COMENTANDO A LEI GERAL DE PROTEÇÁO DE DADOS PESSOAIS -

ESTUDOS ACADÊMICOS - UFF

ORGANIZADORES:

PLINIO LACERDA MARTINS

MARCOS CÉSAR DE SOUZA LIMA

ALAN MATEUS SAMPAIO DE SOUZA

ALCINÉA DA SILVA MACEDO

DAFNE FREITAS GOMES

DYANA RIBEIRO CAMELO

GABRIEL MOREIRA NASCIMENTO

GIOVANNA CORRÊA KIUCHI

JULIANA SOAVE DOS REIS

LETICIA LACERDA MOURA MARTINS

LUIS EDUARDO DE SOUZA LEITE TRANCOSO DAHER

LUIZ AUGUSTO BARCELOS INÁCIO

MARCOS DA SILVA PEREIRA

MARIA BEATRIZ ALVIM BARROS

MILENA DE AZEVEDO ALMEIDA

PLINIO LACERDA MARTINS

RAFAELA GONÇALVES DUQUE

PUBLICACAO: INSTITUTO DE DIREITO PUBLICO E PRIVADO DO BRASIL– IDPP - UFF

Universidade Federal Fluminense

MARTINS, Plinio Lacerda, SOUZA LIMA, Marcos Cesar, RAMADA, Paula Cristiane Pinto Ramada. Comentando a Lei Geral de Proteção de Dados Pessoais. IDPP: Rio de Janeiro, 2021.

ISBN: 978-65-993766-1-0

Comentando a Lei Geral de Proteção de Dados Pessoais. Direitos dos titular, responsabilidade, encarregados, inteligência artificial.

APRESENTAÇÃO

O presente ensaio jurídico, é fruto das pesquisas dos alunos da disciplina tutela jurisdicional dos dados pessoais do curso de Direito da Faculdade de Direito da Universidade Federal Fluminense no período de 2019-2020.

A finalidade da pesquisa se destina a trazer reflexões a respeito da edição da Lei Geral de Proteção de Dados no Brasil e seus reflexos na sociedade contemporânea.

O trabalho jurídico desenvolvido pelos alunos da graduação, consolida um trabalho de folego, abordando diversos aspectos da LGPD, tais como o tratamento de dados pessoais pelo poder público, o consentimento na LGPD, Autoridade de Proteção de Dados, a questão da inteligência artificial e inclusive a responsabilidade civil dos agentes de tratamento dos dados pessoais.

Acredito que este singelo trabalho possa servir de inspiração para outras pesquisas a respeito da Lei Geral de Proteção de Dados e a necessidade de implementação de politicas publicas para a o efetivo cumprimento da lei.

Plinio Lacerda Martins – Professor adjunto da UFF

SUMARIO

4

INTELIGÊNCIA ARTIFICIAL E ADVOCACIA

Luis Eduardo de Souza Leite Trancoso Daher
Rafaela Gonçalves Duque

I. INTRODUÇÃO

Ab initio, salienta-se que a expressão "Inteligência Artificial (IA)" se refere a um conceito um tanto quanto abstrato e de difícil definição, mas pode-se inferir que esta se relaciona com o ramo da computação e se define como os esforços para se chegar o mais próximo possível de uma inteligência orgânica, como a dos seres humanos.

O pressuposto de imitar as funções cognitivas humanas concede à IA uma polivalência de temas em seu escopo, interseccionando as mais variadas áreas do conhecimento, tornando a Inteligência Artificial multifacetada. Por sua característica multidisciplinar, a IA pode ser aplicada no mundo jurídico, favorecendo a otimização de processos, redução de custos, aumento da produtividade e melhora dos resultados obtidos.

A partir desse viés, contextualiza-se que, anualmente, milhões de ações são ajuizadas no Brasil.[1] Essa judicialização em massa implica verdadeiro congestionamento do sistema judiciário e, por conseguinte, uma maior lentidão nas decisões a serem tomadas.

Isto porque, o enorme volume de informações associadas aos processos judiciais acaba comprometendo a efetividades do trabalho dos operadores do direito que, como seres humanos que são, possuem limitações cognitivas para lidar com o excesso de demanda no judiciário.[2]

Sendo assim, o expressivo número de ações, tramitando nos mais diversos tribunais do país, demonstra uma grande necessidade de buscar soluções e mecanismos tecnológicos que visem imprimir maior celeridade e economia às atividades judiciais, bem como menor dispêndio de tempo dos profissionais envolvidos. [3]

---

[1] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. Inteligência Artificial no Direito: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018.
[2] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 8. ISBN 978-65-00-03948-1.
[3] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. Inteligência Artificial no Direito: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias. Salvador: Organização Comitê Científico, 2018, v.4, p.2.

Nesse sentido, a Inteligência Artificial (IA) tem sido utilizada, cada vez mais, na procura da melhora da qualidade e eficiência dos serviços jurídicos, através da construção de sistemas computacionais capazes de complementar as habilidades cognitivas dos diferentes operadores jurídicos, tornando efetivo o processo decisório.[4]

Além de favorecer uma melhor compreensão dos processos cognitivos e da inteligência humana, a IA tem sido uma grande aliada na construção dos processos de raciocínio e argumentação jurídica, o que contribui para uma melhora e evolução do Direito em si, como matéria. [5]

Nesse desiderato, o presente estudo busca discutir brevemente a aplicação da inteligência artificial na atividade jurídica e no mundo hiperconectado, perpassando pelas técnicas de raciocínio automatizado[6] e de representação de conhecimento[7], a fim de melhor delinear as principais aplicações práticas da IA.

Vale destacar que, sob o viés da automatização da tomada de decisões em âmbito jurídico, não se pode olvidar que muitas tarefas, antes consideradas como prerrogativas humanas, hoje são executadas por *estes* operadores autômatos[8]

Essa evolução tecnológica, em que *Inteligências Artificiais* e mecanismos automatizados detêm poder para tomada de decisões, nos leva a refletir sobre os efeitos desses sistemas para a autonomia pessoal e, consequentemente, sobre a necessidade de se preservar os direitos fundamentais, o que sugere a importância de recorrermos à ética como instrumento capaz de encaminhar soluções que, eventualmente, possam consolidar-se em alternativas legislativas[9], além de ressaltar a importância do direito à revisão de decisões automatizadas.

Por derradeiro, o estudo, além de abordar as aplicações práticas da IA no mundo jurídico, irá discorrer sobre a ética e a Proteção de Dados Pessoais como instrumentos de salvaguarda dos direitos fundamentais, tendo em vista a prática automatizada das decisões dos

---

[4] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 3. ISBN 978-65-00-03948-1.

[5] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 8-9. ISBN 978-65-00-03948-1.

[6] Segundo a Autora Rosario Girardi, o raciocínio automatizado visa a construção de sistemas de computação que automatizam o processo cognitivo. O termo foi, tradicionalmente, associado ao raciocínio dedutivo como praticado em matemática e lógica formal. Existem quatro tipos principais de raciocínio: dedução, indução, abdução e analogia.

[7] As linguagens de representação de conhecimento, como a lógica formal, são utilizadas para representar computacionalmente as regras de inferência do processo de raciocínio.

[9] DONEDA, D.C.M.; MENDES, L.S.; SOUZA, C.A.P.; ANDRADE, N.N.G. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. Pensar: Revista de Ciências Jurídicas, Fortaleza, v.23, n.4, p. 1-17, out./dez.2018.

operadores do direito e o iminente risco de serem violadas as garantias constitucionais do *due processo of law*[10], como igualdade, publicidade e segurança jurídica.

Assim, a artigo será organizado da seguinte forma: em um primeiro momento, serão levantadas algumas considerações iniciais sobre a Inteligência Artificial e a sua relação próxima com os dados. Posteriormente, será abordada a importância da ética na regulação da IA. Em sequência, teremos como ponto focal as principais aplicações da IA no Direito, sob a luz das técnicas de raciocínio automatizado e representação do conhecimento. Por fim , teremos as conclusões do estudo e uma breve discussão sobre os desafios ainda existentes na aplicação da IA no mundo jurídico.

II. O INÍCIO DE TUDO

Quando se trata de Inteligência Artificial, abordar a face histórica desta discussão e a maneira como este conceito se ramifica atualmente é essencial para compreendermos seus desdobramentos multidisciplinares. Em 1943, Warren McCulloch e Walter Pitts apresentaram um artigo que falava pela primeira vez no conceito de redes neurais, estruturas de raciocínio artificiais que imitam o nosso sistema nervoso, com seus nós interconectados funcionam justamente como os neurônios humanos, sendo um bom pontapé inicial para a IA.[11]

Em 1950, Alan Turing desenvolveu uma forma de avaliar se uma máquina consegue se passar por um humano em uma conversa por escrito. Denominado teste de Turing, originalmente conhecido como Jogo da Imitação, o experimento deu título ao filme que retratou a vida do pesquisador, além de representar um marco para a ciência no ramo das IA's.[12]

A primeira vez que se falou sobre Inteligência Artificial, como um campo de estudo acadêmico, foi em 1956, em uma conferência em Darthmouth College, uma universidade estadunidense. O termo cunhado por John McCarthy caiu como uma luva para esta matéria que foi impulsionada a partir da segunda guerra mundial, tendo nomes como Allan Turing, Ada Lovelace, Herbert Simon e o próprio John McCarthy como principais idealizadores.[13]

---

[10] Princípio fundamental do processo civil, previsto na Constituição da República Federativa do Brasil de 1988, em seu art. 5º, inciso LIV. A partir desse princípio decorrem todas as consequências processuais que garantiriam aos litigantes o direito a um processo e uma sentença justa.
[11] FRAZÃO, Ana; MULHOLLAND, Caitlin; Inteligência Artificial e Direito: ética, regulação e responsabilidade. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 41.
[12] CARNEIRO, Tayná; FALCÃO, Cintia Ramos. Direito Exponencial: o papel da Novas Tecnologias no Jurídico do Futuro. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. P. 337.
[13] FEIGELSON, Bruno; MALDONADO, Viviane Nóbrega. Advocacia 4.0. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p.75.

Para entendermos suas aplicações práticas, precisamos realizar um esforço no sentido de categorizar a IA, de entendermos que não existe pura e simplesmente um único tipo de Inteligência Artificial, e sim diversas ramificações desta matéria. Devemos, portanto, levar em conta a existência de três grandes grupos: Inteligência Artificial Limitada (ANI), Inteligência Artificial Geral (AGI) e Superinteligência (ASI).[14]

A ANI ou "IA Fraca" (*Weak AI*) é caracterizada por ser o tipo mais básico de IA, é o nível mais baixo, que consegue apenas se especializar em uma área específica, como a emblemática IA jogadora de Xadrez, por exemplo. Essa categoria se subdivide ainda em **Máquinas Reativas**, que literalmente somente reagem às situações, não possuem nenhuma capacidade de memória e aprendizado com situações passadas, e IA's de **Memória Limitada**, que dizem respeito às máquinas que conseguem processar situações passadas (memória) para fundamentar a decisão atual.[15]

Um exemplo que já estamos ficando acostumados a ver são os carros autônomos, eles observam a velocidade e a direção dos outros carros para decidirem o que fazer, além disso, aprendem com os erros que outros carros autônomos, que estejam interligados ao seu sistema, cometeram anteriormente. [16]

Já a AGI, conhecida como "IA Forte" (*Strong AI*) ou "IA nível humano", relaciona-se a uma Inteligência artificial que possui domínio e *expertise* em diversas áreas, não mais se limitando a apenas uma específica. Esta IA se equivaleria à capacidade intelectual e multidisciplinaridade do ser humano e passaria com facilidade no Teste de Turing, relatado anteriormente. Este tipo de Inteligência Artificial ainda não foi concebido, continua objeto exclusivo das obras de ficção científica e, assim como a anterior, é subdividida em dois grupos, que segundo Martha Gabriel são[17]:

> – **Máquinas Cientes**: classe de mentes computacionais que não apenas "enxergam" o mundo (criam representações), mas também conseguem "perceber" outros agentes ou entidades – elas compreendem que as pessoas, criaturas e objetos no mundo podem ter pensamentos e emoções que precisam ser consideradas para ajustar o seu próprio comportamento (ciência). Essas habilidades são essenciais para permitirem interações sociais, e é a partir delas

[14] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 188-190.
[15] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 188-190.
[16] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 188-190.
[17] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 188-190.

> que os humanos formaram sociedades – seria muito difícil, ou mesmo impossível, trabalharmos juntos sem compreender as motivações e intenções uns dos outros, e sem considerar o que o outro sabe sobre si e o ambiente.
>
> – **Máquinas Autoconscientes**: essa classe de sistemas de IA vai além na Teoria da Mente e possui "autoconsciência". Em outras palavras, elas têm consciência não só sobre o seu exterior, mas também sobre si mesmas. Essa é uma diferença grande em relação a ter ciência apenas do que está do lado de fora – seres autoconscientes conhecem os seus estados internos, e são capazes de prever os sentimentos dos outros. Por exemplo, nós pressupomos que alguém que está chorando está triste porque, quando estamos tristes, nós choramos. Da mesma forma que a inteligência, a consciência é algo difícil de se definir, mas que conseguimos facilmente reconhecer.[18]

Por fim, há ainda a Superinteligência (ASI), que compreende desde computadores um pouco mais inteligentes e desenvolvidos em áreas como criatividade científica, conhecimentos gerais e habilidades sociais até aqueles que podem ser milhões de vezes melhores do que nós. Esse é o conceito principal de Inteligência Artificial que perambula pelo universo cinematográfico e literário, discorrendo até mesmo sobre a possibilidade da Singularidade Tecnológica, uma hipótese em que as mudanças paradigmáticas da história humana correlacionadas com o desenvolvimento desenfreado de tecnologias relacionadas à Superinteligências Artificiais culminariam inevitavelmente na extinção da raça humana.[19]

III. OS DADOS E A INTELIGÊNCIA ARTIFICIAL

Em perspectivas mais contemporâneas e realistas, é necessário que tenhamos consciência de que a Inteligência Artificial se manifesta de forma mais palatável e concebível a partir do nascimento da internet, a partir do momento em que começamos a digitalizar nossas vidas. Há um fenômeno no meio dessa realidade digital, dessa sociedade da informação, que atua como marco impulsionador da IA e de tantas outras tecnologias atualmente: o "*Big Data*".

A internet surge como um dos melhores métodos para se gerar e armazenar dados e, conforme a tecnologia avança, essa possibilidade de gerar, armazenar e gerenciar dados aumenta. À medida em que se expandem os HD's[20] e a velocidade de transferência da internet aumenta,

[18] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 188-190.
[19] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 188-190.
[20] Os Hard Disks ou simplesmente HD's são unidades de armazenamentos de dados muito comuns em computadores e notebooks.

mais combustível é injetado no tanque da "*Big Data"* e maior e de mais qualidade é o banco de dados amostrais que pode ser utilizado para aprimorar a IA.[21]

Neste sentido, podemos e devemos caracterizar o *Big Data* como um fenômeno intrínseco ao mundo hiperconectado em que estamos cada vez mais inseridos. É importante destacar que além da internet, que funcionou como um facilitador da proliferação e consequente criação de mais dados no mundo, precisamos conceituar e dar o devido destaque também à Internet das Coisas (*Internet of Things – IOT*) que já mudou o paradigma de captação e armazenamento de dados.[22]

Não há um conceito específico definido para Internet das Coisas, mas podemos dizer que ela consiste na interconexão de objetos ordinários, de modo que estes objetos formam uma enorme rede de dispositivos que interagem entre si, captando, analisando e gerando dados. No âmbito da *IOT*, há a presença de três conceitos elementares para seu funcionamento: conectividade, uso de sensores/atuadores e capacidade computacional de processamento e armazenamento de dados. Podemos citar como exemplo a pulseira inteligente que conta seus passos e transfere para o aplicativo de saúde do seu celular, tudo através da internet. Neste delinear e com o avanço da Internet das Coisas, estima-se um fluxo de dados ainda maior para o futuro.[23]

Neste cenário de abundância de dados é necessário designar alguns esforços para gerir e organizar este amontoado, sendo este acontecimento, como já mencionamos, denominado de *Big Data*, um efeito cascata do mundo digitalizado, caracterizado justamente pela inconcebível quantidade de dados gerada e a capacidade de se ordenar dentro deste espectro.[24]

Por intermédio do fenômeno da digitalização e datificação[25] da vida, passamos a vivenciar um paradigma da necessidade de criação de novos direitos fundamentais, além da reinterpretação daqueles que já existiam, sob a lente tecnológica da sociedade conectada. É nesta linha de raciocínio que se discute o direito à Proteção dos Dados Pessoais, como uma extensão

---

[21] MAGRANI, Eduardo. Entre Dados e Robôs: Ética e Privacidade na Era da Hiperconectividade. 2ª ed. Porto Alegre: Arquipélago Editorial, 2019. p.22-24.
[22] MAGRANI, Eduardo; Entre Dados e Robôs: Ética e Privacidade na Era da Hiperconectividade. 2ª ed. Porto Alegre: Arquipélago Editorial, 2019. p.22-24.
[23]MAGRANI, Eduardo. Internet das Coisas. 1ª ed. Porto Alegre: FGV Editora, 2018. p. 20
[24] MAGRANI, Eduardo. Entre Dados e Robôs: Ética e Privacidade na Era da Hiperconectividade. 2ª ed. Porto Alegre: Arquipélago Editorial, 2019. p.22-24.
[25] Datificação é a transformação de nossas vidas em dados computadorizados, ou seja, é a representação eletrônica de nossas fotos, vídeos, gostos, comportamentos e costumes, que criam versões abstratas de nós por meio das tecnologias da informação, que tem o potencial de refletir concretamente no mundo físico.

lógica dos direitos personalíssimos à intimidade, vida privada, honra e imagem dos indivíduos, trazidos pelo inciso X do artigo 5º da Constituição da República Federativa do Brasil.[26]

Um embate entre o direito à Proteção de Dados Pessoais e as tão discutidas Inteligências Artificiais, que se alimentam e utilizam como base conjuntos de dados, era uma consequência previsível. Em alguns aspectos estes conceitos se cruzam, entretanto, nos interessa somente o direito a revisão de decisões automatizadas derivado da proteção de dados e da utilização, cada vez mais corriqueira, de mecanismos de IA em tribunais, bancos de análise de crédito e qualquer outro ambiente que envolva decisões automatizadas na prática.

Um dos institutos mais importantes e presentes no campo da IA e das tomadas de decisões autônomas é o de *Machine Learning*[27] (ML), que basicamente se traduz em um algoritmo[28] com capacidade para interpretar, criar padrões e literalmente aprender "sozinho". Claro, tudo isso com o estímulo correto, dado pelo cientista da computação, engenheiro ou qualquer pessoa que esteja alimentando uma máquina com essas características. É deste arranjo que nascem as tomadas de decisão automatizadas, realizadas por Inteligências Artificiais com capacidade de Aprendizado de Máquina. [29]

Ainda sobre o *Machine Learning*, absorve-se a importante lição de Caitlin Mulholland e Isabella Z. Frajhof:

> O uso de programas de aprendizado por máquinas, conhecido pelo termo *machine learning*, permite que sejam criados sistemas de Inteligência Artificial (IA) que desenvolvem a capacidade de tomadas de decisão absolutamente autônomas em relação à interferência humana. Isto é, torna-se possível por meio de tratamento de dados em massa – *inputs* – o desenvolvimento de autoaprendizagem das máquinas – *i.e.* programas e sistemas – que permite o alcance de determinados resultados – *outputs* – independentemente de qualquer mediação por um ser humano. Ou seja, o próprio sistema alcança resultados por meio de processos dedutivos e análises estatísticas que vão sendo determinados com base em correlações realizadas pela IA. Esses resultados, em não raras vezes, são obtidos sem que seja possível, *a priori*, reconhecer os padrões adotados pela IA para a análise de dados selecionados e o modo de trabalho que levaram a esses *outputs*.[30]

---

[26] CARNEIRO, Tayná; FALCÃO, Cintia Ramos. Direito Exponencial: o papel da Novas Tecnologias no Jurídico do Futuro. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. p. 469-470

[27] No Brasil é comumente chamado de Aprendizado de Máquina, a tradução literal de Machine Learning.

[28] Algoritmos são basicamente uma sequência de regras que mostram o passo-a-passo necessário para executar uma tarefa específica.

[29] FEIGELSON, Bruno; MALDONADO, Viviane Nóbrega. Advocacia 4.0. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p 79.

[30] FRAZÃO, Ana; MULHOLLAND, Caitlin; Inteligência Artificial e Direito: ética, regulação e responsabilidade. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 265 e 266.

Quando uma máquina tem a capacidade de se orientar sozinha por meio de estruturas de *Big Data*, funcionando de maneira mais próxima ainda a um conjunto orgânico, esta recebe a alcunha de Deep Learning. Este conceito foi concebido baseado na ideia de redes neurais, se estruturando por meio da sobreposição de diversas camadas não lineares de processamento de dados, de maneira muito mais próxima ao cérebro humano.[31]

Dito isto, faz-se necessária uma reflexão relacionada ao titular de dados, indivíduo que sofre as consequências da utilização de dados no processo de aprendizado de máquina. Neste seguimento, é válido destacarmos que alguns esforços já vêm sendo notados e a recém vigorada Lei Geral de Proteção de Dados traz, em seu artigo 20, o que estudiosos do assunto denominam "direito à explicação".

Este direito decorre do princípio da transparência e preceitua que o titular de dados deve ter direito à revisão de decisões tomadas exclusivamente com base na análise de dados, por mecanismos automatizados. Com isso, a legislação resguarda o direito a uma análise humanizada, que leve em conta fatores menos inteligíveis e claros para um ente que não é dotado de inteligência emocional, social e muito menos de raciocínio crítico que demande a compreensão e a interpretação de outros fatores que não sejam dados brutos.[32]

O direito à revisão das decisões é pressuposto essencial para a construção de uma regulação madura e inserida em uma cultura protecional de dados pessoais, além de revelar, juntamente com as demais legislações de proteção de dados, uma inclinação à aplicabilidade do Princípio da Precaução na Regulação de Inteligência Artificial.[33]

Neste seguimento, quando falamos em tomada de decisão por meio de Inteligência Artificial, precisamos considerar ainda os pressupostos para a criação e construção desse ente computadorizado. Questionamentos acerca da imparcialidade, eticidade e construção algorítmica enviesada precisam ser levantados quando discutimos o tema.

---

[31] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 210 a 214.
[32] FRAZÃO, Ana; MULHOLLAND, Caitlin. Inteligência Artificial e Direito: ética, regulação e responsabilidade. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 265 e 266.
[33]FRAZÃO, Ana; MULHOLLAND, Caitlin. Inteligência Artificial e Direito: ética, regulação e responsabilidade. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 215.

