsabilidade que é do tipo solidária, está condicionada à possibilidade de quem repara o dano ao titular ter direito de regresso contra os demais responsáveis, na medida dos seus próprios (LIMA, 2019, online).

Portanto gerentes, administradores, sócios e empregados estão vinculados ao controlador e são responsáveis por todos os atos na operação de tratamento de dados. Os funcionários e outras pessoas físicas, vinculadas ao operador também atuarão em seu nome e, as consequências dos atos lesivos sofridos pelo usuário serão aplicadas judicial e administrativamente, conforme o explicitado na LGPD, em seu artigo 42.

De acordo com Vieira (2019), quando se fala em responsabilidade civil, entende-se que há uma exigência relevante de reparação de dano causado a terceiro, de forma ilícita.

Isso pode envolver dois tipos:

a) a responsabilidade contratual é aquela decorrente do trabalho resultante, que resultante da inadimplência do atraso, que pode até ser consequência da incompetência na execução de uma cláusula de compliance (VIEIRA, 2019);

b) a responsabilidade extracontratual, relativa ao dever de reparação dos danos resultantes da violação de direitos, de direitos de personalidade, por exemplo, é idêntica à violação de um direito civil. Então, o sujeito que a violar e causar dano a terceiro terá a obrigação de reparar o dano causado (VIEIRA, 2019).

Assim, o próprio Código Civil tem responsabilidade fundamentada em dois conceitos, sendo o primeiro o de ato ilícito, conforme artigo 186, e o segundo o de abuso de direito, conforme previsto no artigo 187. *In verbis:*

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito. Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes (BRASIL, CC, 2020).

Assim, começa-se a entender que, quando alguém pratica um ato em desacordo com o que diz a lei, causando dano ou prejuízo a terceiro, deve, de alguma forma, reparar o dano causado. E mais de uma pode ser a forma de reparação, como corrobora Vieira (2019, p. 29), quando afirma que:

> O ato ilícito, portanto, é aquele praticado em desacordo com a ordem jurídica que ocasiona a violação de direitos e causa prejuízos a outrem. O ato ilícito pode ser penal, administrativo ou civil bem como pode acarretar dupla ou tripla responsabilidade, por exemplo, um crime ambiental que ofende os particulares (ilícito civil), a sociedade (ilícito penal) e é passível de sanções administrativas. A consequência do ato ilícito civil é a obrigação geral de reparar o dano, disposta no caput do art. 927 do Código Civil de

> 2002. Além disso, existem situações em que se responde por terceiros, devendo existir uma conexão entre o responsável e o executor do ato. Há também a hipótese de dano causado por coisa da qual se é proprietário. Por outro lado, nos moldes do art. 187 do CC, a noção de ato ilícito foi ampliada, para considerar como ilícito aquele ato que, originalmente é lícito, mas foi exercido fora dos limites impostos pelo seu fim econômico ou social, pela boa-fé objetiva ou pelos bons costumes.

A questão da responsabilidade e indenização por danos imputados aos agentes de tratamento foi inserida na Secção III do Capítulo VI, intitulada "Dos agentes de tratamento de dados pessoais". O título do art. 42 "caput" dispõe sobre o dever de indenização civil por danos materiais, morais, individuais ou coletivos, imposta aos controladores e operadores, nas hipóteses de operações de tratamento de dados, em que haja infração à LGPD.

Conforme visto no tópico 4.1.2, a legislação de proteção de dados estabelece um conjunto de princípios e regras que buscam criar um ambiente de responsabilidade proativa, ou seja, de caráter preventivo, considerando o risco potencial de lesão na coleta e tratamento de informações, especialmente tendo em vista os riscos inerentes a uma sociedade classificadora (FRAZÃO, 2019, p. 35), e propõe um sistema de responsabilização capaz de proporcionar proteção efetiva à vítima e reparação integral do dano distribuído entre os arts. 42 a 45 da lei.

Dessa forma, conforme o que foi narrado neste trabalho conclui-se que em um mundo em que buscamos novas tecnologias, acabamos expondo nossas informações de maneira inconsciente sem

saber onde vai parar, por isso é necessário de uma lei voltada para proteção, sendo assim, poderemos utilizar nossas ferramentas com liberdade e privacidade para que os dados fornecidos não sejam expostos e utilizados por terceiros como forma de lucro e pesquisas sem o consentimento do titular dos dados.

Devido a esse fato, as empresas, precisam se adaptar na forma de coletarem os dados fornecidos pelos titulares, pois deverá seguir expressamente os ditames legais e juntamente os princípios da boa-fé, o direito à intimidade, à liberdade de expressão, à honra e à imagem.

A forma de manuseio dos dados será realizada por um processo que, após as informações serem fornecidas pelo titular, o controlador será responsável em determinar o tratamento adequado, o operador será quem realizará o tratamento dos dados em nome do controlador, por fim, o encarregado será indicado para realizar o controle da comunicação entre o controlador, titular e a Autoridade Nacional de Proteção de Dados. Todos os procedimentos estarão sendo monitorados pelo órgão fiscalizador/regulador e caso seja comprovado algum comprometimento de dados, há sanções que variam, de acordo com as infrações cometidas, que estão previstas no artigo 52 da lei.

Com essa breve análise sobre o consentimento da nova lei geral de proteção de dados, é possível compreender mais sob a forma de adequação e cuidados com que as empresas devem se adaptar ao uso de softwares atualizados e seguros, que possam monitorar o uso, a movimentação e o repouso dos dados para que impossibilite o vazamento e, consequentemente, as sanções previstas, e principalmente instruir e treinar seus funcionários e ter pessoas

especializadas da área da tecnologia que conheçam os caminhos, para que não tenha falha no sistema.

REFERÊNCIAS BIBLIOGRÁFICAS

FRAZÃO, Ana. **Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados.** In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p. 23-52

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico], coordenação. -- 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

GROSSI, Bernardo Menicucci. **Lei Geral de Proteção de Dados:** Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial [recurso eletrônico] - Porto Alegre, RS: Editora Fi, 2020.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais.** RM Digital Education. 1ª Edição. Goiânia – GO. 2019.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

VIEIRA, Victor Rodrigues Nascimento. **Lei geral de proteção de dados:** uma análise da tutela dos dados pessoais em casos de transferência internacional. 2019. 77 f. TCC (Graduação) - Curso de Direito, Universidade Federal de Uberlândia, Uberlândia, 2019. 1