DIGE - Direito Internacional e Globalização Econômica
ISSN: 2526-6284

Larissa Monaco Caranti
lmonacocaranti@gmail.com

Tatiana Lie Fukuhara
lieholanda@gmail.com

Responsabilização de Empresas à luz da Lei Geral de Proteção de Dados

Corporate liability regarding the use of data according to the brazilian data protection legislation

Larissa Monaco Caranti[1]

Tatiana Lie Fukuhara[2]

RESUMO

Neste breve trabalho, estudaremos a evolução da proteção de dados tendo como maior foco de estudo a responsabilização na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) , cujo conteúdo é de suma importância para o tratamento de dados no âmbito nacional. Não restam dúvidas de que, no cenário atual, a informação é crucial para o funcionamento das grandes e pequenas empresas, entretanto, o uso dos dados pessoais não é ilimitado. Desta forma, também analisaremos a responsabilidade no âmbito empresarial quanto à utilização dos dados.

PALAVRAS-CHAVE: Responsabilização; Empresas; LGPD

ABSTRACT

In this brief work, we will study the evolution of data protection with the main focus of study being the liability in the *Lei Geral de Proteção de Dados Pessoais* "General Law for the Protection of Personal Data" (13.709/2018), which is of paramount importance for the processing of data at the national level. There is no question that in the current scenario, information is crucial for the operation of large and small companies, however, the use of personal data is not unlimited. Therefore, we will also analyze corporate liability regarding the use of data.

KEY-WORDS: Corporate liability; data privacy; digital law.

[1] Estudante da graduação em Direito na Pontifícia Universidade Católica de São Paulo (PUC-SP). Endereço eletrônico: lmonacocaranti@gmail.com
[2] Estudante da graduação em Direito na Pontifícia Universidade Católica de São Paulo (PUC-SP). Endereço eletrônico: lieholanda@gmail.com

Larissa Monaco Caranti
lmonacocaranti@gmail.com

Tatiana Lie Fukuhara
lieholanda@gmail.com

SUMÁRIO

INTRODUÇÃO

Decorrente da criação humana, o Direito é expressão dos interesses da sociedade, o que o torna dinâmico. Em outras palavras, é imprescindível que os institutos jurídicos acompanhem a evolução social para que, de fato, sejam um reflexo da vida em determinado momento histórico, bem como garantam a segurança jurídica dos indivíduos.

O final do século XX foi marcado por drásticas mudanças no meio de produção capitalista, decorrentes da chamada Revolução Técnico-Científico-Informacional e da introdução de novas tecnologias ao mercado. A era informacional causou mudanças sociais tanto benéficas, quanto maléficas, porém, incontestavelmente profundas e rápidas, o que deu causa a situações isentas de adequada regulamentação jurídica, como a proteção de dados em um cenário em que a informação passou a ser considerada como o "novo petróleo".

A tentativa de regulamentação da proteção de dados remonta aos anos 1970, contexto histórico em que o Estado era o maior armazenador de informações, diferentemente do momento atual, em que as entidades privadas são as principais detentoras de dados. A partir da década de 70, portanto, diversos estudiosos realizaram descobertas benéficas no campo digital, todavia, em 1986, o alemão Markus Hess conseguiu hackear um portal e usou essa conexão para acessar e comprometer aproximadamente 400 computadores militares com informações

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

sensíveis, o que demonstra a face obscura do campo da segurança digital. Passados alguns anos, em 1988, Robert Morris tornou-se a primeira pessoa a ser autuada sob o *Computer Fraud and Abuse Act*, após causar o primeiro ataque do tipo *Denial-of-Service*, que consiste em tornar os recursos de um sistema indisponíveis para os seus utilizadores.

O lapso temporal, em termos históricos, entre os primórdios da internet, a criação do *World Wide Web* (www), na década de 1990, e a sua popularização e expansão, na década de 2000, mostrou-se bastante curto, o que acarretou o desenvolvimento de crimes digitais de forma igualmente frenética. Tal situação mostrou-se tão notável que a ciência jurídica passou a criar leis específicas para lidar com estes novos delitos praticados por meio de computadores ou dispositivos conectados a uma rede de conexão.

No contexto da atividade empresarial, as inovações digitais mostraram-se tão impactantes quanto na esfera pessoal dos indivíduos. As empresas modernas, portanto, devem se utilizar das ferramentas tecnológicas a fim de garantir uma experiência positiva aos seus clientes, entretanto, sempre buscando mitigar os riscos e efeitos negativos decorrentes do âmbito digital. Neste sentido, cita-se como de grande importância a segurança de dados financeiros, bem como a proteção de troca de mensagens entre cliente e empresa, buscando sempre garantir a confidencialidade das informações para o alcance de uma experiência verdadeiramente positiva.