Abordar o mundo virtual de forma dissociada do real ou natural não é mais uma possibilidade. É imperioso que se admita a hibridização e a confluência destes dois espectros para que possamos debater acerca de possibilidades regulatórias que minimizem esses impactos.[34]

IV. ÉTICA E REGULAÇÃO

Partindo do ponto de vista de que a facilidade, a otimização de processos e as soluções de atendimento exercem um papel imprescindível no dia a dia das grandes corporações que trabalham com o público e que, em contrapartida a isso, não se almeja abrir mão da proteção de nossos dados pessoais e do direito à privacidade e vida íntima, é premente que façamos um exercício de ponderação, no sentido de melhor balancear os interesses controvertidos.

Essa ponderação se mostra essencial para a construção de uma base regulatória robusta, que respeite o indivíduo titular de direitos, mas que não suprima ao mesmo tempo os avanços tecnológicos e os interesses empresariais benéficos à sociedade.

Em confluência com este entendimento e voltando a abordar a lógica do Princípio da Precaução, não devemos nos olvidar das lições de Bruno Ricardo Bioni e Maria Luciano, que determinam:

> O princípio da precaução fornece um substrato importante para se pensar medidas e estratégias de regulação de IA, notadamente como lidar com situações de riscos de danos ou de desconhecimento dos potenciais malefícios e benefícios desse tipo de tecnologia. A automatização de processos de tomadas de decisão, a partir do emprego de IA, não deve se constituir como um argumento ingênuo em defesa de objetividade e neutralidade. Tais circuitos decisórios carregam escolhas das entidades e pessoas envolvidas na sua construção, sendo modulado pela agenda política e aspectos socioeconômicos, de forma implícita ou explícita, que lhes são subjacentes.[35]

Como destacado pelos autores, a transparência e a dita imparcialidade dos mecanismos de Inteligência Artificial podem não se revelar como exemplos a serem seguidos. A busca pela equidade de tratamento, por meio da objetividade e reflexão da realidade de uma IA, pode se mostrar um verdadeiro aparato de perpetuação de preconceitos e opressões, sob o risco de ser utilizada ainda para a preponderação de um monopólio ou até mesmo grupo político sobre o outro.[36]

---

[34] DE LIMA, Ana Paula M. Canto; HISSA, Carmina Bezerra; SALDANHA, Paloma Mendes. Direito Digital: Debates Contemporâneos 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 23

[35] FRAZÃO, Ana; MULHOLLAND, Caitlin. Inteligência Artificial e Direito: ética, regulação e responsabilidade. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. 228

[36] CARNEIRO, Tayná; FALCÃO, Cintia Ramos. Direito Exponencial: o papel da Novas Tecnologias no Jurídico do Futuro. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. p.415-416.

Neste cenário, buscando uma saída para mirar horizontes de igualdade de fato, encontra-se o princípio da *Accountability* desses sistemas, buscando não mais uma transparência literal e sem propósito, mas uma transparência qualificada, por intermédio dos relatórios de impacto à proteção de dados pessoais (RIPDP) e, acima de tudo, que ensejem ânimos de paridades de armas

Neste ritmo de transparência qualificada para gerar igualdade qualificada, é necessário entender que um processo de regulação prematuro e que não leve em consideração a precaução e os princípios da proteção de dados, livre concorrência, não discriminação, respeito aos direitos humanos, explicabilidade, segurança e desenvolvimento tecnológico pode trazer mais riscos aos direitos fundamentais ao vislumbrar a possibilidade de potencializar cargas e desigualdades históricas e socialmente construídas.[37]

Destacadas estas considerações com relação à regulação e sua íntima relação com a ética e a matérias intrinsecamente ligadas ao direito, partimos então para uma discussão mais empírica. Em muito se correlacionam a prática da advocacia e a utilização da Inteligência Artificial no direito de uma forma geral, e dissecar esta relação é a que se destina o próximo tópico.

V. APLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL NO DIREITO

Antes de adentramos ao tema, faz-se necessário destacar que a inteligência artificial não se confunde com a informática clássica aplicada ao Direito. Enquanto a informática clássica se limita a realizar tarefas ou procedimentos que já foram pré-estabelecidos pelo desenvolvedor, através da programação de algoritmos, a IA vai muito além, já que simula a inteligência humana e seus processos cognitivos, podendo inclusive ter autonomia decisória. [38]

Nesse sentido, a IA, aplicada ao mundo do direito, pode auxiliar o raciocínio jurídico, o conhecimento jurídico, a otimização de grande volume de informações processuais e, até mesmo, a hermenêutica jurídica.[39]

No que tange ao raciocínio jurídico, destaca-se que os processos decisórios, geralmente, são baseados em casos concretos similares, aplicando-se a jurisprudência. Desta forma, a IA, através do uso *softwares*, pode auxiliar a tomada de decisões, à medida em que será

---

[37] FRAZÃO, Ana; MULHOLLAND, Caitlin. Inteligência artificial e direito: ética, regulação e responsabilidade. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 209-210.
[38] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 8-9. ISBN 978-65-00-03948-1
[39] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 38. ISBN 978-65-00-03948-1

mais efetiva a busca por jurisprudência que possa ser aplicada a um caso concreto semelhante a outro já decidido. [40]

O conhecimento jurídico, disponível na forma de normas jurídicas, doutrina e jurisprudência, pode ser organizado, de maneira codificada e mapeada, pelos sistemas de computação, a fim de otimizar o trabalho jurídico. [41]

No que se refere ao grande volume de informações jurídicas, salienta-se que a expansão dos conteúdos do direito; o aumento constante do volume de instrumentos normativos: leis, decretos, portarias etc.; e a intensa mutabilidade do direito, pelas rápidas transformações sofridas pelo conteúdo dos instrumentos normativos, desafia as limitações cognitivas dos operadores humanos, daí decorrendo a importância da IA.[42]

Esse demasiado volume de informações jurídicas leva, à hermenêutica jurídica, a necessidade de criação de mecanismos de interpretação sofisticados com elasticidade conceitual e interpretativa, visando abranger situações não previstas pelas normas e captar o real sentido e alcance do texto normativo.[43]

Enquadrando-se o caso concreto no conceito abstrato da norma, há a aplicação do direito através da subsunção do fato à norma.[44] No entanto, nem sempre é possível a subsunção, já que a norma não consegue prever e disciplinar todos os acontecimentos que surgem pela dinâmica e complexidade das sociedades humanas.

Nesses casos, busca-se a integração do ordenamento jurídico, visando o preenchimento das lacunas conceituais que possam existir, através da analogia, dos costumes, dos princípios gerais de direito e da equidade.

Para preencher tais lacunas conceituais, lançando-se mão de inúmeros métodos interpretativos, há um grande desafio às habilidades cognitivas dos intérpretes humanos. Tal desafio decorre do grande volume de informações que precisa ser manipulado no processo de

---

[40] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 38. ISBN 978-65-00-03948-1
[41] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 38-39. ISBN 978-65-00-03948-1
[42] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 39. ISBN 978-65-00-03948-1
[43] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 39-40. ISBN 978-65-00-03948-1
[44] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 40. ISBN 978-65-00-03948-1

interpretação e subsunção da norma ao caso concreto. Para facilitar esse processo interpretativo, a IA pode ser uma grande aliada no sentido de potencializar as habilidades dos intérpretes do direito.

Para entender como funciona a aplicação da *expertise* tecnológica, propiciada pela inteligência artificial, é preciso abordar algumas técnicas da IA utilizadas no âmbito jurídico, como o raciocínio automatizado e a representação do conhecimento.

O raciocínio automatizado tem sido aplicado em sistemas computacionais na área jurídica. Inicialmente, na forma de sistemas especialistas e, mais recentemente, na forma de agentes de *software.* [45]

Os sistemas especialistas possuem conhecimento especializado sobre assuntos específicos do Direito e são utilizados para a tomada de processos decisórios e, no âmbito dos escritórios de advocacia, para a automatização de tarefas, redução de custos e aumento de lucratividade. Esses sistemas foram criados já nos anos 70 e 80.[46]

Esses sistemas, desenvolvidos na área jurídica, foram projetados com base em regras, por meio de inferências dedutivas do tipo "Se premissa (s) então conclusão", e com base em casos, por meio de inferências do raciocínio analógico do tipo "Se problema então solução", representando exemplos ou casos contendo soluções que poderão ser aplicadas em problemas semelhantes. [47]

Na área jurídica, podemos citar alguns sistemas especialistas, tais como: o Split-Up: baseado em regras que auxiliam na divisão de bens conjugais em casos de divórcio de acordo com a lei australiana;[48] e o CHIRON: sistema baseado em regras e em casos (sistema híbrido), cuja finalidade é fornecer suporte às decisões de planejamento tributário de acordo com a lei e os códigos tributários dos EUA. [49]

---

[45] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. ISBN 978-65-00-03948-1

[46] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 41. ISBN 978-65-00-03948-1

[47] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 41-42. ISBN 978-65-00-03948-1

[48] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 42. ISBN 978-65-00-03948-1 apud Zeleznikow, J., Stranieri, A., & Gawler, M. (1995). Project report: Split-Up-A legal expert system wich determines property division upon divorce. Artificial Intelligence and Law, 3 (4), 267-275.

[49] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 42. ISBN 978-65-00-03948-1apud Sanders, K. E. (1991, May). Representing and reasoning about open-textured predicates. In Proceedings of the 3rd international conference on Artificial intelligence and law, p. 137-144. ACM.

A representação do conhecimento, por sua vez, se dá através do processamento semântico, permitindo uma interpretação mais precisa das informações, normas e jurisprudências, favorecendo, assim, a tomada de decisão.

Nesta toada, infere-se que a aplicação das técnicas da IA é ampla e compreende, na prática, sistemas de pesquisa jurídica, estratégia de litígios, serviços jurídicos *online* de autoatendimentos, modelos de resolução de disputas, revisão e análise de contratos, análise de grandes volumes de dados ("big data"), tradução automática etc.

Nos Estados Unidos, por exemplo, a IA tem sido amplamente utilizada no sistema de *Contract Intelligence* – COIN, cuja função é interpretar acordos de empréstimo comercial e analisar acordos financeiros no âmbito dos bancos norte-americanos, sendo o JP Morgan Chase & Co. o maior deles.[50]

Com a aplicação dessa tecnologia de COIN, estudos têm demonstrado que o trabalho do advogado é reduzido em 360 mil horas ao ano, além de diminuir o número de equívocos na concessão de serviços de empréstimo ocasionados por erro humano.[51]

Nesse mesmo paradigma, podemos citar a tecnologia Chatbot DoNotPay, criada e colocada no mercado, em 2016, pelo programador Joshua Browder. O Chatbot é um robô que atua como um "advogado virtual" e atende no Reino Unido e em Nova York.[52]

A especialidade do robô, inicialmente, era a realização de contestação de multas por estacionamento em local proibido. Mas, diante do expressivo resultado de sucesso, atualmente a tecnologia tem sido empregada para casos de consumidores insatisfeitos com voos atrasados, na confecção de pedido de asilo de refugiados e no suporte a portadores de HIV que desejam entender melhor os seus direitos.

No Brasil, foi criada, em 2013, na cidade de São Paulo, a empresa Finch Soluções, visando o controle do contencioso de massa do escritório de advocacia JBM & Mandaliti. Pioneiramente, a empresa se destacou pela implementação de robôs de captura de informação,

---

[50] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. Inteligência Artificial no Direito: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018.
[51] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. Inteligência Artificial no Direito: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018 apud GALEON, Dom.; HOUSER, Kristin. An AI Completed 360,000 Hours of Finance Work in Just Seconds. 2017.
[52] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. Inteligência Artificial no Direito: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018.

automação e gestão de processos no mundo jurídico e, posteriormente, alargou a sua esfera de atuação para o setor de economia. [53]

Outro exemplo, a nível nacional, é a Looplex, plataforma utilizada para automação inteligente de documentos, como petições e contratos. Entre os serviços da inteligência artificial, oferecidos pela plataforma, há a busca por pesquisas jurídicas e a confecção de Smart Contracts.[54]

A Legal One é um outro exemplo dessa abordagem. De forma automatizada, a plataforma fornece conteúdo de embasamento para questões jurídicas e realiza a gestão e o controle de processos desde a fase inicial até o encerramento.

Desta forma, podemos ver como o expressivo avanço da Tecnologia Artificial, tanto a nível nacional quanto internacional, tem demonstrado aumento da produtividade, redução de custos e melhora na qualidade dos serviços prestados.

VI. CONCLUSÃO

O objetivo do presente artigo foi analisar a importância da Inteligência Artificial no mundo jurídico, abordando desde a parte teórica do assunto até a parte empírica de como essa tecnologia pode ser aplicada na prática, sem a pretensão de exaurir este tema tão vasto. A partir disso, chegamos à conclusão de que a IA exerce um papel essencial no desenvolvimento dos trabalhos realizados pelos operadores do Direito.

Em uma realidade caracterizada por um Judiciário congestionado, ou seja, com excesso de demanda, a IA pode ser a solução para dinamizar, efetivar e otimizar os processos decisórios. Isso não significa dizer que o trabalho humano será substituído por operadores autômatos, uma vez que o uso da Inteligência Artificial, nesse contexto, teria por finalidade aumentar a capacidade operativa dos profissionais do Direito, tornando-os capazes de lidar com o excesso de demanda e com o grande volume de informações jurídicas de uma forma mais pragmática, célere e efetiva.

Todavia, apesar dos benefícios que a IA concede ao mundo jurídico, não podemos negar que a falibilidade das ferramentas tecnológicas, bem como a perspectiva influenciadora dos

---

[53] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. Inteligência Artificial no Direito: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018.
[54] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. Inteligência Artificial no Direito: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018.

vieses algorítmicos, apresentam riscos ao preceito constitucional do *due process of law*, gênese das garantias constitucionais como igualdade, publicidade, imparcialidade e segurança jurídica, devendo a matéria ser, portanto, regulada com atenção aos princípios da precaução e *accountability*, de modo que possamos gozar de seus benefícios sempre observando e controlando os respectivos riscos.

Ex positis, no âmbito de utilização das IA's, é essencial que os profissionais da área jurídica recorram à ética como instrumento de salvaguarda dos direitos fundamentais, vislumbrando-se a possibilidade de revisão das decisões automatizadas.

VII. REFERÊNCIAS BIBLIOGRÁFICAS

FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. **Inteligência Artificial no Direito: Uma realidade a ser desbravada.** Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018.

GIRARDI, Rosario**. Inteligência Artificial Aplicada ao Direito**. 1. ed. Edição do autor. Brasil: 2020, ISBN 978-65-00-03948-1.

DONEDA, D.C.M.; MENDES, L.S.; SOUZA, C.A.P.; ANDRADE, N.N.G. **Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal.** Pensar: Revista de Ciências Jurídicas, Fortaleza, v.23, n.4, p. 1-17, out./dez.2018.

FRAZÃO, Ana; MULHOLLAND, Caitlin. **Inteligência Artificial e Direito: ética, regulação e responsabilidade.** 1ª ed. São Paulo: Thomson Reuters Brasil, 2019.

CARNEIRO, Tayná; FALCÃO, Cintia Ramos. **Direito Exponencial: o papel da Novas Tecnologias no Jurídico do Futuro.** 1ª ed. São Paulo: Thomson Reuters Brasil, 2020.

FEIGELSON, Bruno; MALDONADO, Viviane Nóbrega. **Advocacia 4.0.** 1ª ed. São Paulo: Thomson Reuters Brasil, 2019.

GABRIEL, Martha. **Você, Eu e os Robôs: Pequeno Manual do Mundo Digital.** 1ª ed. São Paulo: Atlas, 2018.

MAGRANI, Eduardo. **Entre Dados e Robôs: Ética e Privacidade na Era da Hiperconectividade**. 2ª ed. Porto Alegre: Arquipélago Editorial, 2019.

DE LIMA, Ana Paula M. Canto; HISSA, Carmina Bezerra; SALDANHA, Paloma Mendes. **Direito Digital: Debates Contemporâneos.** 1ª ed. São Paulo: Thomson Reuters Brasil, 2019.

SOBRE O CONSENTIMENTO NA LGPD

Alan Mateus Sampaio de Souza
Alcinéa da Silva Macedo

Resumo: O presente artigo visa analisar a importância do consentimento em face da LGPD no que se refere ao tratamento de dados pessoais no Brasil. Partindo de conhecimentos primevos busca-se uma compreensão mais precisa e satisfatória a fim de instigar a reflexão e promover a conscientização do leitor sobre o novo dispositivo prestes a entrar em nosso ordenamento pátrio. A pesquisa realizada é bibliográfica, tendo como embasamento a Lei de nº13.709/18 e seus incisos 7º ao 16.

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados, sob o número 13.709/2018, conhecida como LGPD,de nacionalidade brasileira, além da semelhança com o Regulamento Geral de Proteção de Dados (ou GDPR, na sigla em inglês), em vigor nos países que compõem a União Europeia desde maio de 2018, guarda também em seu objeto a complexidade normativa. À similitude ambos os dispositivos jurídicos legislam sobre a proteção dos dados pessoais.

Previa-se que a LGPD viesse complementar a Lei n. 12.965/11 conhecida como Marco Civil da Internet – MCI , já no ano de 2014. No entanto, passados 8 anos desde a entrada em vigor da lei 12.965, em maio de 2014, só agora o legislador buscou estabelecer coesão para que essas duas leis se complementassem, formando um sistema coeso.

No entanto, com previsão de entrada em vigor em fevereiro de 2020, a relação entre LGPD e MCI é muito mais complexa do que aparenta. Não havendo posição assente sobre complementaridade entre ambas.

Neste artigo, que discorre sobre o tratamento de dados pessoais, o enfoque será dado ao que se compreende como Tratamento de Dados Pessoais, localizado entre os artigos 7° e 16 da lei de nº 13.709/18-LGPD.

Ao fazermos uma leitura superficial dos artigos da LGPD acima citados foi possível observar o emprego do vocábulo “consentimento” 25 vezes, como se destaca no art.7º, inciso I (grifo nosso):

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de **consentimento** pelo titular.

2. DO CONSENTIMENTO NA LGPD E DE ALGUNS QUESTIONAMENTOS

De acordo com o site do Sepro.gov,

> Se a gente fosse eleger a principal palavra da Lei Geral de Proteção de Dados Pessoais (LGPD), a escolhida seria, sem dúvidas, CONSENTIMENTO. É o titular, ou seja, a pessoa a quem se referem os dados que deve, se quiser - ao ser questionada, de forma explícita e inequívoca - autorizar que suas informações sejam usadas, por empresas e órgãos públicos, na hora da oferta de produtos e serviços, gratuitos ou não.
>
> Portanto, com a nova lei, fica claro que quem é o verdadeiro dono do dado não é aquele que o utiliza, nem aquele que o salvaguarda em bancos de dados. Nada disso, o dado pessoal é estritamente da pessoa a quem ele diz respeito. Na teoria isso parece algo óbvio, mas na prática não é bem assim. E tem muito dado particular sendo usado para fins que seu dono ou dona real sequer sabem. Usos, inclusive, que podem até mesmo prejudicá-los.

No entanto, o dispositivo jurídico em análise não fornece a devida clareza sobre o que vem a ser o referido "consentimento*"* e como este se materializa na vida prática de um cidadão que adquire um frasco de antiácido estomacal na farmácia e digita seu CPF antes mesmo de abrir a carteira para pagar por este. Nesse momento o cidadão pode questionar qual a finalidade de fornecer seu CPF, visto que é um dado seu.

Como todo novo dispositivo inserto na seara jurídica pátria, a LGPD traz questionamentos dignos de confrontações linguísticos e em relação aos demais dispositivos positivados e já vigentes. Buscando dirimir possíveis confrontações, o art. 5º da LGPD traz uma definição do que se entende por "consentimento":

> Art. 5º Para os fins desta Lei, considera-se:
> [..]
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Tal definição do vocábulo é vaga, pois não dispõe sobre os modos como o consentimento poderá ser exteriorizado. Não é deixado claro se o silêncio poderá ser interpretado como uma forma de consentimento. Sendo assim, omissões poderiam tornar viáveis algumas formas de abuso por parte do Estado ou de alguma empresa privada?

De acordo com Hewdy Lobo (2015),

> São vícios do consentimento, como o erro, o dolo e a coação**, que se fundam no desequilíbrio da atuação volitiva relativamente a sua declaração**. Esses vícios aderem à vontade, aparecem sob forma de motivos que forçam a deliberação e **estabelecem divergência entre a vontade real, ou não possibilitam que esta se forme**.
> São assim mencionados porque o indivíduo está "viciado" no momento da manifestação da sua vontade. Se a pessoa, ou seja, o declarante tivesse real

> conhecimento da situação, não teria manifestado sua vontade da forma a qual foi declarada (grifo nosso)

Nesse sentido, o silêncio pode ser entendido como uma manifestação de vontade eivada de vícios. Para exemplificar, suponhamos um contrato de adesão de 50 páginas e que haja uma cláusula prevendo que o contratante deve entrar em contato na data x sob o risco de não o fazê-lo culminar em autorização para o tratamento de seus dados. Os leitores comum e mediano brasileiros não terão a devida paciência que a leitura deste referido contrato exige.

A LGPD em seu artigo 7º, parágrafo 5º prossegue no campo do consentimento ao instituir a exigência do "consentimento específico", novamente o vocábulo, ainda que associado a um adjetivo, mantém-se vago quanto à sua materialização.

> [...]
> §5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei (grifo nosso).

Nesse sentido, o consentimento específico seria apenas para uma finalidade específica, ou seja, não abarcando questões mais gerais.

Nos artigos que se seguem, do 8° ao 10°, tem se uma das formas de materialização do consentimento que deverá ser por escrito, com cláusula destacada das demais cláusulas contratuais. (art.8º,§1º). Aqui observamos um diálogo de fontes entre o Novo Código Civil de 2002 e a LGPD.

Na parte que trata sobre os contratos, o Novo Código Civil prima por princípios como a boa fé e a função social do contrato, ambos previstos no Código Civil:

> "Art. 421. A liberdade de contratar será exercida em razão e nos limites da função social do contrato.
>
> Art. 422. Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé."

Assim, depreende-se que os contratos para tratamento de dados devem observar princípios como boa fé e a função social do contrato.

O artigo 8° da LGPD prevê forma diversa, que não escrita, de manifestação da vontade do titular. No entanto, não há quaisquer referências às demais formas de consentimento, sendo vedado ao controlador o tratamento de dados eivados de vícios de consentimento.

O mesmo artigo 8° da LGPD, em seu §5º, prevê ainda a revogação do consentimento por parte do titular de forma manifestamente expressa. As perguntas que ficam são muitas : De qual forma essa manifestação deverá ocorrer? Por meio eletrônico, telefônico ou impresso? Em tempos de praticidade e pouca mobilidade urbana, cabe o envio de mensagens por meio de aplicativo para que a revogação se corporifique?

E a pergunta crucial: O que são meios gratuitos e facilitados?

Em consulta ao site da Comissão Europeia - www.ec.europa.eu, é possível verificar uma página dedicada às leis. Sob o título de Data protection, visualizamos explicações didáticas sobre os termos aos quais nos dedicamos à compreensão em linhas anteriores e que não se mostram tão explícitos em nosso ordenamento pátrio.

2.1. DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS NA LGPD

Em relação aos dados sensíveis, observamos que o vocábulo "consentimento*"* aparece 3 vezes entre os artigos 11 e 13.

Observamos uma preocupação por parte do legislador que estes dados só sejam tratados mediante "consentimento explícito", entendido, segundo a GDPR, como dado através de um ato positivo (por exemplo, marcar explicitamente um espaço ou apor uma assinatura num formulário).

Ainda assim o ordenamento prevê as situações em que o tratamento de dados sensíveis é indispensável, independentemente de consentimento do titular, o que pode ser exemplificado em situações ligadas: a políticas públicas; os estudos via órgão de pesquisa; a um direito, em contrato ou processo e à preservação da vida e da integridade física de uma pessoa, entre outros.

Assim, observamos que os dados sensíveis, pelo potencial discriminatório que apresentam, além de poderem ser utilizados de forma criminosa por aqueles adeptos ao extremismo, devem ser protegidos de forma mais rígida.

Em um país onde as desigualdades sociais, raciais e econômicas são abissais devemos sempre nos preocupar com o grau de proteção desses dados e os limites para seu tratamento.

2.2. DO TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E DE ADOLESCENTES

A RGPD, de matriz europeia, não deixou de dar proteção a estes , para tanto, em caso de tratamento de dados pessoais referentes a uma criança, tem de obter o *consentimento* parental.

Há de se observar peculiaridades, uma vez que o limiar etário varia entre os 13 e os 16 anos nos diferentes países da União Europeia, por isso é aconselhável consultar a legislação nacional entre países que a compõe.

A LGPD também não deixou de fora as crianças e os adolescentes, em seu artigo 14 fez ressalvas sobre estes que são classificados como tais. A nova lei tutela não apenas os dados virtuais e online - o texto normativo traz disposições que concernem a todos, escolas, clubes, hotéis e toda sorte de entidades públicas e privadas que lidam com informações relativas a crianças e adolescentes.

O Estatuto da Criança e do Adolescente-ECA, disciplinado pela Lei 8.069/1990 definiu a faixa etária de cada grupo: "Art. 2º Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade."

O legislador preocupou-se além da necessidade de *consentimento específico* por pelo menos um dos pais ou responsável legal, e ateve-se também com o uso do vocabulário a ser usado no que se refere às informações sobre tratamento de dados.

O vocabulário a ser empregado deve ser compreensível aos pais, responsáveis e também à criança, por conseguinte é nosso o entendimento de que o mesmo deve se dar em relação aos adolescentes, visto que também desenvolvem linguajar próprio nesta fase transitória da vida em que não se é criança tampouco adulto.

> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Deste inciso 6º podemos depreender que há, ainda que de forma implícita, uma referência àqueles que são portadores de necessidades especiais, e que se encontram amparados pela Lei 13.146/2015-Estatuto da Pessoa com Deficiência, a ideia de uso de recursos para uma melhor compreensão de crianças e adolescentes faz reforçar nossa perspectiva de não esquecimento destes.

Será possível estabelecer tratamento de dados em conjunto com o Cadastro Nacional de Inclusão da Pessoa com Deficiência (Cadastro-Inclusão) instituído por meio do Decreto 8.954, de 2017 ?

Tal cadastro reúne em um registro público eletrônico informações pelas quais será possível identificar e processar a caracterização socioeconômica da pessoa com deficiência, neste

aspecto verifica-se o diálogo das fontes- LGPD, Estatuto da Pessoa com Deficiência, ECA e Cadastro Nacional de Inclusão da Pessoa com Deficiência.

Se houve tal intenção por parte do Legislador, podemos visualizar grandes avanços na questão da inclusão, partindo de crianças e adolescentes até àqueles que são muitas vezes esquecidos pelos demais segmentos sociais.

Como um dispositivo novo a entrar em vigor, a LGPD traz lacunas que têm sido alvo de questionamentos, entre elas podemos citar: Qual órgão fiscalizará o tratamento de dados de crianças e adolescentes? Com qual idade será dispensável o consentimento dos pais/responsáveis legais para o tratamento de dados de uma criança/adolescente?

Além disso, a lei diz que o consentimento de crianças e de adolescentes ocorre perante a manifestação de seus pais ou representantes legais. Entretanto, muitas crianças e adolescentes possuem redes sociais e, por consequência, assinam contratos de adesão e dão consentimento sobre o tratamento de seus dados pessoas. Assim sendo, qual é a consequência prática disso, de quem é a responsabilidade e qual é o papel da LGPD nisso?

Esse é um outro ponto em que resta uma lacuna jurídica.

3. DOS REQUISITOS DE CONSENTIMENTO

Discorremos ao longo do artigo em tela sobre a necessidade de consentimento em diferentes situações de tratamento de dados: de Dados Pessoais, de Dados Pessoais Sensíveis e por fim, de Dados Pessoais de Crianças e Adolescentes.

Cabe releitura do artigo 5º, inciso XII da LGPD onde se tem a definição do termo em voga:

> "Art. 5º Para os fins dessa lei, considera-se:
> [...]
> XII: consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;"

Assim, compreendemos que o *consentimento* é pressuposto de validade dado ao tratamento de dados e suas manifestações, para ser válida, deve ser constituída de quatro elementos:

(a) Consentimento livre: O usuário não pode ser obrigado a consentir com o tratamento de seus dados pessoais para ter acesso a determinada aplicação de internet. Nesse caso, o consentimento do usuário não é considerado livremente fornecido, podendo o contrato ser invalidado por ineficácia da aceitação;

(b) Consentimento informado: É o consentimento em que são prestadas ao usuário informações sobre a identidade da empresa responsável pelo tratamento de dados e as finalidades a que o tratamento se destina;

A aceitação do usuário, como ato jurídico, sujeita-se ainda aos chamados vícios de consentimento (erro, dolo, coação, etc.), os quais, quando verificados, importam na ineficácia da manifestação de vontade e consequente nulidade do vínculo contratual;

(c) Consentimento inequívoco: É aquele em que deve haver uma ação por parte do usuário indicando sua aceitação, seja pelo envio de um e-mail, assinatura eletrônica, ou até mesmo por um clique em local determinado.

O silêncio do usuário não pode ser considerado consentimento; e

(d) Finalidade específica e determinada: A coleta de dados deve estar sempre vinculada a uma ou mais finalidades específicas e informadas na respectiva Política de Privacidade, sendo coibido o uso de dados para fins não previstos, sem prévio consentimento do usuário.

CONCLUSÃO

A LGDP, como novo dispositivo inserido no ordenamento jurídico pátrio, vem disciplinar o tratamento dos dados pessoais dos nacionais. Ainda que tenhamos provedores de internet muito aquém de países desenvolvidos, somos constantemente surpreendidos com vazamento de dados pessoais e sensíveis capazes de promover prejuízos de diferentes esferas de nossas vidas.

Ainda falta discernimento ao brasileiro médio sobre o que seus direitos e deveres, bem como interesse por atos que são praticados de forma automatizada sem muita reflexão sobre seus danos futuros -digitar o CPF na farmácia, preencher um formulário de loja, entre tantas ações diárias e tidas como triviais em que fornecemos nossos dados sem qualquer questionamento.

Ou seja, é possível que um indivíduo venha a conceder os seus dados para tratamento sem saber porque o faz, e nesse ponto, a LGPD, ao não discorrer sobre os tipos de consentimento que devem ser adotados, deixou de disciplinar um dos pontos cruciais dos tratamento de dados pessoais, que são os tipos de consentimento.

Neste artigo buscamos relacionar importantes dispositivos vigentes para elucidar pontos nos quais encontramos certa obscuridade semântica - ECA, Estatuto da Pessoa com Deficiência, entre outros que vislumbramos alguma conexão, ainda que tênue.

O Código Civil em seu Título V, Capítulo I, Seção I, disciplina os contratos, assim entendemos que o *consentimento* presume um acordo de vontades, onde deve prevalecer os princípios de probidade e boa-fé, visto que o tratamento de dados se estende a diferentes esferas do indivíduo.

REFERENCIAS:

BRASIL. Código Civil, Lei 10.406, de 10 de janeiro de 2002.

Dados pessoais, dados anônimos e dados sensíveis – arts. 5º, 12 e 13. Pensando o Direito. Disponível em: <*http://pensando.mj.gov.br/dadospessoais/eixo-de-debate/dados-pessoais-dados-anonimos-e-dados-sensiveis/*> Acesso em 2/12/2019.

Dados Sensíveis**.** Serpro. Disponível em <https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-sensiveis-lgpd>. Acesso em 2/12/2019 as 16:25

LOBO, Hewdy. **O que é vício de consentimento ?** Jus.com.br, 2015. Disponível em <https://jus.com.br/artigos/43994/o-que-e-vicio-de-consentimento>. Acesso em 23/10/2019.

Fundamento jurídico do tratamento de dados**.** Comissão Europeia. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data_pt>. Acesso em 2/12/2019.

Lei Brasileira de Inclusão**.** Senado. Disponível em : https://www12.senado.leg.br/noticias/materias/2016/01/21/lei-brasileira-de-inclusao-entra-em-vigor-e-beneficia-45-milhoes-de-brasileiros. Acesso em 2/12/2019.

LGPD e os dados de crianças e adolescentes. Cadv. Disponível em :<https://cadv.adv.br/2019/06/18/a-lgpd-e-os-dados-de-crians-e-adolescentes/> Acesso em 2/12/2019 as 19:05

LGPD foi desenvolvida com inspiração em legislação aprovada na Europa. Serasa experian, 2018. Disponível em: <https://www.serasaexperian.com.br/conteudo_lgpd/aspectos-da-gpdr>. Acesso em 1/12/2019.

O que é Consentimento. Significados.com. Disponível em: <https://www.significados.com.br/consentimento/>. Acesso em 23/10/2019.

O RGPD: novas oportunidades, novas obrigações. OP Europa Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/44d8441b-5fc5-11e8-ab9c-01aa75ed71a1/language-fr>. Acesso em 2/12/2019.

Termos de Consentimento informado. Unimed. Disponível em: <https://www.unimed.coop.br/web/regionalsulgoias/servicos/hospital-unimed/termo-de-consentimento/termos-de-consentimento-informado?inheritRedirect=true&redirect=%2Fweb%2Fregionalsulgoias%2Fservicos>. Acesso em 23/10/2019.

Tipos de Consentimento e Proteção de Dados Pessoais: Um Breve Histórico. Instituto de referência em Internet e Sociedade, 2018. Disponível em: <http://irisbh.com.br/tipos-de-consentimento-e-protecao-de-dados-pessoais/>. Acesso em 23/10/2019.

Tirando algumas situações previstas na LGPD, é você, cidadão, que define se seus dados pessoais podem ou não ser tratados por terceiros. Sepro.gov. Disponível em: <https://www.serpro.gov.br/lgpd/cidadao/seu-consentimento-e-lei> Acesso em 23/10/2019.

ANPD – ASPECTOS GERAIS E CRÍTICA

Marcos Da Silva Pereira

RESUMO: A proteção dos dados pessoais ganhou crescente importância ao longo dos anos, com o avanço da tecnologia e os seguidos vazamento de dados virtuais, bem como a constatação de que tem ocorrido uso comercial não autorizado destes dados. A experiência no direito comparado tem demonstrado que é essencial para o sucesso de uma lei de proteção de dados pessoais a criação de um órgão estatal efetivo e independente. O governo brasileiro editou a LGPD sem a criação concomitante da ANPD, que até o momento permanece sem estrutura física para atuar, o que pode ter se revelado bastante prejudicial para o sucesso da LGPD. Os primeiros passos na criação da ANPD por parte do atual governo brasileiro têm demonstrado possível ingerência política, o que vem preocupando parte do Poder Legislativo, do segmento empresarial e da OCDE.

1. INTRODUÇÃO

Com o avanço da tecnologia, em especial das telecomunicações, a proteção dos dados pessoais tornou-se cada vez mais necessária. Tal preocupação ficou ainda mais evidente nos seguidos escândalos de vazamento de dados pessoais, como o Wikileaks, a rede de espionagem governamental revelada por Edward Snowden, bem como o Cambridge Analytica e a rede social Facebook, este envolvendo cerca de 87 milhões de usuários[55].

Neste ínterim, as redes sociais também ganharam um papel relevante. Criadas inicialmente com o propósito de conectar pessoas, ao longo dos anos acumularam uma grande base de dados pessoais. A retenção de dados pessoais ficou tão banalizada a ponto de Zuckerberg, criador da rede social Facebook, declarar, em 2010, que a "era da privacidade acabou"[56].

Conceitos como *data mining*, *big data* e *business inteligence*[57] ganharam importância no meio empresarial, pelo potencial de preverem tendências e aumentarem as vendas, seja dos produtos oferecidos, seja dos próprios dados em si para terceiros, envolvendo uma grande base de dados pessoais alheia ao conhecimento de seus proprietários.

Estes são apenas alguns exemplos da importância de se proteger os dados pessoais, preocupação que passou a ficar mais marcante no ano de 2018, com o vazamento de dados

[55] Disponível em https://www.bbc.com/portuguese/geral-43646687 último acesso em 10/12/2020.
[56] Disponível em https://m.folha.uol.com.br/tec/2010/01/677794-era-da-privacidade-na-internet-acabou-diz-fundador-do-facebook.shtml último acesso em 12/12/2020.
[57] Disponível em https://www.selecthub.com/business-intelligence/bi-vs-big-data-vs-data-mining/ último acesso em 10/12/2020.

provocados pela consultoria Cambridge Analytica[58], quando vários governos no mundo criaram legislações protetivas da intimidade e da privacidade, como foi o exemplo da União Europeia[59].

Neste sentido, também o Brasil tem a incumbência de proteger os dados pessoais de seus cidadãos, não só por meio da edição de normas protetivas, mas também com a criação de um órgão que efetivamente fiscalize, coíba atos ilícitos e crie uma cultura em que as pessoas voluntariamente reconheçam a importância do tema e atuem em sentido preventivo.

No entanto, o Brasil revelou grandes descompassos legislativo e administrativo entre a edição de uma norma protetiva de dados pessoais e a criação da autoridade que os garanta, o que pode comprometer a efetividade da legislação e, principalmente, a criação de uma cultura de proteção de dados pessoais.

2. O CONTEXTO BRASILEIRO – A LGPD VIGENTE SEM UMA AUTORIDADE QUE A GARANTISSE

A LGPD no Brasil tem raízes no ano de 2010[60], com uma consulta pública que debateu o anteprojeto de lei. No entanto, somente em 2018, impulsionado pelo vazamento da Cambridge Analytica, o Brasil se mobilizou, com a elaboração da Lei Geral de Proteção de Dados – LGPD, que ainda contou com *vacatio legis*.

Contudo, a norma foi editada sem que o órgão responsável por garanti-la, a ANPD, sequer fosse criado no mesmo ato. O presidente em exercício à época, Michel Temer, vetou[61] a criação da ANPD sob o argumento de inconstitucionalidade formal do processo legislativo, por afronta ao artigo 61, § 1º, II, 'e', cumulado com o artigo 37, XIX da Constituição.

Posteriormente, por meio da Medida Provisória 869, de 27 de dezembro de 2018, foi criada a ANPD. No entanto, as medidas provisórias possuem eficácia limitada temporalmente, por

---

[58] Disponível em https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018 último acesso em 13/12/2020.

[59] Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679 último acesso em 12/12/2020.

[60] idem

[61] Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm último acesso em 13/12/2020.

60 dias prorrogáveis por igual período, não se revelando o instrumento normativo mais adequado dada a importância do tema.

Assim, somente em 8 julho de 2019 foi sancionada a Lei nº 13.853, já no mandato do Presidente Jair Bolsonaro. No entanto, também nesta ocasião a ANPD não escapou de vetos, que versaram sobre a possibilidade da ANPD aplicar determinadas sanções. Na ocasião, o Presidente justificou o veto da seguinte forma:

> As novas sanções impossibilitariam o funcionamento de bancos de dados essenciais a diversas atividades públicas e privadas, como os utilizados por instituições financeiras, podendo até acarretar prejuízo à estabilidade do sistema financeiro nacional, bem como a entes públicos, com potencial de afetar a continuidade de serviços públicos[62]

No entanto, o Congresso Nacional derrubou tais vetos, restabelecendo a ampliação do rol de sanções administrativas que podem ser aplicadas aos agentes de tratamento de dados.

Em que pese a ANPD ter sido criada em julho de 2019, ainda não foi naquela ocasião em que a autoridade passou a atuar. Somente em 26 de agosto de 2020 foi editado o Decreto 10.474/2020, que "Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança", norma que também não escapou de polêmicas, conforme será abordado no tópico sobre os órgãos da ANPD.

Até o fechamento deste artigo, em que pese a norma supracitada tenha criado a estrutura regimental e os cargos da ANPD, ainda não há estrutura física e pleno funcionamento da autoridade, num descompasso com a criação da LGPD que já dura quase dois anos.

Uma das funções da ANPD é justamente a criação de uma cultura de proteção de dados pessoais, como prevê o art. 55-J, VI da LGPD. Ou seja, idealmente esta autoridade deveria ter sido criada até mesmo antes da LGPD, o que indica o grande descompasso legislativo no caso brasileiro.

---

[62] Disponível em https://www.camara.leg.br/noticias/628942-vetos-derrubados-pelo-congresso-sobre-a-autoridade-de-protecao-de-dados-sao-promulgados/ último acesso em 13/12/2020.

3. A IMPORTÂNCIA DA ANPD

A ANPD tem previsão a partir do art. 55 da LGPD, mas é mencionada em mais de 50 dispositivos ao longo da lei, o que não deixa dúvidas acerca do seu papel de garantir efetividade à norma em destaque.

A LGPD prevê extenso rol de competências para a ANPD, que possui 24 incisos. Dentre eles, Teffé[63] destaca:

> a) zelar pela proteção dos dados pessoais e pela observância dos segredos comercial e industrial; b) fiscalizar e aplicar sanções (tanto ao setor público quanto ao privado), em caso de tratamento de dados realizado em descumprimento à legislação; c) apreciar petições de titular contra controlador, após comprovada a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; d) promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados e das medidas de segurança; e) estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; f) dispor sobre as formas de publicidade das operações de tratamento de dados pessoais; g) solicitar às entidades do poder público que realizem operações de tratamento de dados informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; h) editar regulamentos e procedimentos sobre proteção de dados, bem como sobre os relatórios de impacto; e i) realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização sobre o tratamento de dados efetuado pelos agentes de tratamento, incluído o poder público.

Relevante destacar que a proteção dos dados pessoais é, segundo Teffé e Viola[64], um dos requisitos para que o Brasil e sua legislação sejam reconhecidos como adequados ao modelo de tratamento de dados pessoais estabelecido na Europa por meio do GDPR. Segundo os autores, na América do Sul, apenas Argentina e Uruguai receberam essa chancela até o momento.

A proteção de dados pessoais por meio de uma autoridade forte e independente também se revelou de suma importância para que o Brasil ingresse na OCDE[65], o que recentemente

---

[63] Disponível em https://www.jota.info/opiniao-e-analise/artigos/por-que-precisamos-de-uma-autoridade-nacional-de-protecao-de-dados-07012020 último acesso em 11/12/2020

[64] Disponível em https://itsrio.org/wp-content/uploads/2018/12/autoridade-protecao-de-dados.pdf último acesso em 13/12/2020.

[65] Disponível em https://www.consumidormoderno.com.br/2019/03/20/relacao-lgpd-desejo-brasil-ocde/ último acesso em 13/12/2020.

foi reforçado pela organização por meio de extenso relatório[66]. Até o momento, na América Latina apenas Chile, Colômbia e México garantiram o ingresso na organização[67], que se revelou uma das prioridades do governo Bolsonaro[68].

Também é essencial que haja uma efetiva cooperação internacional entre os estados, pois os dados pessoais são transfronteiriços, o que levou a OCDE a editar diretrizes para a sua efetiva proteção[69]. Multinacionais, redes sociais e organizações privadas de diversas naturezas manipulam dados pessoais, de modo que é essencial que haja uma efetiva cooperação estatal por meio de suas autoridades de proteção de dados.

A importância do órgão também é destacada pelo segmento empresarial. Mais de 80 entidades[70] de diversos setores assinaram carta aberta reforçando a necessidade de que a ANPD tenha efetividade, bem como haja independência técnica na escolha de seus membros.

Evidente, portanto, que a atuação da ANPD não só é primordial para a garantia de direitos fundamentais sob grande ameaça no atual contexto das telecomunicações como também cria segurança jurídica para que pessoas e organizações realizem negócios e tenham meios de evitar que segredos comerciais e industriais sejam vazados em operações ilícitas.

4. ANPD NO DIREITO COMPARADO

A experiência internacional vem demonstrando o papel essencial da ANPD na proteção dos dados pessoais, especialmente pelo caráter transfronteiriço do objeto, como foi abordado.

Teffé e Viola[71] destacam o papel da autoridade no Reino Unido, França, Itália e Argentina. No caso do Reino Unido, o chamado Gabinete do Comissário de Informação trata-se de autoridade regional e não nacional, vinculado ao Parlamento e não ao Executivo, remunerado

---

[66] Disponível em https://www.oecd.org/digital/a-caminho-da-era-digital-no-brasil-45a84b29-pt.htm?utm_campaign=newsletter_-_27102020&utm_medium=email&utm_source=RD+Station último acesso em 13/12/2020.

[67] Disponível em https://g1.globo.com/mundo/noticia/2020/04/28/colombia-se-torna-o-37o-pais-membro-da-ocde.ghtml último acesso em 13/12/2020.

[68] Disponível em https://economia.uol.com.br/noticias/redacao/2020/10/19/bolsonaro-exalta-parceria-com-trump-e-diz-entrar-na-ocde-e-firme-proposito.htm último acesso em 13/12/2020.

[69] Disponível em http://www.oecd.org/sti/ieconomy/15590254.pdf último acesso em 13/12/2020.