Considerando a necessidade de adaptação a esse mercado cada vez mais interligado e dependente de ferramentas tecnológicas, as empresas enfrentam novos desafios, dentre eles o de atender adequadamente ao regramento imposto pela Lei nº 13.709/2018. Tendo isso em vista, o presente estudo tem como objetivo analisar brevemente as responsabilidades civil e administrativa, no âmbito empresarial, frente à caracterização de eventuais violações ao regime de proteção de dados pessoais.

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

1. HISTÓRICO DA PROTEÇÃO DE DADOS

Iniciaremos nosso estudo a partir de um breve histórico das leis de proteção de dados ao redor do globo, que vieram a ser grande fonte de inspiração para a atual Lei de Proteção de Dados vigente no território nacional.

1.1 As gerações da proteção de dados

A informação tornou-se o elemento nuclear para o desenvolvimento da economia, em razão da evolução tecnológica recente que criou mecanismos capazes de transmitir informações de forma muito rápida. Todavia, a importância dos dados pessoais foi notada após a Segunda Guerra Mundial, quando a máquina administrativa percebeu que, a partir de informações, poderia coordenar de forma mais eficiente seu crescimento.

De acordo com a visão de Viktor Mayer-Schonberger, professor da Universidade de Oxford, a evolução das leis de proteção de dados pessoais pode ser dividida em quatro gerações. A primeira delas traz a ideia de que a proteção de informações pessoais nasce da necessidade de processamento de dados dos cidadãos pelo Estado, o que chegou a gerar certa preocupação no sentido de que um Estado extremamente vigilante, nos moldes da obra “1984”, de George Orwell, poderia surgir e sufocar a liberdade individual. Em suma, a primeira geração de proteção de dados volta-se à esfera governamental.

Neste cenário em que o Estado foi centralizado como destinatário de regulamentos, um exemplo das leis de primeira geração é o *Privacy Act* estadunidense, datado de 1974, o qual teve como finalidade estabelecer práticas governamentais de uso, armazenamento e utilização de informações dos cidadãos americanos.

Transcendendo a esfera do poder público e as bases de dados estatais, a segunda geração de leis de proteção de dados preocupa-se também com o âmbito privado, ou seja, levando em consideração a analogia emprestada de André Carvalho Ramos com a obra de Orwell, o "Grande Irmão" (único detentor de dados), é

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

desmantelado em diversos "Pequenos Irmãos", (diversos bancos de dados de natureza estatal ou privada). Outra característica importante da segunda geração é o início de um maior protagonismo do indivíduo em determinar o fluxo de suas informações pessoais.

Seguindo a tendência de maior controle pelo indivíduo de seus dados, a terceira geração das leis de proteção de dados busca, nas palavras de Bruno Ricardo Boni, a autodeterminação informacional, ou seja, a maior participação do indivíduo desde a coleta até o compartilhamento de seus dados. Todavia, essa geração apenas abarcou alguns indivíduos, o que fez com que logo se tornasse obsoleta.

Por fim, a quarta geração das leis de proteção de dados, que prevalece até hoje, foi marcada pela criação de autoridades independentes para a aplicação das normas, buscando garantir a centralidade do consentimento do indivíduo quanto aos seus dados sem que isto se tornasse um empecilho para a sua efetiva participação social. Foi em meio a este processo evolutivo que o consentimento passou a ser caracterizado, nas palavras de Bioni, como "livre, informado, inequívoco, explícito e/ou específico" pelo direito comunitário europeu, no âmbito da União Europeia.

1.2 A proteção de dados na União Europeia

A proteção de dados tem como origem o continente Europeu, uma vez que seus países integrantes foram os pioneiros na edição de normas cuidando do tema. Entretanto, apesar do surgimento de tais normas, o verdadeiro marco da regulamentação da proteção dos dados pessoais tomou forma na Convenção 108, da década de 1980, de *Strasburg*, do Conselho da Europa.

Consequência do movimento promovido pela Organização para Cooperação e Desenvolvimento Econômico (OCDE), a Convenção 108, que é uma norma de direito internacional, teve como objetivo harmonizar as legislações de proteção de dados pessoais já existentes, além de estabelecer relações entre a proteção de dados e o livre fluxo informacional[3]. Ademais, o documento foi de

[3] Preâmbulo da Convenção 108 do Conselho da Europa: "Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples"

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

extrema importância para a elaboração da Diretiva Europeia de Dados Pessoais (EC nº 95/46) que buscou garantir aos indivíduos maior controle de seus dados pessoais e operacionalizar o consentimento, qualificando-o como livre, informado, inequívoco, explícito e/ou específico, como já mencionado nas linhas acima, bem como trazer deveres aos detentores dos dados (*data controllers*). Neste sentido, nas palavras de Bioni:

> "(...) A diretiva irá impor não só o direito de o titular dos dados controlá-los, mas simetricamente, deveres aos *data controllers* - quem processa os dados pessoais - para aperfeiçoar tal estratégia regulatória."

Importante ressaltar que uma diretiva, nos termos do artigo 288 do Tratado sobre Funcionamento da União Europeia, se diferencia de um regulamento, no sentido de que o regulamento é imediatamente aplicável à ordem jurídica de cada país membro, enquanto a diretiva depende de elaboração de legislação própria para determinar o modo de sua aplicação.

Pois bem, em meio à crescente utilização da tecnologia e às mudanças nos costumes dos indivíduos e empresas que resultaram em um ambiente onde a informação tornou-se importante moeda de troca, entrou em vigor, em 2018, o Regulamento Geral de Proteção de Dados Pessoais da União Europeia (GDPR - General Data Protection Regulation)[4], que substituiu a Diretiva nº 95/46.

Para além de unificar a proteção de dados para todos os 28 países membros da União Europeia, homogeneizando as regras já vigentes referentes à privacidade no continente, a GDPR criou moldes no que tange ao assunto da proteção de dados pessoais, o que significa dizer que muitas das leis aprovadas após a sua vigência tomaram como inspiração a GDPR, incluindo a Lei Geral de Proteção de Dados, atualmente em vigor no Brasil.

[4] GDPR - disponível em: https://gdpr-info.eu/

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

2. A PROTEÇÃO DE DADOS NO BRASIL

Analisaremos agora, de forma genérica, a Lei Geral de Proteção de Dados, vigente atualmente no Brasil.

2.1 LGPD - Lei Geral de Proteção de Dados

Conforme supramencionado, a evolução tecnológica e as mudanças significativas no modo de interação entre indivíduos e empresas foram importantes fatores na elevação da importância dos dados pessoais para o mercado. Levando isto em consideração, muitos pensadores contemporâneos caracterizem a própria informação como sendo a mais importante moeda de troca da atualidade, o que não é diferente no território brasileiro.

É fato que o Direito deve acompanhar o seu tempo, portanto, a crescente utilização de dados pessoais por empresas, para otimizar sua produção, havia de ser regularizada, a fim de que a esfera da privacidade dos indivíduos, direito previsto tanto pela Declaração Universal de Direito Humanos de 1948, quanto pela Constituição Federal de 1988, não fosse prejudicada.

Neste contexto, algumas regras disciplinando o uso, armazenamento, disponibilização, comunicação e violação do uso de dados pessoais começaram a surgir. Dentre elas, é possível citar como exemplo o artigo 43 do Código de Defesa do Consumidor que cuidou dos bancos de dados e cadastros dos consumidores. Neste caso, o legislador buscou abarcar todo e qualquer banco de dados que atingisse o livre desenvolvimento do consumidor, não apenas aqueles que apresentem informações negativas dos indivíduos. Ou seja, nas palavras de Bioni:

> "A legislação consumerista optou por conferir ao consumidor o direito de controlar as suas informações pessoais (...). Com efeito, toda a

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

> normatização ali desenhada desemboca para que o consumidor seja capacitado para autodeterminar as suas informações pessoais."

Outros exemplos de normas infraconstitucionais que abarcam o assunto dos dados pessoais são a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet (Lei nº 12.965/2014).

Para além das normas mencionadas, em 14 de agosto de 2018 foi publicada a Lei Geral de Proteção de Dados, Lei nº 13.709/2018, um diploma legal específico e direcionado para a proteção de dados pessoais que teve como molde as legislações internacionais de mesma natureza, como a Diretiva nº 95/46 e GDPR europeia.

Importa apontar, todavia, que, apesar de publicada em 2018, a Lei Geral de Proteção de Dados apenas passou a ter vigência completa em 1º de agosto de 2021, uma vez que alguns de seus artigos (52, 53 e 54) tiveram sua *vacatio legis* alterada pela Lei nº 14.010/2020.

Pois bem, partiremos para uma breve análise do mencionado diploma. Logo em seu artigo 1º, a LGPD determina seu alcance ao tratamento dos dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, inclusive no meio digital, bem como a sua finalidade de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da pessoa natural.

Importante ressaltar que por um lado, o diploma traz a previsão da "autodeterminação informativa", mencionada no capítulo anterior, o que significa dizer que a pessoa natural determinará com base no consentimento a disponibilização de seus próprios dados. Por outro lado, a LGPD tem como fundamento o "desenvolvimento econômico e tecnológico e a inovação", que esclarece que a finalidade da norma não é frear o desenvolvimento econômico do Estado ou de particulares, o que tem respaldo normativo do artigo 218 da Constituição Federal.