[70] Disponível em https://www.abracom.org.br/2020/09/8075/ último acesso em 13/12/2020.

[71] Disponível em https://itsrio.org/wp-content/uploads/2018/12/autoridade-protecao-de-dados.pdf último acesso em 12/12/2020.

exclusivamente por taxa. O órgão tem a seu dispor para exercer sua autoridade algumas ferramentas, como[72]:

> estabelecer processo criminal, penalidades monetárias, aplicação e fiscalização do cumprimento da lei e, em algumas circunstâncias, auditoria. O comissário de informações. Também tem o poder de aplicar multa monetária em um controlador de dados. As ferramentas não são mutuamente exclusivas, podendo ser aplicadas de forma combinada, a depender do caso

No caso italiano, a autoridade é independente, autônoma e transparente, transparência compreendida como "a acessibilidade total das informações relativas à organização e atividade do garantidor". Tem como princípios lealdade, imparcialidade, integridade, confidencialidade e cumprimento adequado dos deveres e atua na prevenção contra todas as formas de corrupção.

No exemplo francês, trata-se de autoridade administrativa de controle independente totalmente autônoma das demais atividades desempenhadas pelo Estado francês e autoridades públicas ou privadas "não podem se opor à ação da comissão ou de seus membros e devem tomar todas as medidas cabíveis a fim de facilitar sua atividade" e publica anualmente um relatório de prestação de contas demonstrando resumidamente os serviços prestados naquele ano.

Na Argentina, a autoridade é intitulada como Direção Nacional de Proteção de Dados órgão vinculado ao Ministério da Justiça e dos Direitos Humanos, mas com a ressalva, em lei, de que o Diretor da autoridade somente poderia ser exonerado pelo Poder Executivo por mal desempenho das suas funções.

Teffé e Viola pontuam, ainda, que a Argentina também sofreu críticas pelo risco à independência do órgão, mas foi proativa neste sentido, com as correções necessárias:

> A Direção Nacional de Proteção de Dados Pessoais ser órgão da administração direta vinculado a um ministério foi objeto de críticas quanto à sua real independência. Não por acaso, em 2017, após a aprovação do GDPR, a autoridade de controle Argentina tornou-se a Agência de Acesso à Informação Pública (Agencia de Acceso a la Información Pública), criada sob o regime de autarquia, com todas as características de uma autoridade independente, o que inclui autonomia funcional e financeira, diretor com mandato fixo e pessoal técnico e administrativo dedicado.

[72] idem

Em Portugal, a autoridade é exercida pela Comissão Nacional de Proteção de Dados[73], "entidade administrativa independente com poderes de autoridade, que funciona junto da Assembleia da República" que tem "atribuição genérica controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na Lei".

O modelo português tem obtido considerável sucesso nas pesadas sanções aplicadas aos violadores da Lei, com multas que em alguns casos podem chegar a 80 mil euros[74], ao passo que no modelo brasileiro o Poder Executivo, tanto com o Presidente Michel Temer quanto com Jair Bolsonaro houve uma tentativa de mitigar as sanções, mas que foi barrada pelo Poder Legislativo, como já foi estudado.

Não obstante, segundo Teffé e Viola, o Brasil optou por seguir modelo semelhante a países como Malta e Luxemburgo[75], "totalmente financiados pelo Estado conseguem aumentar suas receitas por meio, por exemplo, de multas impostas a controladores, em razão do cometimento de infrações por descumprimento da lei de proteção de dados".

No entanto, é possível observar que as linhas gerais adotadas pelos países europeus e a Argentina também estão presentes no modelo de autoridade brasileiro. Resta verificar como será na prática a atuação da autoridade, até mesmo porque ainda tramitam no Congresso iniciativas que têm por objetivo mitigar a responsabilidade dos violadores, o que pode enfraquecê-la[76].

5. NATUREZA JURÍDICA

O projeto de lei 4060/2012, de relatoria do Deputado Orlando Silva (PC do B), previu que a ANPD seria uma autarquia especial, com independência financeira, técnica e funcional. No entanto, a autoridade foi efetivamente criada nos termos do §1º do art. 55-A da LGPD, que assim dispõe:

---

[73] Disponível em https://eportugal.gov.pt/entidades/comissao-nacional-de-protecao-de-dados#:~:text=A%20CNPD%20%C3%A9%20a%20Autoridade,de%20pessoas%20residentes%20no%20estrangeiro. Último acesso em 13/12/2020

[74] Disponível em https://www.conjur.com.br/2020-out-31/portugal-modelo-brasil-vazamento-dados último acesso em 13/12/2020

[75] ibidem

[76] Disponível em https://www.jota.info/opiniao-e-analise/artigos/a-lgpd-na-gangorra-projeto-de-lei-n-1-179-2020-aprovado-no-congresso-nacional-05062020 último acesso em 13/12/2020

> A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.

Observe-se que não houve a efetiva autonomia desejada, pois há direta subordinação à Presidência da República, o que leva ao risco de ingerência política, o que será aprofundado adiante. No entanto, a natureza jurídica transitória, segundo Maffeis[77], pode ter sido justamente uma resposta a falta de independência, adiando a definição do tema.

Outra questão é que houve vetos à capacidade da autoridade obter recursos próprios, como aqueles oriundos de consultorias técnicas, bem como o de cobrar taxas[78]. Isto certamente compromete a independência financeira da autarquia, na medida em que retaliações à sua atuação em tese podem ocorrer mediante cortes orçamentários.

Na época, o deputado Orlando Silva comentou a dificuldade política de insistir na criação da autoridade com a natureza jurídica prevista no projeto de lei. Segundo ele, foi melhor criar desta forma do que a LGPD permanecer sem nenhuma autoridade que garantisse sua eficácia e efetividade[79].

6. ÓRGÃOS DA ANPD – COMPOSIÇÃO E PRIMEIRAS POLÊMICAS

São órgãos da ANPD, segundo o art. 55-C da LGPD, o Conselho Diretor, o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, as Ouvidorias, Corregedorias, órgão de assessoramento jurídico próprio e as unidades administrativas e unidades especializadas necessárias à aplicação.

As Ouvidorias e Corregedorias basicamente atuam como em qualquer outro órgão, sendo a primeira essencialmente responsável por ser o canal direto com o cidadão e as Corregedorias pela adequação dos atos do órgão às normas que o regulamenta. As unidades

---

[77] Disponível em https://migalhas.uol.com.br/quentes/307712/protecao-de-dados--advogados-avaliam-impactos-da-lei-que-criou-a-anpd último acesso em 07/12/2020.
[78] Disponível em https://www12.senado.leg.br/noticias/materias/2019/07/09/lei-que-cria-autoridade-nacional-de-protecao-de-dados-e-sancionada-com-vetos último acesso em 13/12/2020
[79] Íntegra do discurso disponível em https://www.youtube.com/watch?v=kfTzDD00Nns&feature=youtu.be&t=14040 último acesso em 09/12/2020

especializadas são os “braços e pernas” da ANPD, atuando de forma regionalizada a fim de garantir a sua efetividade.

Merecem maior destaque neste estudo o Conselho Diretor e o Conselho Nacional da Proteção dos Dados Pessoais, tanto pela sua importância na gestão da autoridade quanto pelas recentes polêmicas nas suas composições, o que despertou a atenção de diversos segmentos nacionais e internacionais.

O Conselho Diretor, cuja previsão encontra-se no art. 55-D da LGPD, já teve a sua primeira composição, o que foi objeto de polêmicas[80], por envolver a escolha de três militares, de um total de cinco, além da presidência ser exercida por um militar.

O Conselho Nacional da Proteção dos Dados Pessoais tem previsão nos arts. 58-A e 58-B da LGPD e é órgão bastante plural, composto por 23 membros de diversos segmentos de nossa sociedade, como da Câmara dos Deputados e do Senado, CNJ, Ministério Público, bem como de diversos segmentos da sociedade civil.

Tal Conselho tem importantes atribuições, como a elaboração de diretrizes e o fornecimento de subsídios para a Política Nacional de Proteção de Dados Pessoais, relatórios de impacto, estudos e debates, ações a serem realizadas pela ANPD e o fomento do conhecimento sobre a matéria.

No entanto, assim como o Conselho Diretor, o órgão não escapou de polêmicas[81]. O Decreto Legislativo 394/2020, de autoria do Deputado Alessandro Molon[82], tem por objetivo sustar pontos do Decreto 10.747/20, que criou a estrutura regimental e dos cargos que compõem a ANPD. Isto porque o Decreto 10.747/20 prevê que os representantes da sociedade civil para o CNPD serão escolhidos mediante lista tríplice elaborada pelo Conselho Diretor, sem qualquer critério objetivo.

Uma vez que o Conselho Diretor é composto por maioria de militares, surge a possibilidade teórica de que os representantes da sociedade civil a serem escolhidos tenham o

---

[80] referência

[81] Disponível em https://www.camara.leg.br/noticias/691086-projeto-susta-partes-do-decreto-que-criou-autoridade-nacional-de-protecao-de-dados/ último acesso em 12/12/2020

[82] Disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2262148 último acesso em 12/12/2020

mesmo viés ideológico da maioria do Conselho Diretor, prejudicando a pretensa pluralidade prevista na teleologia do art. 58-A da LGPD, que criou o CNPD.

Neste sentido pontuou o parlamentar:

> Esse duplo filtro do governo certamente acarretará um CNPD com visão semelhante à do conselho diretor e à do Executivo federal. Isso vai na contramão do que pretendeu a lei, que deu um caráter multissetorial ao conselho, com diversidade de visões e pluralidade de opiniões. O conselho consultivo só se justifica se efetivamente representar a sociedade.

Molon também criticou a escolha da presidência do CNPD, que, segundo o art. 15, I do Decreto 10.747/20, será exercida pelo representante da Casa Civil, que já tem o poder de indicar os membros do Conselho Diretor, como dispõe o art. 12 da norma em evidência. Portanto, a pretensa natureza jurídica de autarquia com independência funcional está longe de ser respeitada.

Por fim, mais uma vez indicando possível viés ideológico, a norma atacada, diz o Deputado, prevê a requisição de militares para a ANPD e dispõe que tais profissionais se subordinam ao Gabinete de Segurança Institucional da Presidência da República para fins disciplinares e de remuneração. Conclui que "na prática, esses militares não se submeterão à ANPD, o que compromete sua isenção e autonomia".

Também o meio empresarial tem apresentado preocupação com possível ingerência política no órgão. Em carta aberta[83], 80 segmentos empresariais reforçaram a importância da independência técnica da ANPD, que possui papel central na proteção dos dados pessoais.

A possível ingerência política também despertou a atenção da OCDE, que elaborou relatório[84] recomendando ao governo brasileiro que garanta a independência da ANPD[85]. Em um dos trechos do relatório, a OCDE recomendou "reavaliar e alterar as condições que estabelecem a Autoridade Nacional de Proteção de Dados (ANPD), no Artigo 55-A da Lei 13.709, para garantir que a Autoridade opere com total independência a partir da data de seu estabelecimento".

---

[83] Disponível em https://www.abracom.org.br/wp-content/uploads/2020/09/CARTA-FRENTE-LGPD-14.09-divulga%C3%A7%C3%A3o.pdf último acesso em 13/12/2020

[84] Disponível em https://www.oecd-ilibrary.org/sites/45a84b29-pt/index.html?itemId=/content/publication/45a84b29-pt último acesso em 13/12/2020.

[85] Disponível em https://g1.globo.com/politica/noticia/2020/10/26/ocde-pede-que-governo-brasileiro-garanta-independencia-de-orgao-de-protecao-de-dados.ghtml ´´ultimo acesso em 13/12/2020.

CONCLUSÃO

A ANPD possui um papel essencial na proteção de dados pessoais, de modo que é essencial que a autoridade tenha suficientes independências técnica e financeira. A experiência estrangeira adotando essa premissa tem se revelado bastante eficaz, o que certamente é um exemplo a ser seguido pelo governo brasileiro.

No entanto, o risco de ingerência política no órgão é iminente, por meio das políticas e escolhas que o Poder Executivo vem adotando, fato que não passou despercebido pelo Parlamento, a sociedade civil e por órgãos internacionais relevantes, como a OCDE.

A pretensa pluralidade, idealizada no projeto de lei da LGPD, não tem se verificado na prática, o que pode comprometer a eficácia da norma. A participação de diversos setores é de suma importância em um tema complexo, que pode ser enxergado tanto pela ótica do direito privado quanto pelo direito público, afetando direitos individuais e coletivos.

Destaque-se também que as seguidas tentativas legislativas de mitigação das sanções é outro fator que pode dificultar o papel protetivo da ANPD, algo que a experiência estrangeira, como de Portugal, revelou ser um diferencial para a proteção dos dados pessoais.

Uma vez que até o momento do fechamento deste artigo a ANPD não possui uma estrutura física, que a possibilite atuar, ainda não é possível analisar os impactos das medidas adotadas pela autoridade. Como a proteção de dados pessoais não deveria ser uma política de governo, mas de Estado, somente o tempo e a troca de governos de diferentes ideologias vão dizer o futuro da ANPD e da proteção dos dados pessoais.

TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO: ARTS 23-32.

Dafne Freitas Gomes

Maria Beatriz Alvim Barros

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados é, essencialmente, uma regulamentação geral das operações de tratamento de dados, que foi pautada em princípios éticos como a transparência, a não discriminação e a prestação de contas, e na consagração do direito dos titulares de dados à autodeterminação informativa. A LGPD foi redigida com o intuito de mitigar os riscos relacionados ao tratamento indevido e/ou abusivo de dados e, ao mesmo tempo, viabilizar que novos negócios e tecnologias sejam desenvolvidos em um ambiente de segurança jurídica. Insta salientar, que a LGPD surgiu com o propósito de harmonizar os interesses legítimos de titulares de dados e de empresas. O objetivo da lei não é frear o desenvolvimento tecnológico, mas tão somente compatibilizar direitos e expectativas, de forma a impulsionar a inovação e ensejar o tratamento legítimo dos dados pessoais.

Além disso, a referida lei é essencial para a harmonização de normas sobre proteção de dados já vigentes no Brasil, como por exemplo o Código de Defesa do Consumidor e a Lei de Acesso à informação (Lei n° 12.527). Tal harmonização pode ser vista se analisada a sentença trazida pelo Professor Plínio, contra a **CYRELA BRAZIL REALTY S/A EMPREENDIMENTOS E PARTICIPAÇÕES**, em que o magistrado faz uso tanto do CDC como da LGPD para fundamentar seu parecer, estabelecendo o diálogo das fontes como método de aplicação das leis.

2. DAS REGRAS

A LGPD recebe grande destaque sob a perspectiva da iniciativa privada. Todavia, deve-se considerar que sua aplicabilidade se estende a qualquer tipo de "tratamento de dados pessoais" e alcança também o Poder Público, que deve se adequar às obrigações ali impostas. Assim, dada a relevância do tema, o Capítulo IV da lei foi inteiramente dedicado ao tratamento de dados pessoais pelo Poder Público.

Vejamos, a seguir, os artigos concernentes ao Capítulo IV da LGPD:

O artigo 23 da LGPD aborda o tratamento dos dados pessoais pelo poder público, que pode ser realizado quando houver uma finalidade pública de interesse também público e somente quando houver real necessidade do tratamento para a execução dessas obrigações legais. Nessa perspectiva, a LGPD estabelece princípios, garantias, deveres e direitos dos cidadãos, dos prestadores de serviços e do próprio Poder Público, conforme o caput do artigo 23. Conforme transcrito, o referido artigo admite o tratamento de dados pelo Poder Público nas seguintes situações: a) para o atendimento de finalidade pública; b) na persecução do interesse público; c) com o objetivo de executar as competências legais; d) para cumprir atribuições legais do serviço público.

No tocante à finalidade, para Celso Antônio Bandeira de Mello, é basicamente “o objetivo que o ato administrativo deve alcançar, de acordo com o comando legal”. O Autor sustenta que a finalidade é um elemento do ato administrativo e que está vinculada a um interesse público. Quando a Administração Pública atua no campo da privacidade e dos dados pessoais, a operação de tratamento é, sem sombra de dúvida, um ato administrativo e como tal, detém como pressuposto de validade a sua finalidade.

Seguindo a análise, podemos observar que o artigo não aborda o compartilhamento de dados ou o tratamento de dados sensíveis, e isso abre espaço para que informações biométricas, por exemplo, venham a ser tratadas em nome da segurança pública. Essa tem sido uma polêmica bastante discutida devido a alegação de haver antinomias entre a LGPD e a identificação civil nacional.

Isso porque, na LGPD, veda-se o compartilhamento de dados sensíveis, com exceção de “... dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos." (artigo 11, II, "b"). O artigo 23 da lei, por sua vez, estabelece os parâmetros para o tratamento de dados pessoais pelo poder público: deve ser realizado para uma finalidade pública, norteada pelo interesse público, e com o objetivo de executar suas competências legais ou atribuições legais do serviço público.

Não há, portanto, uma autorização para o compartilhamento generalizado de dados pessoais, muito menos os sensíveis, como os biométricos. Ainda assim, é de notar que a vinculação ao "interesse público" e a finalidade de "execução de políticas e serviços públicos" dá margem a

uma interpretação extensiva que permitiria o compartilhamento dos dados em nome da "eficiência da administração pública" e da "segurança pública".

Ainda nesse sentido, precisamos trazer o Decreto 10.046, publicado pelo Governo Federal, em 2019, e que procura facilitar o compartilhamento de dados pessoais entre órgãos públicos, além de instituir o cadastro base do cidadão, um grande banco de dados federal que reunirá informações provenientes de diversas entidades. Farão parte desse cadastro o que o decreto chama de dados cadastrais, dados biográficos e dados biométricos. Embora o decreto informe explicitamente que respeitará o que está disposto na LGPD, há muitas dúvidas acerca dessa relação, principalmente porque até o momento de sua instituição a lei ainda não vigorava.

Há muitos pontos conflitantes quando se analisa o Decreto 10.046 frente à LGPD, a começar pela própria segmentação dos dados pessoais. Enquanto a LGPD fala em “dados pessoais” e “dados pessoais sensíveis”, o decreto classifica os dados dos cidadãos em “cadastrais”, “biográficos”, “biométricos” e “atributos genéticos”. Para a LGPD, dados relacionados à origem étnica, opinião política, genética e biometria de uma pessoa, por exemplo, são dados sensíveis e requerem um tratamento especial por parte de empresas e órgãos públicos. O decreto, por sua vez, estabelece três categorias de compartilhamento para os dados na esfera pública (amplo, restrito e especifico), cabendo ao gestor dos dados a classificação. Note-se, portanto, que o decreto e a LGPD tem diversos contrapontos.

Outra controvérsia, é que o decreto determina a criação de um Comitê Central de Governança de Dados (CCGD), para gerir as regras e a operação do cadastro base do cidadão. Ele será constituído apenas por representantes indicados pelo poder executivo. O problema é que a LGPD estabelece a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão federal que vai regular e fiscalizar o cumprimento da lei. A ANPD terá um conselho diretor com cinco membros, todos indicados pelo presidente da República, mas que, uma vez escolhidos, não podem ser demitidos pelo poder executivo. Para alguns especialistas, haveria sobreposição de atribuições entre ANPD e CCGD, o que poderia provocar impasses que somente seriam resolvidos mediante judicialização.

Por fim, o artigo 23, traz que para operações da esfera pública que envolvam tratamentos de dados pessoais, deve ser apontado um encarregado para zelar pelo bom uso e

segurança das informações. Após formada, a ANPD pode determinar como devem ser anunciadas as medidas de segurança e as formas de tratamento.

No Artigo 24, conforme disposto, as pessoas jurídicas de direito privado são as associações, sociedades, fundações, organizações religiosas, partidos políticos e empresas individuais de responsabilidade limitada, instituídas por iniciativa de particulares.

Já as empresas públicas são os entes de administração direta União, Estados, Distrito Federal, Territórios e Municípios, as autarquias, as fundações públicas e as demais entidades de caráter público. Por último, as sociedades de economia mista são formadas tanto por capital público quanto privado, sendo que a parcela de capital público deve ser maior.

Para os fins da LGPD, as sociedades de economia mista e as empresas públicas estão sujeitas às mesmas diretrizes e regras das empresas de direito privado particular quando operarem em regime de concorrência, ou seja, para fins comerciais e/ou mercadológicos. Enquanto isso, se estiverem aplicando políticas públicas dentro de seus respectivos âmbitos de execução, serão consideradas da mesma forma que os demais órgãos do poder público.

Por isso, verificada a necessidade de tratar dados pessoais, primeiramente deve o ente público identificar sob qual condição atua, uma vez que as consequências de atuar em regime concorrencial ou regime de finalidade pública são diferentes, desde os requisitos a serem atendidos até às sanções previstas em eventual desalinho com a lei. Entendemos que é nesse ponto que reside uma das grandes complexidades no tratamento dispensado aos entes públicos pela LGPD, uma vez que pode acontecer de o mesmo dado ao ser utilizado para finalidades diversas requerer o atendimento de requisitos diversos.

Importante destacar a equiparação realizada pelo artigo 23, §4º, que atribui aos serviços notariais e de registro exercidos por delegação o mesmo tratamento dispensado aos entes públicos quando necessitarem realizar o tratamento de dados pessoais.

Já os artigos 25, 26 e 27 da LGPD encarregam-se de descrever como e quando pode/deve ocorrer o compartilhamento dos dados pessoais geridos pelo setor público. No artigo 25, preservando a eventual necessidade de execução de políticas e serviços públicos, e também pela descentralização da atividade pública e pelo livre acesso à informação por parte dos cidadãos,

a LGPD orienta que os dados pessoais tratados nessas esferas devem ser mantidos de forma a permitir o uso compartilhado.

Já o artigo 26, complementando diretamente o artigo 25, é claro quanto à vedação ao compartilhamento dos dados em posse da Administração Pública com entidades privadas, com exceção em casos que a transferência se faça necessária com o fim específico e determinado de execução descentralizada da atividade pública.

O artigo 27, por sua vez, determina que, via de regra, deve haver consentimento do proprietário dos dados para que eles sejam compartilhados entre a Administração Pública e algum ente privado, exceto quando necessários para execução da atividade pública e nas exceções previstas no artigo 26.

O artigo 28 da LGPD versava sobre a publicidade da comunicação ou o uso compartilhado de dados pessoais entre órgãos e entidades de direito público porém foi vetado pois poderia dificultar algumas ações públicas de fiscalização e controle da utilização desses dados, uma vez que seria obrigatória a publicidade.

Já o artigo 29 dispõe sobre a autoridade nacional de Proteção pode solicitar informações sobre os dados às entidades do poder público. Ele tem poder para solicitar informações específicas sobre os dados e também pode exigir a realização do tratamento. Todos esses poderes são com o objetivo de garantir que a LGPD esteja sendo cumprida.