Diante disto, fica bastante clara a ponderação de interesses presente no corpo da LGPD. Em outras palavras, não há sombra de dúvidas quanto à importância do papel da tecnologia no desenvolvimento econômico atual, e não há como negar a

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

utilidade dos dados pessoais na seara corporativa. Neste sentido, a Lei Geral de Proteção de Dados busca, ao mesmo tempo, salvaguardar a privacidade dos indivíduos, bem como garantir o desenvolvimento econômico que se utiliza dos dados pessoais.

3. RESPONSABILIZAÇÃO NA LEI Nº 13.709/2018

Realizadas as prévias considerações a respeito da Lei nº 13.709/2018, percebe-se que o legislador atribuiu uma grande importância à proteção de direitos fundamentais, como os da liberdade, o da privacidade e o do livre desenvolvimento da pessoa natural. Para tanto, foram estabelecidas diretrizes principiológicas a serem seguidas durante o tratamento de dados. Prevalece, neste sentido, a imperiosa necessidade de o titular dos dados consentir previamente com o tratamento de dados e de ter direito ao pleno conhecimento de sua finalidade, necessidade e duração.

Dentre os princípios arrolados pelo legislador, no artigo 6º da Lei Geral de Proteção de Dados, ainda que todos se complementem e sejam de igual importância para a melhor proteção dos dados pessoais, é possível destacar alguns, devido à matéria em presente estudo, qual seja, a responsabilidade de pessoas jurídicas. Têm-se, assim, o princípio da segurança, o princípio da prevenção e o princípio da responsabilização e prestação de contas[5].

O primeiro pressupõe a utilização de uma série de medidas capazes de proteger os dados do titular contra eventuais acessos não autorizados ou contra práticas ilícitas ou acidentais que possam resultar na destruição, na perda, na alteração, na comunicação ou na difusão de dados. De maneira conjunta, busca-se reforçar a necessidade de prevenir quaisquer danos resultantes do processo de tratamento de dados. Por fim, fundamentado no princípio da responsabilização e da prestação de contas, os agentes de tratamento (controlador e operador) devem demonstrar que adotam medidas eficazes, as quais comprovem a observância das normas de proteção de dados.

[5] Vide art. 6º, inc. VII, VIII e X, da Lei nº 13.709/2018.

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

Então, este último princípio, também conhecido como princípio da *accountability*, sugere que não basta o agente de tratamento ter cumprido as regras previstas em Lei, é imprescindível que comprove esse atendimento, até mesmo quando não for verificado qualquer descumprimento ou irregularidade (LIMA, 2020, p. 305).

Tendo em vista esses princípios, o legislador previu duas formas de responsabilização — civil e administrativa —, as quais serão analisadas a seguir, separadamente. Além disso, também traremos destaque ao impacto positivo que a adoção de mecanismos de *compliance* pode ter sobre o desenvolvimento da atividade empresarial, principalmente no cenário em que são verificadas eventuais violações à Lei Geral de Proteção de Dados.

3.1 A Responsabilidade Civil

O legislador previu a regra geral de responsabilidade civil, no artigo 42, "caput", da Lei nº 13.709/2018, bem como o dever de ressarcimento dos danos. Segundo este dispositivo, então, o controlador ou o operador que violar a legislação de proteção de dados pessoais, causando dano patrimonial, moral, individual ou coletivo a outrem, em consequência da própria atividade de tratamento de dados, é obrigado a reparar esses danos. Excepcionalmente, é possível a solidariedade entre os agentes, com direito de regresso conferido àquele que reparar o dano ao titular[6].

A responsabilidade civil possui um significado técnico específico, pois trata-se de "situação jurídica de quem descumpriu determinado dever jurídico, causando dano material ou moral a ser reparado" (NADER, 2016, p. 6). Em sentido semelhante, Carlos Roberto Gonçalves afirma que a responsabilidade civil é um dever jurídico sucessivo, consequência da violação de uma obrigação, um dever jurídico originário. Assim, a responsabilidade civil representa a fonte de restauração do equilíbrio moral e patrimonial, a partir do dano provocado (GONÇALVES, 2020, p. 20-22).

[6] Vide art. 42, §2º e §4º, da Lei nª 13.709/2018.

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

Válido ressaltar, ademais, que a doutrina entende pela existência de duas modalidades de responsabilidade civil, a subjetiva e a objetiva. A responsabilidade civil subjetiva é a regra, segundo o Código Civil de 2002[7], de modo que se exige prova de culpa ou de dolo do causador do dano para que haja obrigação de repará-lo. Já na responsabilidade civil objetiva, prevalece a ideia de que há o exercício de determinada atividade, a qual oferece algum perigo ou representa um risco, este assumido pelo indivíduo, motivo pelo qual é obrigado a ressarcir eventuais danos, independentemente da comprovação de sua culpa (GONÇALVES, 2020, p. 28-29).

A Lei nº 13.709/2018 não prevê qual modalidade de responsabilização civil deve ser adotada, afinal, não indica expressamente a necessidade de comprovação do elemento subjetivo da culpa, mas também não o dispensa expressamente. Trata-se de um assunto polêmico e que exige maiores discussões. A seguir, resumimos alguns argumentos já suscitados por alguns juristas, a respeito da matéria.

Capanema, por exemplo, entende que o artigo 42, "caput", da Lei Geral de Proteção de Dados, pressupõe a desnecessidade de discussão sobre a culpa do agente de tratamento de dados, frente aos danos causados. Neste sentido, o legislador propositalmente reconheceu a hipossuficiência do titular e a possibilidade de inverter o ônus da prova, no parágrafo 2º, de forma que a responsabilidade civil objetiva confere uma maior proteção ao titular dos dados (CAPANEMA, 2021, p. 166).

Outros, por outro lado, entendem que o elemento subjetivo da culpa é essencial para o reconhecimento da responsabilidade do agente de tratamento de dados. Isto porque, segundo alguns defensores da responsabilidade civil subjetiva, o artigo 43 da Lei nº 13.709/2018 traz três hipóteses de exclusão da responsabilidade. Comprovada a inexistência de culpa, tem-se a desnecessidade de responder pelo eventual dano causado, pois o agente de tratamento apenas

[7] Vide arts. 186 e 187, do Código Civil de 2002, sobre a responsabilidade civil subjetiva. A responsabilidade civil objetiva é tratada excepcionalmente no art. 927, § único, do Código Civil de 2002.

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

desempenhava uma imposição legal. Aqui, é válido relembrar que o legislador previu expressamente o princípio da responsabilização e prestação de contas no artigo 6º.

Então, quando os agentes de tratamento provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído, como não possuíam qualquer vínculo de fato com o tratamento de dados realizado, não são responsabilizados. Quando os agentes de tratamento realizaram o tratamento de dados pessoais a que lhes foi atribuído, mas provarem que não houve violação à norma de proteção de dados, também não são responsabilizados. Por fim, quando provarem que o dano foi resultado de culpa exclusiva do titular dos dados ou de um terceiro, não há que se falar em responsabilidade.

Há ainda mais um posicionamento defendido por alguns, um meio-termo pautado em uma responsabilidade civil "sui generis". Nesta, o legislador teria optado por uma proteção específica, considerando o risco da atividade de tratamento de dados pessoais, e uma forma de prevenção pela responsabilização, para evitar eventuais danos. Assim, a Lei nº 13.709/2018 traria uma responsabilidade civil que combina graus de subjetividade e de objetividade. Ao mesmo tempo em que a Lei traz a previsão geral de responsabilidade civil no artigo 42, "caput", enumera hipóteses de exclusão da responsabilidade no artigo 43.

Chegando ao fim do tema da responsabilidade civil, destaca-se que a própria Lei nº 13.709/2018 prevê expressamente a possibilidade de aplicação da Lei nº 8.078/90 (Código de Defesa do Consumidor - CDC), quando o titular tiver seu direito violado, no âmbito das relações de consumo[8]. Neste caso, há a manutenção das regras de responsabilidade civil objetiva do CDC, independentemente de comprovação da culpa, pois o risco integral do negócio é atribuído ao próprio fornecedor (NUNES, 2019, p. 216/222). Aqui, tem-se a manifestação da própria finalidade do CDC, a de proteger o consumidor, parte hipossuficiente e mais vulnerável da relação consumerista, de maneira que a responsabilidade subjetiva restaria insuficiente para resolver adequadamente as demandas fundadas no consumo (TARTUCE, 2021, p. 676).

[8] Vide art. 45 da Lei nº 13.709/2018.

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

Tendo em vista o breve exposto, interessante encerrá-lo com o nosso posicionamento, no que tange à natureza jurídica da responsabilidade civil prevista na Lei Geral de Proteção de Dados. Salienta-se, contudo, que se trata de um tema que ainda irá suscitar muitas discussões, de modo que a literatura jurídica e a própria atuação do magistrado deverão cuidar de estabelecer qual a modalidade a ser adotada.