O artigo 30 trata da possibilidade de a autoridade poder adicionar novas diretrizes sobre o compartilhamento desses dados e também sobre a forma de como esse tratamento vai ser comunicado, uma vez que com o veto do artigo 28 a publicidade não é mais obrigatória.

3. DA RESPONSABILIDADE

Nos artigos 31 e 32 da Lei Geral de Proteção de Dados vão ser tratados aspectos acerca da responsabilidade do ente sobre os dados que estão sob sua guarda.

O artigo 31 dispõe acerca da autoridade nacional poder enviar medidas cabíveis para impedir ou para qualquer violação à LGPD quando o tratamento desses dados estiverem sendo feitos pelos órgãos públicos.

Já o artigo 32 trata da possibilidade da solicitação de relatórios de impacto à proteção de dados e até sugerir a adoção de padrões e práticas para o tratamento de dados pelo poder público

CONCLUSÃO

Depois da análise dos seguintes artigos, podemos inferir que a autoridade nacional é grande responsável para garantir que as normas da LGDP sejam devidamente aplicadas e por conferir como o tratamento de dados pelos órgãos públicos está sendo feito.

O tratamento dos dados pessoais pelo poder público é uma questão de suma importância uma vez que os bancos de dados desses órgãos públicos são responsáveis por armazenar dados de milhões de pessoas por todo o Brasil, sendo estes de diversas naturezas. Ainda que, uma vez que são órgãos públicos, os cidadãos possuem maior confiança em que seus dados estão seguros e bem tratados.

OS AGENTES DE TRATAMENTO NA LGPD

Gabriel Moreira Nascimento

Milena De Azevedo Almeida

A Lei Geral de Proteção de Dados Pessoais surge exatamente no momento em que o mundo passa a sofrer os efeitos, tanto benéficos quanto maléficos, da grande Revolução Digital. É em razão dessa nova face da globalização que se fez um esforço, por parte dos representantes da sociedade brasileira, de regular o mundo digital, para que os direitos dos cidadãos que constam sob a égide do Direito brasileiro não sejam vilipendiados pelas mudanças dos tempos. A presente obra busca, através da análise bibliográfica de diferentes autores e obras, sintetizar os principais conhecimentos acerca de algumas figuras importantíssimas dentro da lógica da LGPD, os denominados agentes de tratamento, que são responsáveis pelo trato dos dados pessoais, e também constam como os principais responsáveis em caso de danos causados aos direitos dos titulares desses dados. Tem-se que a LGPD veio em boa hora, mas deve se apressar: muitos de seus institutos ainda estão em crescimento, e boa parte das compreensões acerca deste valioso tema ainda estão em desenvolvimento. Essa obra, pois, surge como mais uma das tentativas de compreender o esforço, feito pelo Direito, de enfrentar a nova realidade social da Era Digital através da LGPD.

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados, doravante referida por sua sigla LGPD, foi a tentativa dos representantes da sociedade brasileira de regular uma parte daquilo que tem se tornado o lócus primário de interação social em nossos tempos: o mundo digital. Tal regulamentação faz-se necessária pela realidade em que se vive – pois que, embora a globalização não seja por todos acessível da mesma maneira, sendo para uns uma maneira de ingressar no cenário global e dele desfrutar de todas as benesses, enquanto para outros a globalização significou a exclusão e a perda de pertencimento devido ao enfraquecimento dos valores tradicionais das sociedades nacionais[86] – o fato claro é que a globalização, em seus efeitos, fez-se sentir por todos, e sem a menor sombra de dúvidas a maior influência por trás desta nova realidade foi a força avassaladora da grande rede, a internet. Como dirá brilhantemente Karen Kohn, na globalização e na digitalização "há de tudo, para quem pode"[87].

[86] BAUMAN, Zygmunt. **Globalização**: as consequências humanas. Rio de Janeiro: Zahar, 1999. Tradução de: Marcus Penchel.

[87] KOHN, Karen; MORAES, Cláudia Herte de. **O impacto das novas tecnologias na sociedade: conceitos e características da sociedade da informação e da sociedade digital**. In: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 2007, Santos. Anais [...]. Santos: Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, 2007. p. 1-13, p. 10.

Ainda que se trate o tema deste trabalho dos agentes de tratamento, cabem aqui explicações mais genéricas e gerais sobre a Lei em si, alguns de seus princípios e seus norteadores, pois que, por óbvio, o tratamento devido deverá seguir tais parâmetros, sendo impossível, pois, esgotar o tema sem tratar daqueles que são alguns dos principais pilares da LGPD.

O primeiro e grandemente importante princípio a ser tratado é o da dignidade humana, o qual, tendo em vista sua ampla gama de aplicabilidade, deverá ser exercido durante a totalidade dos procedimentos de tratamento e durante toda a vigência do contrato não apenas do controlador, figura essa que será apresentada muito em breve, com os clientes dos serviços prestados, aqui denominados titulares dos dados pessoais, mas entre o próprio controlador e seus subordinados, nomeadamente o operador e o encarregado. Do princípio da dignidade humana defluem outros tantos princípios e direitos importantíssimos para a relação que ora analisa-se, como o direito à privacidade, o direito à informação, por parte do titular dos dados, e certas regras limitadoras do livre arbítrio e da discricionariedade dos agentes de tratamento.

Existem outros princípios que regem e direcionam a LGPD, porém o exaurimento destes princípios foge ao escopo deste trabalho, de maneira que se teve por suficiente a apresentação de alguns dos mais importantes. Cabe ainda mencionar mais um princípio: o princípio da não-discriminação, o qual define que não devem ter seu acesso a serviços ou bens negados quaisquer indivíduos em razão de suas opções de vida ou condições e/ou situações que os ponham dentro de um grupo social específico no seio da comunidade de pessoas. Um exemplo que ressalta a importância do princípio da não-discriminação é trazido por Tom Slee, em sua obra *Uberização*, na qual o autor apresenta o fato de que pessoas negras têm uma chance maior de terem negadas suas corridas pelos motoristas do aplicativo Uber, ao mesmo tempo que os motoristas negros têm uma menor chance de encontrar passageiros caso possuam fotos suas em seu perfil do aplicativo[88]. Na mesma obra, Tom Slee traz uma pesquisa, feita pela *National Bureau for Economic Research*, na qual foi descoberto que

> Os resultados indicam um padrão de discriminação, que em Seattle se deu pelo maior tempo de espera para passageiros negros – 35% mais. Em Boston, observamos a discriminação por cancelamentos mais frequentes das viagens de passageiros com nomes afro-americanos. Na soma das viagens, a taxa de cancelamento para nomes afro-americanos foi mais que o dobro, se comparada a nomes que soam como de brancos. Passageiros homens pedindo uma viagem em

[88] SLEE, Tom. **Uberização**: a nova onda do trabalho precarizado. São Paulo: Elefante, 2017. Tradução de: João Peres, p. 136-139.

> áreas pobres tiveram chances três vezes maior de cancelamento quando usaram um nome afro-americano.[89]

Quanto às limitações ao arbítrio e à discricionariedade dos agentes de tratamento, aqui se faz referência, primordialmente, à noção de finalidade, que é inerente à totalidade do tratamento dos dados pessoais, e especialmente àqueles dados pessoais que são considerados sensíveis[90], pois que esses, por serem personalíssimos[91] e conterem demasiadas características intrinsecamente pessoais, poderão afetar gravemente o titular dos dados na medida em que esse possa vir a ser discriminado em razão de tais informações.

Torna-se premente a percepção das similaridades não apenas da LGPD com ordenamentos que regulam matéria similar, tanto no âmbito da Justiça brasileira quanto no âmbito de justiças especializadas no exterior, como é o caso da *General Data Protection Regulation*, mas também dessas similaridades entre a LGPD e outras partes do ordenamento jurídico brasileiro, como ocorre com o Código do Consumidor e até mesmo da Justiça do Trabalho, os quais percebem que, dentro da lógica das relações por esses ramos da Justiça tratadas, existe uma relação desigual, como ocorre, no caso do CDC, na relação entre o consumidor, parte vulnerável, e fornecedor, comumente uma empresa de vulto, bem como também é assegurado, por parte do CDC aos consumidores, o direito à informação, razão pela qual alguns autores compreendem que há um estreito vínculo entre a LGPD e o CDC[92]. O mesmo ocorre na Justiça do Trabalho, por pressão da relação desigual entre empregado e empregador, que gera a razão de ser desse ramo especializado da Justiça. Ora, não se diferem dessas situações a situação que se põe a regular a LGPD, pois que a relação entre o titular dos dados pessoais e aquela pessoa, seja ela física ou jurídica, que os detêm é, geralmente, uma relação desigual. Põe-se em xeque, dessa maneira, a privacidade do indivíduo

---

[89] GE, Yanbo *et al*. "**Racial and Gender Discrimination in Transportation Network Companies**" [Discriminação racial e de gênero em companhias de redes de transporte], em *National Bureau of Economic Research*, out. 2016. Disponível em <https://www.nber.org/papers/w22776>, acesso em 11 de dezembro de 2020.

[90] São considerados sensíveis os dados que possam, dizendo de maneira bastante simples e genérica, singularizar o indivíduo como membro de um determinado grupo social específico dentro da sociedade, sendo esses dados sensíveis aqueles que indiquem a "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural", nos termos do art. 5º da LGPD, em seu inciso II.

[91] MULHOLLAND, C. S. **Dados pessoais sensíveis e a tutela de direitos fundamentais**: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, v. 19, n. 3, p. 159-180, 29 dez. 2018..

[92] CANTO, Ana Paula *et al*. **O tratamento de dados pessoais na LGPD: transparência e dever de informação**. In: SALDANHA, Paloma Mendes (org.). O que estão fazendo com meus dados? / a importância da lei geral de proteção de dados. Recife: Serifafina, 2019. Cap. 3. p. 31-42, p. 33. Disponível em: https://www.udop.com.br/noticia/2020/03/03/o-que-estao-fazendo-com-os-meus-dadosy-a-importancia-da-lei-geral-de-protecao-de-dados.html. Acesso em: 11 dez. 2020.

na medida em que não sejam dados os devidos cuidados ao tratamento dos dados pessoais por parte dos agentes de tratamento.

Dessa maneira, a LGPD surge como essa necessidade social de regulamentação dos poderes, deveres e mesmo direitos das duas partes que compõem a relação de fornecimento de dados pessoais, quais sejam: os agentes de tratamento e o titular dos dados. Por ser uma relação desigual, dirá Caitlin Mulholland que:

> o problema da privacidade hoje é causado pelo conflito consequente da assimetria de poderes existente entre os titulares de dados e aqueles que realizam o tratamento dos dados. Esta assimetria gera um desequilíbrio social que, por sua vez, leva à violação dos princípios da igualdade e da liberdade. Proteger de maneira rigorosa os dados pessoais sensíveis se torna, assim, instrumento para a efetivação da igualdade e da liberdade[93].

As violações a esses princípios que norteiam não apenas a LGPD, mas todo o ordenamento jurídico brasileiro, e aos direitos dos titulares dos dados poderão trazer graves problemas a esses últimos. Em verdade, por vivermos em uma sociedade democrática, talvez falhemos em perceber todas as mazelas que poderiam advir da má utilização dos dados pessoais, em especial por parte do Estado, razão pela qual há um capítulo específico sobre o tratamento dos dados pessoais por parte do Estado na LGPD[94]. Mulholland traz alguns exemplos emblemáticos, como o caso da China e de seu sistema de crédito social, surgem como uma das formas através das quais poderia o Estado intervir na esfera de privacidade do indivíduo e, ao fazê-lo e por fazê-lo, limitar direitos outros, como o acesso a serviços e políticas públicas, ferindo, dessa maneira, o princípio de não-discriminação[95].

Finda a contextualização e a análise de alguns princípios importantes para o devido progredir no tema, far-se-á necessário, nesse momento, passar para o exame do objeto de estudo próprio deste trabalho: os agentes de tratamento.

---

[93] MULHOLLAND, C. S. **Dados pessoais sensíveis e a tutela de direitos fundamentais**: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, v. 19, n. 3, p. 159-180, 29 dez. 2018.
[94] Ver Capítulo IV, da Lei Geral de Proteção de Dados, que regula o tratamento de dados pessoais pelo Poder Público.
[95] Ibid, p. 161.

2. OS AGENTES DE TRATAMENTO

Em linhas gerais, os agentes de tratamento são as pessoas físicas ou jurídicas responsáveis pelo tratamento dos dados pessoais, sendo dois os agentes de tratamento que atuam diretamente no tratamento de dados, a saber: o controlador e o operador. O encarregado, outro agente de tratamento, o qual será melhor explicado em momento posterior, trata mais da relação entre os titulares, o controlador e a Autoridade Nacional de Proteção de Dados (ANPD)[96], que dos dados pessoais em si. A análise dessas figuras é de suma importância não apenas para o entendimento pleno do funcionamento da LGPD e do tratamento de dados, mas para a responsabilização de indivíduos ou pessoas jurídicas, no caso de ocorrerem problemas que danifiquem ou ameacem direitos.

3. O CONTROLADOR

O Controlador é a pessoa física ou jurídica que irá determinar a maneira pela qual serão tratados os dados pessoais. Em termos genéricos, é a pessoa que tomará as principais decisões acerca do tratamento de dados, sendo, por essa razão, o principal responsável em caso de ocorrer algum injusto, cabendo a ele responder, salvo nos casos de ser incluído o operador solidariamente, pelos danos causados aos titulares em razão da violação da segurança dos dados[97] seja esse dano de ordem patrimonial, moral, individual ou coletivo, quando ocorrido em decorrência de violação à LGPD, sendo o controlador obrigado a repará-los[98]. A figura do controlador é apresentada no inciso VI do artigo 5º da LGPD[99] como “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”[100]. Suas atribuições são várias, mas é notável que a maior parte delas se refere a obrigações de mando, sendo a execução de suas ordens atribuição mais típica do operador, figura que será posteriormente examinada.

---

[96] MATTOS, Bruna *et al*. **Dos agentes de tratamento dos dados pessoais**. In: SALDANHA, Paloma Mendes (org.). O que estão fazendo com meus dados? / a importância da lei geral de proteção de dados. Recife: Serifafina, 2019. Cap. 8. p. 77-85, p. 77. Disponível em: https://www.udop.com.br/noticia/2020/03/03/o-que-estao-fazendo-com-os-meus-dadosy-a-importancia-da-lei-geral-de-protecao-de-dados.html. Acesso em: 11 dez. 2020.
[97] Ver parágrafo único do art. 44 da LGPD.
[98] Ver art. 42 da LGPD.
[99] Vale mencionar que o artigo 5º funciona, dentro da LGPD, como um grande repositório de definições dos conceitos e ferramentas que são frequentemente trazidos no texto dessa lei.
[100] Ver art. 5º, VI da LGPD.

O controlador, de maneira geral, é a empresa que presta algum serviço ou vende determinados produtos e, ao fazê-lo, armazena, processa, elimina ou realiza outros tratamentos com os dados pessoais do titular. Cabem alguns exemplos, os quais poderão tornar a elucidação desse agente de tratamento mais simples. Uma grande empresa de e-commerce, como a Amazon, seria tomada como um controlador dentro da LGPD, por ser essa empresa responsável pelas ações de natureza decisória que se referem ao tratamento de dados de seus consumidores, sendo a execução dessas decisões função típica do operador, que, nesse caso, geralmente é uma empresa de TI.

Mas não é necessário, no ordenamento brasileiro, ser uma empresa de grande vulto – ou sequer uma empresa – para ser considerado como controlador: um advogado que trabalha autonomamente, por exemplo, poderá também ser considerado um controlador, pois a ele cabem as decisões sobre o tratamento de dados pessoais. Ainda nesse mesmo exemplo, percebe-se que, caso não possua o advogado alguma pessoa empregada que exerça a função de operador, poderá o advogado ele próprio ser considerado, para efeitos de aplicação da LGPD, tanto como controlador quanto como operador, não havendo qualquer limitação, em nosso ordenamento, em relação a essa situação.

Dentre as responsabilidades daquele que é o mais importante agente de tratamento de dados pessoais no âmbito da LGPD constam algumas que são mais relevantes que outras, devendo ser aqui mencionadas[101]. São elas: a observância dos princípios gerais e da garantia dos direitos do titular (Artigo 7º, §6º); a obtenção do consentimento, quando esse for necessário (Artigo 7°, §5°; Artigo 8°, §6°); o informe e a prestação de contas; a garantia da portabilidade (Artigo 9°; Artigo 18; Artigo 20); a garantia da transparência no tratamento de dados baseado em legítimo interesse (Artigo 10, §2°); a manutenção do registro das operações de tratamento de dados pessoais, especialmente quando baseada no legitimo interesse (Artigo 37); a elaboração do relatório de impacto à proteção de dados pessoais (Artigo 10; §3°; Artigo 38); a indicação do encarregado pelo tratamento de dados (Artigo 41); o reparo de danos patrimoniais, morais, individuais ou coletivos causados por violação à legislação de proteção de dados pessoais (Artigo 42 e 44, Parágrafo único); a adoção de medidas de segurança, técnicas e administrativas (artigo 46); a garantia da segurança da informação em relação aos dados pessoais, mesmo após seu término (Artigo 47); manter comunicação com a autoridade nacional e com o titular em caso de ocorrência de incidente de

[101] MATTOS, Bruna et al. **Dos agentes de tratamento dos dados pessoais**. In: SALDANHA, Paloma Mendes (org.). O que estão fazendo com meus dados? / a importância da lei geral de proteção de dados. Recife: Serifafina, 2019. Cap. 8. p. 77-85, p. 79. Disponível em: https://www.udop.com.br/noticia/2020/03/03/o-que-estao-fazendo-com-os-meus-dadosy-a-importancia-da-lei-geral-de-protecao-de-dados.html. Acesso em: 11 dez. 2020.

segurança que possa ameaçar ou causar danos a direitos dos titulares (Artigo 48); agir de forma a mitigar possíveis danos (Artigo 48, §2°); formular regras e práticas inerentes à boa governança (Artigo 50).[102]

Ver-se-á que o controlador não é uma figura tão fixa quanto possa parecer em um primeiro momento, de maneira que a simples divisão de funções dentro de uma empresa não sedimenta ser uma pessoa o controlador e outra o operador ou o encarregado. Dessa forma, é apenas mediante a observação do caso concreto que será possível delimitar quem é o controlador e quem é um mero operador. Retornar-se-á a esse ponto em momento posterior, quando do exame do operador do tratamento dos dados pessoais, para que fique mais coesa a explicação[103].

Há ainda a possibilidade de haver co-controladores, isto é, a existência de mais de um único controlador. Tal ocasião deverá ser verificada não apenas na relação contratual estabelecida entre as pessoas físicas ou jurídicas, mas também da situação fática observável no caso concreto. Em caso de estarem tais controladores diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados, deverão os controladores responder solidariamente, por força do inciso II do artigo 42 da LGPD.

Por fim, para fins de ser também realizada uma análise através do direito comparado, a legislação brasileira diverge da europeia por possibilitar que o controlador seja pessoa natural[104], ao passo que a GDPR só possibilita que a função de controlador seja feita por pessoa jurídica[105].

Antes de passar para o exame da próxima figura dos agentes de tratamento, o operador, cabe fazer uma análise de uma importantíssima ferramenta da LGPD: o relatório de impacto à proteção dos dados pessoais.

4. O RELATÓRIO DE IMPACTO À PROTEÇÃO DOS DADOS PESSOAIS

Em um primeiro momento, cabe informar que o relatório de impacto é importante por se tratar de uma ferramenta que visa não a remediar eventuais danos causados aos dados pessoais dos titulares, mas sim prevenir que esses danos possam vir a ocorrer. A lógica, portanto, é de prevenção, não de indenização. Não se trata o relatório de impacto de um documento que visa

[102] Todas as menções a artigos nas responsabilidades deste parágrafo referem-se aos artigos da LGPD.
[103] KREMER, Bianca. **Os agentes de tratamento de dados pessoais**. In: MULHOLLAND, Caitlin (org.). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipelago, 2020. p. 289-318, p. 293
[104] Ver artigo 5º, VI, da LGPD.
[105] Ver artigo 4º, VII, da GDPR.

informar à ANPD os danos ocorridos e as medidas que serão tomadas para que sejam indenizados os que foram danificados, mas indicar a essa importante autoridade nacional as formas através das quais é realizado o tratamento de dados pessoais e quais medidas estão sendo efetivamente tomadas para prevenir qualquer possibilidade de dano. Ademais, o relatório de impacto é uma ferramenta adaptável, e não estritamente burocrática: deve ser flexível para que possa ser modelado de acordo com as necessidades e especificidades de cada caso concreto e possa informar, da melhor maneira possível, a ANPD sobre os riscos inerentes ao tratamento de dados pessoais, com especial ênfase dada àqueles dados sensíveis, por parte dos que gerenciam esses dados.[106]

Também é importante notar o quanto o relatório de impacto relaciona-se com outros artigos dentro da própria LGPD, como é o caso que ocorre entre o RIPD e o artigo 37 da LGPD, que determina que devem o controlador e o operador manter registro das operações de tratamento de dados[107]. Ora, não faria sentido manter esses registros caso não houvesse a possibilidade, por parte de alguma autoridade competente – nesse caso a ANPD – de verifica-los, de maneira que o relatório de impacto serve como ferramenta para que se efetive esse artigo em algo prático.

O interessante, aqui, é que a própria forma do relatório e impacto é maleável devido a ser a LGPD bastante nova e a ANPD ainda mais recente, estando essa autoridade ainda em processo de formação e tendo a lei entrado em vigor apenas em agosto de 2020[108]. Dessa maneira, é possível dizer que as formas ainda estão sendo construídas, e que se aprende ao caminhar pelos caminhos da aplicação da LGPD. Não obstante essa situação, o relatório de impacto deve possuir, em seu conteúdo, algumas informações mínimas, as quais estão estabelecidas no parágrafo único do artigo 38 da LGPD, quais sejam:

> a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.[109]

Como foi dito anteriormente, o relatório de impacto à proteção dos dados pessoais é uma atribuição do controlador, de maneira que a comunicação sobre esse ponto deve ser realizada entre esse e a ANPD, o que não impede, entretanto, que essa atribuição seja realizada pelo operador

---

[106] GOMES, Maria Cecília Oliveira. **Relatório de impacto à proteção de dados**: uma breve análise da sua definição e papel na LGPD. Revista do advogado, nº 144, p. 174-183, nov. 2019.
[107] Ver artigo 37 da LGPD.
[108] Informações extraídas do site do Senado. Disponível em https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor#:~:text=A%20entrada%20em%20vigor%20da,no%20artigo%204%C2%BA%20do%20PLV Acesso em 11 de dezembro de 2020.
[109] Ver parágrafo único do artigo 38 da LGPD.

ou sequer pelo encarregado, o que se torna perceptível através de uma interpretação sistemática da lei[110]. Não deve, entretanto, restringir-se a simples questões de *accountability* daquele perante a ANPD, ou somente de uma mera adequação das práticas de tratamentos de dados pessoais por parte do controlador às normas da LGPD, mas sim indicar todo um padrão de medidas que serão feitas no sentido de mitigar a possibilidade de danos, diminuir o risco, criar, dessa forma, uma melhor e mais responsável forma de exercer a governança da própria empresa no tratamento dos dados pessoais. O relatório de impacto deve demonstrar, para além das adequações formais à LGPD, a vontade das empresas de praticarem suas atribuições nesse âmbito com a mais estrita boa-fé, outro princípio de imensurável importância.