Em que pese outros posicionamentos, entendemos que a intenção do legislador está inclinada à previsão de uma responsabilidade civil objetiva. Para tanto, destacamos que a Lei nº 13.709/2018 cuida de dados pessoais, matéria intrinsecamente relacionada às garantias fundamentais do titular de dados. Não há dúvidas de que este titular, ainda que observadas todas as diretrizes principiológicas da Lei, é a parte mais frágil durante o tratamento de dados. Dessa maneira, aproximando-se do regime consumerista de responsabilização e considerando a fragilidade do titular de dados frente aos agentes de tratamento, assim como a sensível importância do bem jurídico em questão, a responsabilidade civil objetiva parece ser a mais adequada para garantir a efetiva proteção dos dados pessoais e a responsabilização de quem causar eventuais danos. Por fim, como consequência, as hipóteses do artigo 46 do mesmo diploma legal representam situações excepcionais, em que o legislador optou por afastar expressamente essa responsabilidade.

3.2 A Responsabilidade Administrativa

Feitas as devidas ponderações acerca da responsabilidade civil prevista na Lei Geral de Proteção de Dados, analisa-se brevemente a questão das sanções administrativas e a importância de os empresários adotarem programas de *compliance*, no que tange à cadeia de tratamento de dados pessoais. Em face de eventual infração a disposições da Lei em comento, a demonstração de que a atividade empresarial possuía um conjunto de ações e diretrizes a serem observadas é considerada no momento da aplicação de sanções.

Primeiramente, o objetivo do presente estudo não é o de esgotar comentários sobre cada um dos dispositivos referentes à responsabilidade administrativa, mas sim o de destacar a importância de conhecer a legislação e de

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

incorporar medidas que direcionem o funcionamento da atividade empresarial ao seu efetivo cumprimento. O fato de conhecer as normas de proteção de dados e de manter-se atualizado acerca deste específico regramento é essencial para que os agentes de tratamento de dados pessoais não sejam surpreendidos pela aplicação de sanções. Desde multas diárias à eventual proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados, o legislador buscou definir sanções administrativas proporcionais à importância do bem jurídico em proteção.

Como já mencionado anteriormente, a Lei Geral de Proteção de Dados visa ao resguardo de direitos fundamentais do titular de dados. Em uma sociedade que se transforma rapidamente e possui uma dependência expressiva a meios digitais, para garantir a finalidade precípua da carta constitucional, de garantir a proteção de direitos individuais e coletivos, é condizente a possibilidade de aplicação de sanções rigorosas. Busca-se, para tanto, prevenir a ocorrência ou a recorrência do dano e, frente à inobservância de regras administrativas, o órgão de controle está plenamente autorizado a impor sanções, nos termos da Lei.

Segundo o artigo 65, inciso I-A, da Lei nº 13.709/2018, entraram em vigor, a partir do dia 1º de agosto de 2021, seus artigos 52 a 54, que tratam das sanções administrativas aplicáveis. Já a responsabilidade civil tratada no tópico anterior, passou a ser aplicável 24 (vinte e quatro) meses após a data da publicação da Lei[9]. Assim, percebe-se que a responsabilidade administrativa da Lei Geral de Proteção de Dados é um tema recente e que deve ser observado com cuidado por pessoas jurídicas que realizam o tratamento de dados pessoais, pois fatos ocorridos após 1º de agosto de 2021 e infrações de natureza continuada iniciadas antes de 1º de agosto de 2021 já estão sujeitos à eventual sanção de cunho administrativo.

Observa-se pelo artigo 52, "caput" e incisos, que, tendo em vista as infrações cometidas pelos agentes de tratamento de dados, a Autoridade Nacional de Proteção de Dados (ANPD) está autorizada a aplicar variadas sanções administrativas. Apesar de somente a ANPD possuir essa competência, ainda é

[9] Vide art. 65, inc. II, da Lei nº 13.709/2018.

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

possível aplicar sanções administrativas, civis ou penais, previstas na Lei nº 8.078/90 (Código de Defesa do Consumidor) e em outras legislações específicas[10].

Para a aplicação dessas sanções, deve haver um prévio procedimento administrativo, o qual possibilite a ampla defesa, além de exigir-se uma ponderação sobre uma série de circunstâncias relacionadas ao caso concreto, dentre elas: a boa-fé e a condição econômica do infrator; a reincidência; e a adoção de política de boas práticas e governança e de medidas corretivas[11]. Acerca de instrumentos de governança corporativa, em especial, nota-se como adquirem importância na proteção de dados pessoais[12].