Maria Cecília Gomes irá indicar três partes principais que compõem, quando postas em conjunto, o relatório de impacto. Para a autora, tais partes são:

> (i) documentação do controlador; (ii) descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais; e (iii) medidas, salvaguardas e mecanismos de mitigação desses riscos.[111]

Também deve o relatório de impacto ser compreendido como uma ferramenta de uso contínuo, o que se torna claro quando se pensa no caso do lançamento de um novo produto por parte de uma empresa, momento no qual deverá essa empresa, caso queira agir estritamente de acordo com as normas de boa governança, elaborar um relatório de impacto para que sejam avaliados e apresentados os riscos e as medidas que estão sendo tomadas para enfrenta-los[112].

Essa importantíssima ferramenta serve, pois, como uma forma através da qual as empresas garantem à autoridade nacional que suas práticas de tratamento de dados pessoais adequam-se às regras da LGPD, bem como estabelece, para além dessa parte mais burocrática, indicações de que a empresa está agindo conforme preceitos importantes da relação entre ela e seus consumidores, os titulares de dados, e fazendo todo o possível para que esses últimos tenham assegurados seus direitos, pois que terão sido realizadas todas as medidas necessárias à diminuição do risco inerente à atividade de tratamento de dados pessoais através de uma avaliação desses mesmos riscos.

---

[110] GOMES, Maria Cecília Oliveira. **Relatório de impacto à proteção de dados**: uma breve análise da sua definição e papel na LGPD. Revista do advogado, nº 144, p. 174-183, nov. 2019, p. 177-178.
[111] Ibid, p. 177.
[112] GOMES, Maria Cecília Oliveira. **Relatório de impacto à proteção de dados**: uma breve análise da sua definição e papel na LGPD. Revista do advogado, nº 144, p. 174-183, nov. 2019, p. 177-178, p. 179.

5. O OPERADOR

Tendo sido feita a análise sobre o controlador, o exame da figura do operador e de suas atribuições na LGPD resta bastante simplificada, pois o operador é, tão simplesmente, a pessoa, física ou jurídica, de direito público ou privado, responsável por executar as ordens do controlador. Dessa maneira, tem-se que o operador não é livre para alterar a finalidade do uso dos dados pessoais, ou para fugir das diretrizes do controlador. Não obstante essas limitações, é notável que o operador possui certo grau de liberdade no exercício de sua função, pois a absoluta adequação às diretrizes do controlador não só não é possível, como não é útil ao processo e à funcionalidade do tratamento dos dados pessoais[113]. Assim sendo, deverá o operador adequar o exercício de suas funções conforme forem se apresentando questões e ele relacionadas. O que diferencia o controlador do operador, portanto, não é uma mera capacidade decisória daquele e uma total incapacidade desse, mas o grau no qual se é exercida essa capacidade: ele será muito maior, mais significativo e terá impactos muito mais relevantes no caso do controlador.

E é nesse momento que é necessário terminar um comentário que fora iniciado no momento da análise da figura do controlador: o de que a figura do operador, bem como a do controlador, não é tão estável quanto possa parecer. Não obstante ter uma empresa definido em um contrato com outra empresa que seria a primeira a controladora do tratamento de dados pessoais e a segunda a operadora, caso a segunda possua um grau de gerência por demasia elevado, poderá ela ser considerada, também, como controladora, e não como uma mera operadora[114]. Essa concepção é de fundamental importância para a definição das responsabilidades e de quem irá arcar com eventuais prejuízos, sendo importante notificar, desde já, que respondem solidariamente o controlador e o operador por danos causados durante o tratamento de dados pessoais caso tenha sido esse dano decorrente do não cumprimento, por parte do operador, das obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador[115], ressalvados os casos que excluem a responsabilidade dos agentes de tratamento[116].

---

[113] MATTOS, Bruna et al. **Dos agentes de tratamento dos dados pessoais**. In: SALDANHA, Paloma Mendes (org.). O que estão fazendo com meus dados? / a importância da lei geral de proteção de dados. Recife: Serifafina, 2019. Cap. 8. p. 77-85, p. 78. Disponível em: https://www.udop.com.br/noticia/2020/03/03/o-que-estao-fazendo-com-os-meus-dadosy-a-importancia-da-lei-geral-de-protecao-de-dados.html. Acesso em: 11 dez. 2020.

[114] KREMER, Bianca. **Os agentes de tratamento de dados pessoais**. In: MULHOLLAND, Caitlin (org.). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipelago, 2020. p. 289-318, p. 293.

[115] Ver art. 42, I, da LGPD.

[116] Ver art. 43 e incisos, da LGPD.

Diferentemente da situação que ocorre com o controlador, há uma equivalência entre o conceito do operador, na legislação brasileira[117], e de sua figura análoga na GDPR, o subcontratante, que é tido como o processador de dados pessoais[118].

6. O ENCARREGADO

Em linhas gerais, o encarregado é a figura responsável por auxiliar o controlador no cumprimento das obrigações legais de proteção de dados, por meio de monitoramento e aconselhamento.

Partindo da novíssima Lei Geral de Proteção de Dados, temos o conceito de encarregado disposto no art. 5, VII, *in verbis*:

> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)

Dessa forma, fica claro que o encarregado possui, primordialmente uma tarefa de conectar os demais sujeitos interessados no tratamento de dados a empresa. Podendo esses sujeitos serem o próprio órgão regulador (ANPD), a partir da comunicação de novas diretrizes, ou mesmo os próprios titulares dos dados através de um canal de recebimento das reclamações relacionadas ao tratamento de dados.

Adicionalmente, o artigo também estabelece a necessidade do encarregado ser indicado diretamente pelo controlador ou mesmo pelo operador.

Importante ressaltar que tal inciso sofreu modificação prévia para constar a redação atual. Nesse sentido, anterior a vigência da Medida Provisória nº 869, que posteriormente foi ratificada na Lei 13.853 de 2019, o encarregado somente poderia ser pessoa natural. Isto é, pessoa capaz de contrair direitos e deveres na ordem civil.

> VIII - encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;

---

[117] Ver art 5º, VII da LGPD.
[118] Ver art 4º, VIII, da GDPR.

Tal redação prejudicava, principalmente, as empresas de médio a grande porte, as quais tendem a contratar uma prestadora de serviço para exercer a tarefa de controle dos dados com a maior segurança possível. Ademais, agrega maior imparcialidade durante o tratamento dos dados, bem como maior competitividade da empresa no mercado

Tendo a necessidade de adequar à lei as demandas da sociedade, o legislador optou pela alteração da norma possibilitando que também pessoas jurídicas pudessem atuar no papel de encarregado.

Adentrando o Capítulo VI, Seção II que trata em específico "Do Encarregado pelo Tratamento de Dados Pessoais" tem-se o art. 41 que dispõe que "o controlador deverá indicar encarregado pelo tratamento de dados pessoais".

Dessa forma, em consonância com o próprio art. 5, VII, temos que a figura do controlador como quem deverá indicar o encarregado para exercer as funções. Como se pode perceber o art. 41 não menciona a indicação feita pelo operador, o que torna incerto em quais hipóteses essa indicação ocorrerá.

Primordialmente, o texto inicial da Lei 13.853 apontava que as hipóteses nas quais o operador deveria indicar o encarregado seriam objeto de regulamentação pela Autoridade Nacional de Proteção de Dados (ANPD). Contudo, o presidente da República vetou esse trecho da lei, permanecendo vago quais situações tal indicação é possível.

Seguindo para os parágrafos do art. 41, tem-se, em seu §1º, que:

> A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

Tal paragrafo explica-se na medida em que se entende que o papel do controlador é construir "pontes" entre os titulares dos dados e a empresa contratada para trata-los[119]. Assim, para que a comunicação de possíveis erro no tratamento dos dados é importante o acesso direto ao encarregado, para que o mesmo possa sanar eventuais problemas.

O §2 do art. 41 trata do papel do encarregado. Vale ressaltar que não se trata de rol taxativo, apenas exemplificativo da atuação desse agente. Como primeira atividade temos que o encarregado deve "aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e

[119] MATTOS, Bruna et al. **Dos agentes de tratamento dos dados pessoais**. In: SALDANHA, Paloma Mendes (org.). O que estão fazendo com meus dados? / a importância da lei geral de proteção de dados. Recife: Serifafina, 2019. Cap. 8. p. 77-85, p. 77. Disponível em: https://www.udop.com.br/noticia/2020/03/03/o-que-estao-fazendo-com-os-meus-dadosy-a-importancia-da-lei-geral-de-protecao-de-dados.html. Acesso em: 11 dez. 2020.

adotar providências". Conforme dito anteriormente, o encarregado é responsável por ser um canal de comunicação dos titulares com a empresa, solucionando problemas e orientando os titulares.

A segunda atividade, estabelecida no inciso II, refere-se a "receber comunicações da autoridade nacional e adotar providências", sendo essa uma competência interna do encarregado. Nesse interim, o agente é responsável por implementar dentro da empresa as diretrizes estabelecidas pela Autoridade Nacional de Proteção de Dados. Medida essa extremamente importante, uma vez que visa manter a empresa atualizada e dentro dos padrões da legislação.

O inciso III também trata da função voltada para a empresa do encarregado. Nesse sentido, impõem-se que o agente deve "orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais ". Dessa forma, se entende que o agente possui uma função de estruturar um complience dentro da empresa, informando os próprios funcionários sobre as novas normas e resoluções editadas pela Autoridade Nacional de Proteção de Dados. Por consequência, criando uma cultura de cuidado com os dados pessoais dentro da empresa.

Finalmente, o inciso IV traz uma competência mais genérica atribuindo ao encarregado o papel de "executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares." Isso demonstra que o encarregado nada mais é que um subordinado direto do controlador, devendo em observância a lei, respeitar os direcionamentos dados por ele.

Passando para o §3 temos que "A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados." Nesse sentido, vale ressaltar que o encarregado no Brasil é agente obrigatório a toda pessoa que lide com dados pessoas, desde o consultório médico até as grandes empresas multinacionais. Contudo, esse entendimento do legislador é muito criticado, uma vez que em se tratando de pessoas jurídicas de pequeno porte a contratação de um encarregado onera em excesso o empreendedor. Tendo isso em vista, há uma crença de que a tendência é que essa obrigatoriedade cesse na medida em que a lei for colocada em pratica, através do art. 41, §3. Isso porque tal artigo estabelece que a ANPD pode dispensar a necessidade de indicação do encarregado, observando-se a "a natureza e o porte da entidade ou o volume de operações de tratamento de dados." a natureza e o porte da entidade ou o volume de operações de tratamento de dados."

7. COMPARATIVO GDPR X LGPD

Conforme foi anteriormente apresentado, a GDPR é a lei equivalente a LGPD na Europa, e é através dela que os países do continente Europeu traçam normas para salvaguardar os dados pessoais dos cidadãos.

Vale ressaltar que a LGPD se inspirou na legislação europeia em muitos aspectos[120], porém há distinções significativas que merecem ser tratadas com relação aos agentes de tratamento. Dentre elas, a principal é o papel do DPO (*Data Protection Officer*) que no Brasil é o equivalente ao encarregado[121].

Entre ambos os agentes a principal diferença é que o encarregado é agente obrigatório a todas as pessoas que lidam com dados pessoais[122], enquanto o DPO se faz necessário apenas em casos específicos estipulados em lei[123].

Existem outras diferenças menos fundamentais, uma delas é que o DPO não poderá receber instruções sobre o exercício de suas funções, conforme art. 38, 3 da GDPR. Em contrapartida, conforme inciso IV do art. 41, o encarregado deve executar as demandas determinadas pelo controlador.

Por fim, o DPO possui um maior número de tarefas colocadas na legislação que o encarregado, bem como, no geral lidam com um maior volume de dados ou então com o grupo específico dos dados sensíveis.

8. RESPONSABILIDADES DO ENCARREGADO

Observando-se a legislação de proteção de dados art. 6, X c/c art. 42, resta evidente que a responsabilidade pelo cumprimento das normas de proteção de dados são do controlado ou do operador.

Adicionalmente, conforme o art. 2 da CLT, o responsável pela atividade econômica é o empregador, tendo, inclusive, o próprio STF, sob a égide da Súmula 341, definido que há

---

[120] MULHOLLAND, C. S. **Dados pessoais sensíveis e a tutela de direitos fundamentais**: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, v. 19, n. 3, p. 159-180, 29 dez. 2018, p. 167.
[121] Ver art. 5º, VIII, da LGPD c/c art. 37 da GDPR.
[122] Ver art. 41 da LGPD.
[123] Ver art. 37 da GDPR.

responsabilidade presumida do empregador pelos atos culposos praticados pelo empregado. Trata-se, aqui, de responsabilidade objetiva.

Dito isso, para que ocorra a responsabilização do empregado é necessário que o empregador comprove que o ato ilícito cometido seja fruto de ação ou omissão feita com dolo ou que agindo culposamente teve o como resultado o dano involuntário, prescindindo ainda, no último caso, a necessidade de previsão contratual para ressarcimento com base em culpa.

Dessa forma, entendendo-se o encarregado como um trabalhador celetista, subordinado ao operador e ao controlador, é razoável não ser ele responsabilizado de forma pessoal.[124]

Logo, qualquer eventual responsabilização na pessoa física do empregado só seria possível, conforme a legislação, no caso de ação ou omissão com dolo ou nos casos de ação ou omissão culposa em que houver previsão contratual. Para tanto é necessário a comprovação do nexo causal entre o fato intencional praticado e o evento danoso.

Em resumo, por ser um funcionário celetista, o encarregado não possui autonomia para tomada de decisões, especialmente as que envolvem riscos, por conseguinte, é visto como subordinado ao operador e ao controlador. Assim, a empresa por mais que orientada pelo Encarregado permanece livre para decidir seguir ou não as diretrizes por ele informadas, o que corrobora com a ideia de que não há que se falar em responsabilização por parte do empregado.

CONCLUSÃO

Conforme foi possível verificar ao longo desta pequena obra, os agentes de tratamento são as pessoas sobre as quais recairão as responsabilidades e as atribuições do tratamento de dados pessoais, devendo estes agentes adequarem-se às determinações legais e contratuais que porventura estabelecerem entre si. Ademais, não se findam suas responsabilidades apenas no texto da LGPD, mas devem ser compreendidas também através de uma análise sistêmica de toda a LGPD e do diálogo das fontes com outros institutos e princípios do ordenamento jurídico brasileiro como um todo. A LGPD é bastante nova, como o é o tema que ela visa regular, mas a necessidade de regulamentação já se faz com atraso: o mundo, em sua infinita evolução, não para,

[124] CABELLA, Daniela Monte Serrat *et al*. **Responsabilidade civil do encarregado pelo tratamento de dados pessoais: regime celetista**. Migalhas, 15 de outubro de 2020. Disponível em < https://migalhas.uol.com.br/depeso/334947/responsabilidade-civil-do-encarregado-pelo-tratamento-de-dados-pessoais--regime-celetista> Acesso em 11 de dezembro de 2020.

e deverá o Direito saber caminhar para se adequar às novas realidades do século XXI e de todos os que vierem depois, a fim de que possam ser garantidos os direitos das muitas pessoas que a ele estão submetidas.

REFERÊNCIAS BIBLIOGRÁFICAS:

BAUMAN, Zygmunt. **Globalização**: as consequências humanas. Rio de Janeiro: Zahar, 1999. Tradução de: Marcus Penchel.

CABELLA, Daniela Monte Serrat; LIMA, Denise; FERREIRA, Raíssa Moura; ROCHA, Ana Beatriz. **Responsabilidade civil do encarregado pelo tratamento de dados pessoais: regime celetista**. Migalhas, 15 de outubro de 2020. Disponível em < https://migalhas.uol.com.br/depeso/334947/responsabilidade-civil-do-encarregado-pelo-tratamento-de-dados-pessoais--regime-celetista> Acesso em 11 de dezembro de 2020.

GE, Yanbo et al. "**Racial and Gender Discrimination in Transportation Network Companies**" [Discriminação racial e de gênero em companhias de redes de transporte], em National Bureau of Economic Research, out. 2016. Disponível em <https://www.nber.org/papers/w22776>, acesso em 11 de dezembro de 2020.

GOMES, Maria Cecília Oliveira. **Relatório de impacto à proteção de dados**: uma breve análise da sua definição e papel na LGPD. Revista do advogado, nº 144, p. 174-183, nov. 2019.

KOHN, Karen; MORAES, Cláudia Herte de. **O impacto das novas tecnologias na sociedade: conceitos e características da sociedade da informação e da sociedade digital**. In: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 2007, Santos. Anais [...]. Santos: Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, 2007. p. 1-13.

KREMER, Bianca. Os agentes de tratamento de dados pessoais. In: MULHOLLAND, Caitlin (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipelago, 2020. p. 289-318.

MATTOS, Bruna; ANDRADE, Genifer; BATISTA, Hélio; LUMACK, Leonardo. Dos agentes de tratamento dos dados pessoais. In: SALDANHA, Paloma Mendes (org.). **O que estão fazendo com meus dados?** / a importância da lei geral de proteção de dados. Recife: Serifafina, 2019. Cap. 8. p. 77-85. Disponível em: https://www.udop.com.br/noticia/2020/03/03/o-que-estao-fazendo-com-os-meus-dadosy-a-importancia-da-lei-geral-de-protecao-de-dados.html. Acesso em: 11 dez. 2020.

MULHOLLAND, C. S. **Dados pessoais sensíveis e a tutela de direitos fundamentais**: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, v. 19, n. 3, p. 159-180, 29 dez. 2018.

SLEE, Tom. **Uberização**: a nova onda do trabalho precarizado. São Paulo: Elefante, 2017. Tradução de: João Peres.

A RELEVANCIA DAS AGENCIAS DE PROTEÇÃO DE DADOS PESSOAIS PARA O DIREITO DO CONSUMIDOR.

Plinio Lacerda Martins

Leticia Lacerda Moura Martins

Resumo: Foi editada no Brasil a Lei Geral de Proteção de Dados, lei 13.709/2018, que sofreu influencias da *General Data Protection Regulation* (*GDPR*) que entrou em vigência em 25 de maio de 2018, com objetivo de garantir a proteção de dados pessoais na Europa, em razão do armazenamento de informações por parte de empresas. Todavia, no Brasil foi vetado a criação da Autoridade Nacional de Proteção de Dados (ANPD) autarquia que seria vinculada ao Ministério da Justiça, com atribuição inclusive de aplicar sanções na hipótese do uso de dados fora da legislação. Observa-se que nos Países com Agencia de Proteção de Dados a legislação protetiva possui maior eficácia em razão da fiscalização e aplicação de sanções.

Abstract: The General Data Protection Act, law 13709/2018, was published in Brazil and was influenced by General Data Protection Regulation (GDPR), which came into force on May 25, 2018, in order to guarantee the protection of personal data in Europe , due to the storage of information by companies. However, in Brazil, the creation of the National Data Protection Authority (ANPD) was banned, which would be linked to the Ministry of Justice, with the attribution of sanctions in the hypothesis of the use of data outside the legislation. It is observed that in the Countries with Data Protection Agency the protection legislation is more effective due to the supervision and application of sanctions

1. INTRODUÇÃO

Zygmunt Bauman, na célebre frase que *na sociedade de consumidores, ninguém pode se tornar sujeito sem primeiro virar mercadoria,* sintetiza que o consumidor por meio dos dados fornecidos no mercado de consumo, torna-se uma série de números armazenados em bancos de dados negociáveis.[125]

Assim, os dados pessoais do consumidor, circulam na sociedade de consumo, arquivados em bancos de dados amplamente mercantilizados em aplicativos e redes sociais inclusive gratuitos, sem aquiescência do mesmo.

Em 25 de maio de 2018, entrou em vigor na União Europeia a *General Data Protection Regulation – GDPR.*, objetivando garantir a proteção de dados pessoais na Europa, em razão do armazenamento de informações por parte de empresas.

A GDPR foi aprovada pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho em 27 de abril de 2016, possuindo como objetivo a proteção dos dados pessoais dos

[125] BAUMAN, Zygmunt. Vida para consumo: a transformação das pessoas em mercadoria. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2008. p. 20

cidadãos e também a segurança jurídica no mercado de consumo em especial no mercado digital, substituindo assim a Diretiva 95/46/EC, de 1995 [126].

Constata-se que no Brasil a GDPR influenciou a recente lei 13.709/2018, sancionada este ano, denominada Lei Geral de Proteção de Dados, considerada como a primeira legislação brasileira a tratar especificamente do direito à privacidade.

Contudo, diferente dos demais países que possuem Agência reguladora de dados pessoais, no Brasil, seguiu tramite diverso das demais Agencias de Proteção de Dados deixando assim dúvidas a respeito da independência da Agencia criada, alvo de análise neste ensaio jurídico, sem a pretensão de esgotar o assunto, busca trazer reflexões a respeito do impacto em relação a autonomia da APD.

2. LEI ESPECIFICA DE DADOS PESSOAIS NO BRASIL SUPRE LACUNA LEGISLATIVA.

O Brasil era o único país da América Latina que não dispunha de uma legislação específica de proteção a dados pessoais.

Existem inúmeras leis que disciplinam o direito de acesso a informação como a Lei de Acesso a Informação (LAI), a Lei do Marco Civil, a Lei do Castro Positivo, Código Civil, o próprio Código de Defesa do Consumidor, Decreto dos contratos eletrônicos, etc... Porém, conforme mencionado pela própria Lei do Marco Civil, faz-se necessário lei especifica para a proteção e tratamento dos dados pessoais armazenados pelos setores públicos e privados.