A ideia de governança corporativa aproxima-se muito aos programas de *compliance*, pois criar condições para o desenvolvimento e manter um efetivo programa de *compliance* é, em última análise, uma decisão de gestão. Assim, a governança corporativa relaciona-se ao modo como as companhias são geridas e a como suas decisões de gestão são tomadas. *Compliance*, por sua vez, é a exigência de conformidade com o regramento aplicável, com as políticas internas de cada companhia e com as exigências da ética empresarial (CASTRO, 2021, p. 3-17).

Tendo isso em vista, em matéria de direito digital, discute-se a *accountability*[13], também chamada de responsabilidade demonstrável, por meio da qual a atividade empresarial assume uma maior responsabilidade sobre o processo de tratamento de dados pessoais. Então, caso a atividade desenvolvida envolva tratamento de dados pessoais, exige-se que as instituições se responsabilizem, demonstrando que se utilizavam de mecanismos adequados, justos e éticos. Trata-se de uma manifestação da proposta de *compliance* a ser demonstrada à Autoridade Nacional de Proteção de Dados, pois a atividade empresarial comprova seu

[10] Vide art. 52, §2º, da Lei nº 13.709/2018. O art. 55-K, parágrafo único, do mesmo diploma legal, ainda define que a ANPD deve articular sua atuação com os demais órgãos e entidades de competência sancionatória e normativa relacionada à proteção de dados pessoais. Neste sentido, cabe à ANPD assumir o papel de órgão central de interpretação da LGPD e de estabelecer normas e diretrizes a serem implementadas.
[11] Além destes parâmetros e critérios, outros estão arrolados no art. 52, §1º, da Lei nº 13.709/2018.
[12] Vide art. 50 da Lei nº 13.709/2018, sobre boas práticas e governança.
[13] Note-se a previsão, no art. 6º, inc. X, da Lei nº 13.709/2018, do princípio da responsabilização e prestação de contas, chamado por alguns de princípio da *accountability*.

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

comprometimento com o regramento relativo à proteção dos dados pessoais (CASTRO, 2021, p. 517).

Por meio de efetivos programas de *compliance*, além de permitirem uma melhor gestão de risco da atividade empresarial de tratamento de dados pessoais, são considerados uma atenuante no momento de aplicação de sanções administrativas. Para tanto, obviamente, esses programas devem observar requisitos mínimos, como os previstos no artigo 50, inciso I e alíneas, da Lei nº 13.709/2018, a fim de evitar "programas de fachada".

Assim, aproximando-se do fim da discussão sobre a responsabilidade administrativa, ressalta-se o papel do *compliance* na busca pela garantia da legislação sobre dados pessoais. Adotar políticas de boas práticas e de governança aumenta a competitividade da atividade empresarial, pois assegura ao titular de dados uma maior transparência acerca da cadeia de tratamento de dados pessoais, além de representar, como já mencionado, um critério atenuante quando houver eventual descumprimento à Lei nº 13.709/2018. Então, parece interessante que as atividades empresariais adequem-se a essa nova realidade, na qual já estão sujeitas à aplicação de sanções administrativas, incorporando mecanismos capazes de comprovar seu comprometimento com o regramento de proteção de dados.

CONCLUSÕES

Tendo em vista o exposto, ressaltamos a importância de as empresas conhecerem e observarem com cuidado o texto da Lei nº 13.709/2018. Com a vigência recente da totalidade de seus dispositivos, esse diploma legal representa uma maior segurança ao titular de dados pessoais, ao condicionar os agentes de tratamento de dados a uma série de regras a serem observadas sob o risco de responsabilização.

Assim, para assegurar os direitos fundamentais da liberdade e da privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural,

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

o legislador estabeleceu duas formas de responsabilização — civil e administrativa —, objetos de análise neste breve trabalho.

Pudemos observar, neste sentido, que a Lei Geral de Proteção de Dados não indica expressamente se a responsabilidade civil é objetiva, subjetiva ou, ainda, "sui generis", como alguns defendem, porém, entendemos que a teoria objetiva é a que mais se adequa à finalidade do diploma legal em comento. Isto porque, diante de um diálogo entre suas diretrizes principiológicas e o objeto jurídico a que visa assegurar, a responsabilização civil objetiva parece ser a que garante uma maior proteção ao titular de dados pessoais.

Ademais, ao tratarmos da chamada responsabilidade administrativa, cujos dispositivos já se encontram vigentes, utilizamos a oportunidade para destacar a importância de as empresas adotarem programas de *compliance*. Baseado no próprio princípio da *accountability*, expressamente previsto na Lei nº 13.709/2018, é interessante que a atividade empresarial integre políticas de boas práticas e de governança, garantindo uma maior transparência ao titular de dados e demonstrando efetivamente que buscava observar o regramento de proteção de dados pessoais.

Então, considerando principalmente o tratamento de dados em meios digitais, com os quais as atividades empresariais modernas têm se inter-relacionado com cada vez mais expressividade, é essencial, dentro dessa nova realidade, garantir uma proteção específica para o titular de dados. Para tanto, as empresas devem conhecer a legislação de proteção de dados pessoais, seguindo-a e colocando-a em prática, conscientes de que eventuais violações realmente poderão sujeitá-las ao regime de responsabilização civil ou administrativa da Lei nº 13.709/2018.

REFERÊNCIAS

- ALMEIDA, Juliana Evangelista e LUGATI, Lys Nunes. *Da Evolução das Legislações Sobre Proteção de Dados: A Necessidade de Reavaliação do Papel do Consentimento como Garantia da Autodeterminação Informativa*. 2020. Disponível em: https://periodicos.ufv.br. Acesso em 25 de outubro de 2021.

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

- BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento* - 2. Reimpr. Rio de Janeiro: Forense 2019.

- CAPANEMA, Walter Aranha. *A responsabilidade civil da Lei Geral de Proteção de Dados*. Cadernos Jurídicos da Escola Paulista da Magistratura, São Paulo, 2021. Págs. 163-170.

- CASTRO, André Carvalho (coord.) et al. *Manual de Compliance*. 3ª Edição. Rio de Janeiro: Forense, 2021. E-book. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786559640898/epubcfi/6/2%5B%3Bvnd.vst.idref%3Dcover%5D!/4/2/2%5B63a8e59c-cf38-4efb-bc9a-4a0f895662aa%5D%4051:2>. Acesso em 11 de outubro de 2021.

- GOV.BR. *Perguntas e Respostas: Sanções Administrativas: o que muda após 1º de agosto de 2021?* Publicado em 30 de julho de 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021>. Acesso em 11 de outubro de 2021.

- GONÇALVES, Carlos Roberto. Direito Civil Brasileiro. Vol. 4. *Responsabilidade Civil*. 15ª Edição. São Paulo: Saraiva Educação, 2020. E-book. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553615957/pageid/5>. Acesso em 8 de outubro de 2021.

- KOEPSEL, Alice de Medeiros. *Adoção e efeitos dos programas de compliance à luz da Lei Geral de Proteção de Dados Pessoais*. Trabalho de Conclusão de Curso. Direito. Universidade do Sul de Santa Catarina. Tubarão, p. 71, 2020. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/5452/1/MONOGRAFIA%20-%20ALICE%20KOEPSEL.pdf>. Acesso em 11 de outubro de 2021.

- LIMA, Cíntia Rosa Pereira D. (coord.). *Comentários à lei geral de proteção de dados: Lei nº 13.709/2018, com alteração da Lei nº 13.853/2019*. São Paulo: Almedina, 2020. Pág. 305. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>. Acesso em 8 de outubro de 2021.

Larissa Monaco Caranti
lmonacocaranti@gmail.com
Tatiana Lie Fukuhara
lieholanda@gmail.com

- MAZON, Filipe Augusto. *Responsabilidade Civil do Controlador/Operador de Dados Pessoais no Âmbito da Lei 13.709/18 (LGPD)*. Trabalho de Conclusão de Curso. Direito. Universidade Evangélica de Goiás. Anápolis, p. 82. 2021. Disponível em: <http://repositorio.aee.edu.br/jspui/handle/aee/18223>. Acesso em 8 de outubro de 2021.

- NADER, Paulo. Curso de Direito Civil. Vol. 7. *Responsabilidade Civil*. 6ª Edição. Rio de Janeiro: Forense, 2016. E-book. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788530968724/epubcfi/6/10%5B%3Bvnd.vst.idref%3Dcopyright%5D!/4/10/3:70%5Bu%20d%2Ce%20q%5D>. Acesso em 8 de outubro de 2021.

- NUNES, Rizzato. *Curso de Direito do Consumidor*. 13ª Edição. São Paulo: Saraiva Educação, 2019.

- UNITED STATES DEPARTMENT OF JUSTICE. Overview of the Privacy Act of 1974 - 2020 Edition. Disponível em: https://www.justice.gov/opcl/privacy-act-1974. Acesso em 25 de outubro de 2021.

- PECK, P.P S*egurança Digital - Proteção de Dados nas Empresas*. Grupo GEN, 2020. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597026405/. Acesso em: 04 de agosto de 2021.

- TARTUCE, Flávio. *Responsabilidade Civil*. 3ª Edição. Rio de Janeiro: Forense, 2021. E-book. Pág. 676. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786559640959/epubcfi/6/10%5B%3Bvnd.vst.idref%3Dhtml5%5D!/4/20/1:29%5B0-0%2C40%5D>. Acesso em 8 de outubro de 2021.