Em relação aos dados públicos, há o entendimento que a lei de acesso a informação, Lei 12.527/2011, já efetua a regulação dos dados públicos estabelecendo o tratamento das informações pessoais que *deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais* (art. 31)[127], permitindo inclusive aplicação da lei do *habeas data* como mecanismo de acesso aos dados de pessoa física ou jurídica constante de registro ou banco de dados de entidades governamentais ou caráter público. Assim dispõe o art. 38 da LAI:

> Art. 38. Aplica-se, no que couber, a Lei no 9.507, de 12 de novembro de 1997, em relação à informação de pessoa, física ou jurídica, constante de registro ou banco de dados de entidades governamentais ou de caráter público.

Em relação ao tratamento dado ao contrato eletrônico pelo Marco Civil da Internet, Dennis Verbicaro, destaca que cabe mencionar a alternativa legislativa, não obstante as respectivas leis e decretos sobre a matéria, insistindo, que discussões e audiências públicas sejam promovidas

---

[126] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

[127] Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

com o propósito de avaliar o tratamento dado ao contrato eletrônico pelo Marco Civil da Internet, aprimorando a experiência do usuário brasileiro enquanto cidadão-consumidor.[128]

Laura Mendes já sustentava a necessidade de criação de lei própria a respeito dos dados pessoais, afirmando que cabe ao Estado, por meio de legislação, prover os mecanismos necessários para que o cidadão possa exercer o controle do fluxo de informações a seu respeito na sociedade[129].

O Ministro Ricardo Villas-Bôas Cueva, do Superior Tribunal de Justiça explanou que embora o Brasil tenha *alguma proteção aos dados pessoais* de seus cidadãos, é urgente que o país aprove uma lei que defina princípios claros na matéria e proteja contra o mau uso de informações pessoais por empresas, sustentando Cueva:

> É preciso que tenhamos urgência na aprovação da lei para que tenhamos alguma proteção de dados", sob pena de serem nossos perfis pessoais vendidos como mercadorias, colocando em risco todos os cidadãos[130].

Registra-se que a maioria dos países possuem legislação especifica em relação a proteção de dados de uma pessoa. Uma lei específica sobre proteção de dados permite que o cidadão tenha controle sobre suas informações, inclusive em relação a forma como são utilizadas por organizações, empresas e pelo próprio governo.

Verifica-se que o Chile possui, desde 1999, a Lei 19.628/99, que regula a proteção aos dados pessoais[131]. Na argentina, a proteção aos dados está consignada na Lei 25.326/2000[132]. No México a legislação de proteção de dados pessoais surgiu em 2010 através da *Ley federal de Protección de Datos Personde los Particularesales em Posesión de los particulares*[133].

A lei tem por objetivo estabelecer padrões mínimos a serem seguidos quando ocorrer o uso de um dado pessoal, devendo possuir ambiente seguro e controlado para seu uso assegurando ao cidadão/consumidor o direito de ser consultado.

A relevância de uma lei sobre proteção de dados pessoais traduz no equilíbrio das assimetrias de poder sobre a informação pessoal existente entre o titular dos dados pessoais e aqueles que os usam e compartilham.

A título de ilustração, foi divulgado pela mídia, que o site de consulta aos dados pessoais denominado *Telefone ninja*, permite a consulta de dados pessoais do consumidor sem a sua anuência. O site defende alegando que a Resolução da Anatel nº 345/2003, permite o acesso

---

[128] VERBICARO, Dennis e MARTINA, Ana Paula Pereira. contratação eletrônica de aplicativos virtuais no Brasil e a nova dimensão da privacidade do consumidor. *Revista de Direito do Consumidor.* São Paulo: RT .RDC VOL. 116 Março - Abril 2018, p.12.

[129] MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais, *In* MARQUES, Claudia Lima e GSELL, Beate. *Novas Tendências do Direito do Consumidor*. RT: São Paulo, 2016, p.188.

[130] Palestra proferida em 15/8/2017, em São Paulo, disponível em: <http://www.conjur.com.br/2017-ago-15/brasil-lei-protecao-dados-pessoais-cueva> Acesso em: 01 out. 2017.

[131] Disponível em http://www.sernac.cl/leyes/comppendio/docs_compendio/ley19628.pdf. Acesso em: 15 jun. 2018.

[132] Disponível em <http://www.jus.gob.ar/datos personales.aspx> Acesso em: 15 jun. 2018.

[133] Disponível em: <http://www.ifai.org.mx/> Acesso em: 15 de jun. de 2018.

dos dados, na hipótese do usuário não ter solicitado a restrição. Dispõe o § 2º e 4º do art. 10 da Resolução Anatel 345/2003:

> Art. 10**.** A Relação de Assinantes deve conter os dados básicos de todos os assinantes com terminais em serviço ou desligados temporariamente e os dos novos assinantes que serão ativados nos prazos previstos na regulamentação subseqüentes à data de fornecimento da Relação de Assinantes.
>
> **§2º** A prestadora deve excluir da Relação de Assinantes, os assinantes que tenham se **manifestado pela não-divulgação de seu código de acesso**.
>
> **§4º** Visando ao fornecimento de exemplar de lista telefônica aos assinantes que tenham **solicitado a não-divulgação de seus dados**, a prestadora deve fornecer à divulgadora listagem contendo exclusivamente os endereços desses assinantes. (grifamos)[134].

A Lei Geral de Telecomunicações consigna um relevante exemplo contrário ao ordenamento jurídico do consumidor, ao estabelecer um dever para o usuário do serviço de telefonia envolvendo os dados pessoais do mesmo. A Lei nº. 9.472/97 ratifica o entendimento, que o usuário de telecomunicações tem o direito a não divulgação de seu código de acesso, caso seja requerido pelo mesmo.

Estabelece o art. 3, inciso VI da lei 9.472/97:

> Art. 3° O usuário de serviços de telecomunicações tem direito:
>
> VI - à não divulgação, caso o requeira, de seu código de acesso [135].

O art. 3 foi regulamentado pela Resolução da Anatel nº 066/98 que afirma:

> Art. 2º Para os fins deste Regulamento, aplicam-se as seguintes definições:
>
> IV - Código de acesso não figurante é aquele que, mediante **solicitação do assinante ou usuário indicado**, não deve constar da relação de assinantes , nos termos do Art. 3º, Inciso VI, da Lei nº 9.472/97; (grifamos)[136].

---

[134] Ver também o art. 13, 14 e 15 da Mesma Resolução.

[135] A mesma lei estabelece no art. 213, §§ 1º e 2º: *Art. 213. Será livre a qualquer interessado a divulgação, por qualquer meio, de listas de assinantes do serviço telefônico fixo comutado destinado ao uso do público em geral.*
§ 1º Observado o disposto nos incisos VI e IX do art. 3° desta Lei, as prestadoras do serviço serão obrigadas a fornecer, em prazos e a preços razoáveis e de forma não discriminatória, a relação de seus assinantes a quem queira divulgá-la.
§ 2º É obrigatório e gratuito o fornecimento, pela prestadora, de listas telefônicas aos assinantes dos serviços, diretamente ou por meio de terceiros, nos termos em que dispuser a Agência.

[136] A Resolução Anatel nº 066/98 no art. 3 assegura o direito a divulgação dos dados in verbis: *Art. 3º Será livre a qualquer interessado a divulgação, por qualquer meio, de listas de assinantes do STFC-LO.*

Faz-se necessário cotejar as normas próprias de defesa do usuário do serviço público[137] com o código de defesa do consumidor, assim como o faz a legislação do consumidor da Itália, que estabelece como norma complementar a norma do consumidor em relação ao Código de Proteção de Dados Pessoais[138].

Ricardo Perlingeiro, em relação a necessidade de lei para regular o acesso a informação pública, afiança que a Corte Suprema de Justiça da Nação Argentina, em 2014, afirmou que a *obrigação de garantir o acesso a informação por mandamento constitucional está a cargo do Estado* e que a Constituição estabelece o direito de acesso a informação pública como uma condição necessária para organizar uma república democrática, sendo indubitável que, a fim de que o direito à informação seja efetivamente garantido, *o Estado deve ditar urgentemente uma lei que, salvaguardando as normas internacionais sobre a matéria e o princípio da razoabilidade, regule de maneira exaustiva o modo como as autoridades públicas devem satisfazer esse direito*"[139].

Já somávamos ao entendimento daqueles doutrinadores que entendiam pela necessidade de uma lei especifica para a proteção dos dados públicos e privados em um único ordenamento jurídico, como dispunha a Diretiva da União Europeia.

Assim, com a edição da lei 13.709/2018 foi preenchido a lacuna da necessidade de uma lei específica de proteção de dados pessoais inclusive dos consumidores.

3.DADOS PESSOAIS DO CONSUMIDOR

O dado pessoal se refere a qualquer informação que possa ser associada a uma pessoa como endereço, profissão, lugares por onde costuma andar, impressões digitais e tantas outras, que conforme foi vista, dá margem a um sistema de processamento de dados e informações recebendo a denominação de fenômeno *Big Data*.

A lei 13.709/2018 conceitua dado pessoal no art. 5 dispondo:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter

[137] A lei 13.460/2017 estabelece normas básicas para a proteção e defesa dos direitos do usuário dos serviços públicos prestados direta ou indiretamente pela administração pública, afiançando que aplicação desta Lei não afasta a aplicação da Lei nº 8.078, quando caracterizada relação de consumo,

[138] O decreto Legislativo nº 196/2003, denominado Código de Proteção de Dados Pessoais da Itália, contem normas de coleta, guarda, armazenamento e tratamento de dados, existindo uma relação de complementaridade entre proteção do consumidor e proteção de dados pessoais, pois a tutela da privacidade, contida no Código de Proteção de Dados Pessoais, contém normas específicas de proteção das informações que são comunicadas pelo cidadão também na condição de consumidor.

[139] PERLINGEIRO, Ricardo; DÍAZ, Ivonne; LIANI, Milena. Princípios sobre o direito de acesso à informação oficial na América Latina. *Revista de Investigações Constitucionais*, Curitiba, vol. 3, n. 2, p. 143-197, maio/ ago. 2016. DOI: http://dx.doi.org/10.5380/rinc.v3i2.46451. p. 150.

> religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), estabelecendo o direito a proteção dos dados de caráter pessoal, afirmando:

> (1) A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.o, n.o 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.o, n.o 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.[140]

Rodotà já lecionava, que a **Convenção do Conselho da Europa** de 28 de janeiro de 1981, para a proteção das pessoas em relação à coleta automática dos dados, e a **Recomendação da OCDE** de 23 de setembro de 1980, contém as diretrizes relativas à proteção da vida privada e à circulação transnacional dos dados de caráter pessoal, extraindo assim os princípios acima relacionados aos dados pessoais[141].

Há varias práticas usuais no dia a dia de quem usa a internet, por exemplo, relacionado aos *termos de uso* de uma aplicação na internet, que basta um click para a liberação de seus dados pessoais para diversos usos, envolvendo um contexto de massificação de coleta de informações que podem estar sendo usadas sem a sua autorização, ou menos sem a aquiescência do objetivo a que se destina.

Na sociedade contemporânea, há um universo com capacidade de captura, como por exemplo os *smartphones* que possuem armazenamento, processamento e análise dos dados de pessoas com que vivemos[142].

Danilo Doneda expõe ao analisar os princípios protetivos dos dados pessoais, concluindo por constatar que tais princípios revelam muito mais do que demandas setoriais, valores gerais ou até a vinculação com a funcionalização de uma garantia fundamental de proteção dos dados pessoais. Por esta razão, mais do que serem considerados dentro do espectro de sua normativa, devem os mesmos ser interpretados de forma extensiva para considerar abarcar e

---

[140] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

[141] RODOTÀ, Stefano. ***A Vida na Sociedade da Vigilância. A Privacidade Hoje***, Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.59.

[142] Em relação aos termos digitais, recomendamos a leitura da obra: *Teoria das Mídias, linguagem ambientes e rede*. Luís Mauro Sa Martinho. Petrópolis, RJ: Vozes, 2015.

proteger todas as situações nas quais possam propiciar a tutela concernente com as características da atual sociedade tecnológica informacional[143].

Em relação a origem da internet, Castells leciona que a internet originou de um esquema ousado, imaginado na década de 1960 *pelos guerreiros tecnólogos da Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos (a mítica Darpa) para impedir a tomada ou destruição do sistema norte-americano de comunicações pelos soviéticos, em caso de guerra nuclear*[144].

Apesar disso, hoje a preocupação atual, volta-se para a popularização das tecnologias de coleta de dados pessoais e a criação de um autêntico mercado envolvendo as informações. Empresas como Google e Facebook têm como núcleo de seu modelo de negócio a venda de publicidade dirigida ao público-alvo de acordo com informações estatísticas de acesso à internet, localização, hábitos de navegação, hábitos de consumo etc.

A questão envolve a alta tecnologia da informação sobressaindo para as tecnologias de vigilância que são as que permitem a interceptação de mensagens, o rastreamento dos fluxos de comunicação e o monitoramento ininterrupto das atividades da máquina.

Este é um tipo de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros, podendo comprometer a privacidade do usuário e a segurança do computador. Algumas de suas funções são, por exemplo, o monitoramento de URLs acessadas enquanto o usuário navega na Internet e captura de senhas bancárias e números de cartões de credito. Conforme afirma Castells, *no ambiente tecnológico atual, toda informação eletronicamente transmitida é gravada, podendo vir a ser processada, identificada e combinada numa unidade de análise coletiva ou individual*[145].

Conforme visto, no Brasil há inúmeras leis de proteção aos dados pessoais, citando como exemplo a Lei 12.414/2011,[146] que disciplinou o cadastro positivo e aspectos sobre proteção de dados pessoais creditício, estabelecendo inclusive o conceito de dados sensíveis no art, 3º, II que dispõe:

> § 3º Ficam proibidas as anotações de:
> I - Omissis -
> II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

Há ainda a Lei 12.737/2012 denominada Lei Carolina Dieckmann[147], que define como crime o fato de invadir dispositivo informático alheio, acrescentando ao Código Penal essa tipificação de crime denominado de delitos informáticos.

---

[143] DONEDA, Danilo. Princípios da proteção de dados pessoais, p.369 a 384, *In Direito e Internet III*, org. Adalberto Simão Filho, Newton De Lucca e Cintia R.P. Lima, São Paulo: Quartier Latin, 2015, p.384.
[144] CASTELLS, Manuel. *A sociedade em rede.* São Paulo: Paz e Terra, 2016, p. 65
[145] CASTELLS, Manuel. *A Galáxia da Internet. Reflexões sobre a internet, os negócios e a sociedade*. Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar Ed., 2003, p. 141 e 142.
[146] A lei 12.414/2011, foi regulamentada através do Decreto 7.829/2012.
[147] Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>Acesso em: 31 de agost. 2018.

A Lei do Marco civil na internet, Lei 12.965/14, disciplina que o uso da internet deve obedecer ao princípio da proteção dos dados pessoais. Contudo, conforme acima citado, a lei do marco civil faz referência a necessidade da obediência ao princípio da proteção dos dados pessoais na forma da lei, demonstrando assim a necessidade de criação de lei própria.

Assim dispõe o art. 3º da lei em comento:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> II - Proteção da privacidade;
> III - Proteção dos dados pessoais, na forma da lei;

Verificamos, que no ano de 2013, o Governo Federal editou o Decreto 7.963 de 2013, instituindo o Plano Nacional de Consumo e Cidadania, denominado PLANDEC, estabelecendo como diretriz, entre outras, a *autodeterminação, privacidade, confidencialidade e segurança das informações e dados pessoais prestados ou coletados, inclusive por meio eletrônico*, porém não restou regulado a questão da proteção e tratamentos dos dados[148].

Neste contexto, em face do registro acima de inúmeras praticas envolvendo os dados pessoais de consumidores, festeja-se a edição da lei 13.709/2018, lei especifica com objetivo de garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa, inclusive do consumidor, particularmente em relação a sua liberdade, privacidade, intimidade, honra e imagem.

3. AUTORIDADE PARA CONTROLE DOS DADOS PESSOAIS

A lei de dados pessoais brasileira, lei 13.709/2018 foi alvo de críticas doutrinárias em razão da criação da Agencia de Proteção de Dados e sua autonomia para apurar os atos infracionais e de fiscalização ao cumprimento.

A doutrina brasileira lamenta o veto presidencial não permitindo a criação da Autoridade Nacional de Proteção de Dados (ANPD), autarquia que seria vinculada ao Ministério da Justiça, que teria atribuição de, por exemplo, elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade, fiscalizar e a aplicar sanções em caso uso de dados fora da legislação.[149]

Rodotà adverte que o poder de controle e intervenção em relação aos dados pessoais não devem mais ser atribuídos somente aos interessados diretos, devem ser confiados também a uma autoridade independente, envolvendo uma responsabilidade pública específica[150].

---

[148] Decreto 7.963 de 15 de março de 2013, art. 2, VII. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7963.htm>Acesso em: 27 de out. 2017.

[149] O veto presidencial explicou que só lei de iniciativa da Presidência da República pode criar cargos e gastos no Poder Executivo, afirmando que a criação da agência reguladora de dados não veio acompanhada da devida previsão de impacto no Orçamento.

[150] RODOTÁ, Stefano. *A vida na Sociedade de Vigilância. A privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008, p.199.

Na Itália, existe a autoridade de garantia, denominado de Garantidor da Proteção de Dados Pessoais, que é o órgão administrativo responsável, pelos casos envolvendo proteção de informações pessoais do consumidor [151], através do decreto Legislativo nº 196/2003, denominado Código de Proteção de Dados Pessoais, contendo normas de coleta, guarda, armazenamento e tratamento de dados pessoais, somados as outras fontes normativas nacionais e europeias.

O Decreto Legislativo n° 196 previu expressamente a figura do Garante, no seu art. 153 e 154, afirmando que, o Garante atuará com plena autonomia e independência de juízo e de valoração[152].

O controle da aplicação das normas contidas no Código de Proteção de Dados Pessoais é efetuado a pedido de algum órgão ou pessoa interessada, sendo realizado de forma paralela o controle por amostragem pelo órgão administrativo fiscalizador denominado Garantidor da Proteção de Dados Pessoais[153], que pode impor sanções de caráter administrativo ou penal.

Na Espanha a Lei 34/2002 atribui as funções de supervisão e controle de seus dispositivos ao Ministério de Indústria, Energia e Turismo, por meio da Secretaria de Estado de Telecomunicações e para a Sociedade da Informação. Nos casos relativos a comunicações comerciais eletrônicas a competência sancionadora recai sobre a Agência Espanhola da Proteção de Dados (AGPD)[154]. A Espanha possui ainda, A Agência Espanhola de Proteção de Dados (AEPD), entidade de direito público é dotada de autonomia, relaciona-se com o Governo por meio do Ministério da Justiça, responsável por velar pelo cumprimento de normativas relacionadas à proteção de dados pessoais, em particular a Lei Orgânica 15/1999[155].

Em Portugal compete a Comissão Nacional de Proteção de Dados – CNPD, a organização e o funcionamento regulamentado pela Lei nº 43/2004. A Comissão Nacional de Proteção de Dados é uma entidade administrativa independente com poderes de autoridade, que funciona junto da Assembleia da República.

Possui a atribuição de controlar e fiscalizar o processamento de dados pessoais, além de cooperar com as autoridades de controle de proteção de dados de outros Estados, nomeadamente na defesa e no exercício dos direitos de pessoas residentes no estrangeiro. As decisões proferidas pela Comissão têm força obrigatória e são passíveis de reclamação e de recurso para o Tribunal Central Administrativo. No caso de processos de contra ordenação, as decisões da

---

[151] Disponível em: <http://pensando.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/21-It%C3%A1lia.pdf > Acesso em: 22 out. 2017.

[152] O Art. 153 do Código em matéria de Proteção de Dados Pessoais estabelece que: *1. Il Garante opera in piena autonomia e con indipendenza de giuduzio e di valutazione. 2. Il Garante e' organo collegiale costituito de quatro componenti, eletti due dalla Camera dei deputatu e due dal Senato dellla Repubblica com voto limitadto. I componenti sono scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competennza dele materie del diritto o dell'informatica, garantindo la presenza di entramble le qualificazioni*. Disponível em: http://www.parlamento.it/parlam/leggi/deleghe/03196dl.htm. Acesso em: 20 abr. 2018.

[153] O Garantidor da Proteção dos Dados Pessoais é autoridade administrativa independente instituída pela Lei da Privacidade, em 1996. Trata-se de órgão colegiado formado por quatro membros eleitos oriundos do Parlamento, para mandato não-renovável de sete anos. Os quatro membros são: Presidente, Vice-Presidente e dois componentes. O órgão é composto por 145 funcionários, divididos entre dirigentes, funcionários operacionais e executivos. O orçamento atual do Garantidor é de EUR 28.597.993,00. Disponível em: <http://pensando.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/21-It%C3%A1lia.pdf>Acesso em: 13 jun. 2017.

[154] Cf. arts. 21 e 22.

[155] A AEPD conta com efetivo de cerca de 150 funcionários, distribuídos entre Secretaria-geral; Subdireção de Registro Geral de Proteção de Dados; Subdireção de Inspeção de Dados Disponível em http://www.agpd.es.

Comissão são recorríveis para os tribunais de pequena instância criminal ou para os tribunais judiciais competentes[156].

Em 1994 foi publicada a Lei nº 2 que estabelece os mecanismos de controle e fiscalização do sistema de informação Schengen (sistema de informação Schengen tem por objetivo preservar a ordem e a segurança pública, incluindo a segurança do Estado, bem como a aplicação das disposições da Convenção sobre a Circulação das Pessoas nos Territórios das Partes Contratantes com o apoio das informações transmitidas por este Sistema)[157].

Na Alemanha o Representante Federal para Proteção de Dados e Liberdade de Informação, denominado de Comissário Federal para Proteção de Dados e Liberdade de Informação (BfDI, na sigla em alemão), é designada pelo Parlamento, por indicação do Governo Federal. O cargo tem independência oficial no desempenho de suas funções, mas está sob a supervisão legal do Governo Federal e sob a supervisão administrativa do Ministério do Interior[158]. O Comissário Federal para a Proteção de Dados e Liberdade de Informação existe desde 1978[159].

Em relação aos dados abertos (*open data*) e a seu acesso gratuito, cabe registrar que a França já possui estrutura para essa atividade. O *Etalab* é unidade que opera diretamente junto ao Primeiro-Ministro da França e tem como competência gerir a política de abertura e compartilhamento de dados abertos [160].

A gestão e proteção de dados pessoais, regulamentada pela Convenção do Conselho da Europa nº 108, de 28 de janeiro de 1981, pela Diretiva europeia nº 95/46/CE, de 24 de outubro de 1995, pela lei 575-2004, de 21 de junho de 2004, e pela 78-17, de 6 de janeiro de 1978, atualizada por modificações ao longo dos últimos aos, especialmente pela lei 2004-801. O controle e tratamento de denúncias são realizados por comissões internas da CNIL[161].

Contudo, a Diretiva europeia nº 95/46/CE foi revogada, com a edição do General Data Protection Regulation, em vigor a partir de 25 de maio de 2018, resultado da iniciativa da União Europeia, garantindo assim nova proteção aos dados pessoais.

---

[156] Disponível em: <http://www.cnpd.pt/bin/cnpd/acnpd.htm>. Acesso: 02 jun. 2014.

[157] Art. 2º, nº 1. Disponível: http://www.cnpd.pt/bin/legis/nacional/Lei2-94-Schengen.pdf. Acesso: 02 jun/2018.

[158] A BfDI, que tem sede em Bonn, conta com o apoio de cerca de 90 funcionários, divididos em 9 departamentos. Suas atribuições, que estão descritas na BDSG, incluem aconselhar e controlar autoridades e órgãos federais, empresas de telecomunicação e de correio. Qualquer pessoa podem recorrer à BfDI se considerar que seus direitos pessoais de proteção de dados foram violados. O sistema alemão, porém, é bastante complexo, e a BfDI não é a única instituição responsável por supervisionar e controlar a implementação das regras de proteção de dados. Cada estado federal alemão tem seu próprio Representante para Proteção de Dados, bem como competência para regular como será feito o controle de proteção de dados de suas instituições e das empresas com sede em seu território. A Baviera, por exemplo, além de um Representante, tem uma agência especial responsável apenas pela supervisão de instituições privadas. O estado federal de Schleswig-Holstein, por sua vez, encarrega uma instituição independente com a responsabilidade de supervisão.

[159] Disponível em < https://www.bfdi.bund.de/DE/BfDI/Artikel_BFDI/AufgabenBFDI.html?nn=5217014#doc5557210bodyText4> Acesso em 13/09/2018.

[160] A entidade coordena a ação dos serviços de Estado e de estabelecimentos públicos, a fim de facilitar a reutilização *a mais ampla possível de suas informações públicas*. O Estado também administra o portal *único interministerial* data.gouv.fr, que congrega e disponibiliza o conjunto de informações públicas.

[161] Câmara com 5 membros podem aplicar sanções pecuniárias de até EUR 300 mil. As decisões da CNIL podem ser objeto de recurso administrativo. Relativamente às sanções, a CNIL aplicou, em 2014, 7 advertências e 7 sanções financeiras, dentre as quais condenação de EUR 150 mil contra a Google por falha de informação, não definição de duração de conservação, falha na base legal para a combinação de dados e falta de obtenção de consentimento.

No Canada há a Lei de Privacidade (*Privacy Act*) [162], em vigor desde 1985, que se aplica a ministérios e órgãos do governo federal e a *Lei de Proteção de Informações Pessoais e de Documentos Eletrônicos* (*Personal Information Protection and Electronic Documents Act* - PIPEDA)[163], sancionada em 2000, que se aplica a organizações do setor privado. O Escritório do Comissário de Privacidade do Canadá (*Office of the Privacy Commissioner of Canada*- OPC) é o órgão responsável pela aplicação das normas de proteção de dados pessoais no país[164].

O México possui a Lei Federal de Transparência e Acesso à Informação Pública Governamental, a Lei Federal de Proteção de Dados Pessoais em Posse dos particulares e seus respectivos regulamentos. Possui autoridade competente para a aplicação da matéria que é o Instituto Federal de Acesso à Informação e Proteção de Dados – IFAI[165].

No Peru, a Lei que regula os dados pessoais é a Ley 29.733[166] de 2013, regulamentada pelo Decreto Supremo n.32.013 e o Código de Proteção e Defesa do Consumidor. No Peru existe a Autoridade Nacional de Proteção de Dados Pessoais (ANPDP), cujas funções são desempenhadas pela Direção Nacional de Proteção de Dados Pessoais do Ministério de Justiça e Direitos Humanos (MINJUS), é a entidade responsável pelo exame das violações à lei de dados pessoais.

No Uruguai a autoridade competente para aplicação imediata da matéria é a Unidade Reguladora e de Controle de Dados Pessoais – URCDP é uma unidade descentralizada da Agencia

---

[162] A Lei de Privacidade, norma federal de direito público, possui três disposições fundamentais: (i) assegura ao cidadão o direito de ter acesso a dados pessoais a seu respeito em poder do governo federal; (ii) impõe ao governo federal a obrigação de implementar políticas e práticas probas de coleta, guarda, utilização e divulgação de informações pessoais sob seu controle; e (iii) cria o Escritório do Comissário para a Proteção da Vida Privada (*Office of the Privacy Commissioner*), subordinado diretamente ao parlamento, para garantir o cumprimento da norma e dirimir conflitos.

[163] Lei de Proteção de Informações Pessoais e de Documentos Eletrônicos (PIPEDA) A "Lei de Proteção de Informações Pessoais e de Documentos Eletrônicos" (*Personal Information Protection and Electronic Documents Act* - PIPEDA), norma federal de direito privado, vigora em todas as províncias que não tenham leis próprias a regulamentar a matéria de modo "substancialmente semelhante" ao daquela norma federal.

[164] Trata-se de órgão independente, que presta contas diretamente à Câmara dos Comuns e ao Senado. A escolha do seu chefe é aprovada pelo Parlamento, com base em indicação feita pelo Gabinete do Primeiro-Ministro. Seis departamentos subordinam-se ao Gabinete do Comissário de Privacidade, quais sejam: a) Direção de Investigações (*Investigations Branch*), composto de duas unidades administrativas: a.1) Direção de Investigações da Lei de Privacidade (*The Privacy Act Investigations Branch*), que recebe e investiga reclamações, no âmbito da Lei de Privacidade, de indivíduos que aleguem não ter acesso a dados pessoais em poder de órgãos de governo, ou que acreditam que seus dados foram coletados, utilizados, divulgados ou manipulados de maneira inapropriada por aqueles órgãos. Esse departamento, ademais, conduz investigações solicitadas diretamente pelo Comissário de Privacidade e recebe notificações de violações de órgãos do governo federal. a.2) Direção de Investigações da PIPEDA (*The PIPEDA Investigations Branch*), que investiga reclamações no âmbito da Lei de Proteção de Informações Pessoais e de Documentos Eletrônicos.

[165]Disponível em: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf> Acesso em: 13 out. 2017. A Lei Federal de Transparência e Acesso à Informação Pública Governamental determinou a criação do Instituto Federal de Acesso à Informação e Proteção de Dados (IFAI). O organismo é autônomo, e seu órgão máximo é o Plenário, composto de 7 conselheiros designados pelo Senado mexicano, posteriormente ratificados pelo Presidente da República. O IFAI é encarregado de 1) Garantir o direito de acesso dos cidadãos à informação pública governamental e 2) Proteger os dados pessoais dos cidadãos, tanto os que estão em possessão do Estado quanto de outros particulares (como empresas). Transmito, a seguir, links para os principais dispositivos legais mencionados acima: -Lei Federal de Telecomunicações e Radiodifusão.

[166] Disponível em <https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf > Acesso em: 15 set. 217.

de Governo Eletrônico e Sociedade de Informação e do Conhecimento a qual integra a estrutura da Presidência da República.

Finalizando, cita-se o caso dos Estados Unidos, que a Federal Trade Comission – FTC, embora não seja um órgão equiparado à Autoridade de Garantia, recebeu a incumbência de fiscalizar a utilização de dados pessoais, que por ter bem cumprido tal encargo, lhe rendeu o título de uma *authority* de fato por alguns estudiosos[167].

Conforme registra Colin Bennett, os Estados Unidos possuem uma regulação abrangente somente para o setor público, não regulamentando o tratamento de dados realizado pelo setor privado, afirmando:

> Os Estados Unidos são agora o único país industrial avançado que ainda não aprovou, nem está em processo de aprovar, uma lei de proteção de dados que abranja também as atividades do setor privado. Embora o Privacy Act de 1974 seja um exemplo desse tipo de legislação, ele é aplicado apenas ao governo federal e sua implementação tem sido muito limitada. No âmbito do poder executivo federal, o Departamento de Administração e Orçamento é tido como o supervisor da aplicação da referida lei pelas agências e órgãos do governo. No entanto, não é uma autoridade "empenhada", em contraste com as agências de proteção à privacidade de outros países, e o seu impacto tem sido tanto esporádico, como brando. Nos Estados Unidos, a adoção de legislação geral para o setor privado tem sido fortemente resistida, e embora existam diversas normas setoriais, a privacidade é protegida de uma forma bastante incompleta[168].

4. CONCLUSÃO

Verificamos assim, que nos países em que não há legislação especifica de proteção de dados pessoais ou mesmo, autoridade de controle de dados pessoais, existem dificuldades na proteção do consumidor e de seus dados. Constatamos, por exemplo, no caso dos Estados Unidos, onde existe lei de proteção à privacidade, no entanto, não tão desenvolvidas quanto na Europa, inexistindo formas de tratamento ou mesmo de autoridade especifica para a questão, muito embora exista a FCT, que é a agência reguladora do comércio dos Estados Unidos.

Nesse sentido, ilustramos como o caso divulgado envolvendo a decisão da FTC, que permitiu que operadoras de cartão de crédito comercializem informações de seus clientes[169], abrindo assim, a porta para a venda de dados cadastrais de usuários[170].

---

[167] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p.387

[168] BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Cornell University Press, 1992, p. 131 (tradução livre).

[169] O site, dos Estados Unidos, *Focus* alega ter detalhadas informações sobre 203 milhões de pessoas, *possuidores do primeiro cartão de crédito, adultos mas ainda vivendo com os pais, pessoas maduras com conhecimento de tecnologias avançadas, novos proprietários de imóveis, compradores com status, grandes gastadores com compras de vitaminas* e *adeptos de regimes alimentares.* CARVALHO, Joatan Marcos. É possível a proteção de dados pessoais? *Revista Luso-Brasileira de Direito do Consumo* - Vol. VII, n. 25 março 2017, Curitiba: Bonijuris, 2017, p. 266.

[170] Também foi noticiado a transferência da regulação das operadoras de telefonia celular da FCC (que trata de comunicações), para a FTC, (que trata de comércio e prestação de serviços), possibilitando a venda de dados cadastrais de usuários de internet móvel e celulares.

Necessário reconhecer o avanço da lei brasileira ao editar a Lei Geral de Proteção de Dados através da lei 13.709/2018, como conquista inclusive para o direito do consumidor.

Conforme relatado, os países que possuem as agências ou órgão fiscalizador de proteção de dados pessoais é permitido a fiscalização e aplicação de sanções, evolvendo o uso indevido dos dados pessoais.

A ausência de autonomia do órgão fiscalizador pode comprometer a lei de dados pessoais prejudicando inclusive o direito do consumidor, parte mais vulnerável no mercado de consumo.

A Recomendação da Diretiva da União Europeia, atualmente revogada pela GDPR já estabelecia a sugestão de criação de autoridade de garantia dos dados pessoais com autonomia e desvinculadas do poder público[171].

Atualmente, a GDPR recomenda a criação de autoridades de controle nos Estados-Membros, habilitadas a desempenhar as suas funções e a exercer os seus poderes com total independência.

Destarte, faz-se necessário registrar a independência da Autoridade Nacional de Proteção de Dados, como órgão autônomo e independente para a efetiva concreção do direito do consumidor, assegurado inclusive a autodeterminação informativa na utilização de seus dados no mercado de consumo.

REFERENCIAS BIBLIOGRÁFICAS:

BAUMAN, Zygmunt. Vida para consumo: a transformação das pessoas em mercadoria. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2008.

BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Cornell University Press, 1992.

CARVALHO, Joatan Marcos. É possível a proteção de dados pessoais? *Revista Luso-Brasileira de Direito do Consumo* - Vol. VII, n. 25 março 2017, Curitiba: Bonijuris, 2017.

CASTELLS, Manuel. *A Galáxia da Internet. Reflexões sobre a internet, os negócios e a sociedade*. Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar Ed., 2003.

CASTELLS, Manuel. *A sociedade em rede.* São Paulo: Paz e Terra, 2016.

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

DONEDA, Danilo. Princípios da proteção de dados pessoais, p.369 a 384, *In Direito e Internet III*, org. Adalberto Simão Filho, Newton De Lucca e Cintia R.P. Lima, São Paulo: Quartier Latin, 2015.

MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais, *In* MARQUES, Claudia Lima e GSELL, Beate. *Novas Tendências do Direito do Consumidor*. RT: São Paulo, 2016.

[171] O art.23 do PL 5276 dispõe que o tratamento de dados pessoais pelas pessoas jurídicas de direito público referenciadas no parágrafo único do art. 1 da lei 12.527, deverá ser realizado para o atendimento de sua finalidade publica, na persecução de um interesse público, tendo por objetivo a execução de competência legais ou cumprimento de atribuição legal pelo serviço público.

MARTINS, Plinio Lacerda. Anotações ao Código de Proteção e Defesa do Consumidor. Rio de Janeiro: Rio de Janeiro. 2005.

PERLINGEIRO, Ricardo; DÍAZ, Ivonne; LIANI, Milena. Princípios sobre o direito de acesso à informação oficial na América Latina. *Revista de Investigações Constitucionais*, Curitiba, vol. 3, n. 2, p. 143-197, maio/ ago. 2016.

RODOTÁ, Stefano. *A vida na Sociedade de Vigilância. A privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008.

VERBICARO, Dennis e MARTINA, Ana Paula Pereira. contratação eletrônica de aplicativos virtuais no Brasil e a nova dimensão da privacidade do consumidor. *Revista de Direito do Consumidor*, São Paulo, n. 116, p. 369-392, 2018.

A RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DOS DADOS PESSOAIS

Dyana Ribeiro Camelo

INTRODUÇÃO

É notório o lépido avanço das tecnologicas, com ênfase na chamada internet, outrora denominada “Arpanet”, que acabou revolucionando o mundo e influenciou sobremaneira a forma como os indíviduos se relacionam. Nesse contexto, surgiu a necessidade de proteção os dados pessoais destes. Com o fim de tutelar e regular o tratamento dos dados pessoais, surgiu a Lei n° 13.709/2018, que embora não se limite apenas a esfera da internet, se dispõe a proteger os titulares em sua relação com os controladores e operadores, através de princípios e regras que orientam, limitam e estabelecem a responsabilização civil destes quando sua ação der ensejo a ocorrência de um dano, conforme as hipóteses previstas na referida Lei.

Com o desiderato de compreender como se dá a responsabilidade civil dos agentes de tratamentos de dados na Lei Geral de Proteção de Dados (LGPD), o presente artigo se dividiu em tópicos e subtópicos. A priori pretende-se analisar o rol normativo que antecedeu a LGPD, bem como entender o contexto em que essa Lei surgiu e o que a procedeu, de forma breve mas que permita compreender o que deu ensejo a sua elaboração.

Além disso, antes de adentrar na análise dos dispositivos da LGPD, faz-se imperioso compreender o instituto da responsabilidade civil, os elementos essenciais que a compõem e as suas espécies. A posteriori, após ser elencados algumas conceituações presentes na aludida Lei, far-se-á um estudo dos artigos 42 ao 45, de modo a compreender o que enseja a responsabilidade civil do controlador e operador, quais as excludentes de responsabilidade, bem como outros institutos tragos à voga pela aludida Lei. Com base nessas informações, poder-se-á vislumbrar a discussão doutrinária a respeito da natureza da responsabilidade civil da LGPD, se subjetiva, proativa ou objetiva.

O presente trabalho, portanto, possui como fim compreender o assunto e contribuir para a disseminação do tema dotado de grande relevância. Para isso, utilizar-se-á o método indutivo, e, tendo isso em vista, far-se-á pesquisa teórica e bibliográfica, como também a análise de dispositivos da Lei n° 13.709/2018, com vistas a alcançar o objetivo pretendido supramencionado.

BREVE CONTEXTO ACERCA DAS LEGISLAÇÃOES DE PROTEÇÃO DE DADOS PESSOAIS

1.1 Instrumentos Normativos que antecederam a Lei Geral de Proteção de Dados Pessoais

Com o surgimento da internet, a coleta e uso dos dados pessoais tornaram-se cada vez mais amiúde na vida dos indivíduos. Não obstante, o que deveria ser utilizado para a benesse dos indivíduos acabou permitindo a prática de diversos crimes, em razão da crença de que a internet é uma "terra sem lei" e, portanto, as práticas ilegais ficariam impunes. Faz-se mister acrescentar que a ausência de uma legislação específica sobre o tema acabou colaborando para esse ambiente promíscuo.
Diante desse contexto, vislumbrou-se a necessidade da criação de diretrizes mínimas para garantir uma maior segurança àqueles que cediam seus dados. Nesse sentido, é consentâneo falar à respeito do arcabouço legal que anteceu a Lei Geral de Proteção de Dados Pessoais (LGPD).

A Carta Magna de 1988 em seu artigo 5°, X, prevê a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (Brasil, 1988). Sob tal ótica, Stefano Rodatà (RODOTÀ, 2008, p. 129) entende o direito a privacidade como "precondição da cidadania na era eletrônica", não podendo ser confiada à lógica da autorregulação ou das atividades contratuais. Logo, possíveis abusos não podem ser admitidos, pois estaria-se invadindo a relação existente entre os indivíduos e o seu Estado.

A Constituição Federal foi procedida pelo Código Civil de 2002, que tutelou a vida privada da pessoa natural, além de conferir extrema relevância aos direitos da personalidade. No entanto, os sistemas normativos supramencionados não lograram êxito na proteção dos dados pessoais, principalmente no contexto de uma sociedade cada vez mais tecnológica.

Em 2014, diante dessas falhas regulatórias, foi promulgado o Marco Civil da Internet (Lei n°12.965/2014), a primeira legislação brasileira criada especificamente para disciplinar as múltiplas situações de direitos e deveres da internet. A legislação apresenta diversas garantias, princípios, direitos e deveres para a utilização da internet no ambiente nacional, deixando explícito em seu artigo 3° que o uso da mesma deveria se pautar no princípio da proteção da privacidade. (BRASIL, 2014).

Embora tenha trazido importantes diretrizes que orientaram a lei específica criada posteriormente, o Marco Civil da Internet ainda era incompleto e não tratava de forma tão eficiente a questão da proteção de dados pessoais, até porque, como preceituou Rebeca Garcia (2016, p. 163), "trata-se de um marco regulatório, ainda pendente de regulamentação e ainda com diversas questões em abertos." Nesse contexto, a Lei 13.709/2018 surgiu para justamente regulamentar de modo específico as atividades que envolvem o tratamento de dados pessoais.

A LEI GERAL DE PROTEÇÃO DADOS PESSOAIS

A Lei Geral de dados pessoais, n° 13.709, de autoria do Deputado Milton Monti, foi publicada a priori em 14 de agosto de 2018 com um *vacattio legis* longo para alguns dispositivos. Em 28 de dezembro de 2018 entraram em vigor os artigos referentes à Autoridade Nacional de Proteção de Dados e ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (BRASIL, 2018); e em 18 de setembro de 2020 os demais dipositivos.

A mencionada lei traz em seu corpo diretrizes, princípios e regras que estabelecem como se dará, no âmbito nacional, o tratamento dos dados pessoais, inferindo direitos e obrigações aos agentes de tratamento e aos titulares, com o objetivo de proteger os direitos fundamentais dos indivíduos e assim promover o livre desenvolvimento da personalidade da pessoa natural. Embora não se restrinja ao ambiente virtual, é notório que, em razão do veloz e alto número de processamento e transmissão de dados via internet, a LGPD será amplamente aplicada para regulamentar as relações existentes no espaço *online*.

> A Lei nº 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionadas ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionadas às pessoas (PINHEIRO, 2018, p. 15).

Por fim, há de se mencionar a Proposta de Emenda à Constituição n° 17/2019, que anseia conferir status constitucional à proteção de dados pessoais, inserindo-o no artigo 5° da Constituição Federal que abarca os direitos fundamentais. Conforme apontou Danilo Doneda (2011, p. 103), “a proteção de dados pessoais não se estrutura, no ordenamento brasileiro, a partir de um complexo normativo unitário”, sendo reconhecido, como supramencionado, por meio da interpretação dos direitos que preceituam a inviolabilidade da intimidade e da vida privada. De todo modo, o esforço demonstra a importância e o valor dado ao tema, reconhecendo a íntima e intrísica relação entre os dados e os seus titulares e os riscos que o envolvem, até porque, conforme o autor, “hoje em dia as pessoas são reconhecidas em diversos relacionamentos não de forma direta, mas mediante a representação de sua personalidade, fornecida pelos seus dados pessoais”. Logo, diante de uma correlação tão próxima entre dados pessoais e a própria identidade do indivíduo, faz-se mister repensar sobre a adequabilidade dos dados nos diplomas legais, principalmente na Constituição Federal.

Dado o exposto, é possível identificar a complexidade da questão referente aos dados pessoais que, por sua natureza, ensejou múltiplas dificuldades aos instrumentos normativos que pretenderam regulamentá-los. A LGPD certamente é um diploma necessário que surgiu para suprir lacunas existentes e proporcionar um ambiente mais transparente e seguro para os titulares dos dados pessoais.

RESPONSABILIDADE CIVIL

A responsabilidade civil, conforme as palavras de Carlos Roberto Gonçalves, "é um dever jurídico sucessivo[2] que surge para recompor o dano decorrente da violação de um dever jurídico originário[3]" (2019, n.p.). Nesse sentido, sempre que uma pessoa, natural ou jurídica, infringir uma norma, caberá à mesma arcar com as consequências desse ato, fato ou negócio danoso, isto é, incumbe-lhe o dever de indenizar a vítima do evento danoso.

O avanço tecnológico, o crescimento populacional e as relações cada vez mais vultosas e complexas dão azo a novos paradigmas sociais, o que acaba por obrigar que o instituto da responsabilidade civil se reinvente para abarcar as novas situações e conceder tutela aos indivíduos que por algum motivo são lesados em seus direitos, tornando possível a restauração do equilíbrio moral e patrimonial destes em razão de uma ação danosa de outro agente.

A responsabilidade civil está presente quando o devedor descumpre o que fora estabelecido em um contrato ou negócio jurídico, a chamada responsabilidade civil contratual, ou quando o indivíduo deixa de observar um dever geral, vigente na sociedade, conceituada como responsabilidade civil extracontratual (Tartuce, 2018, p. 47). Na LGPD, grande parte da responsabilidade civil dos agentes de tratamento é extracontratual, já que a referida lei institui diversos deveres de conduta, os quais, se descumpridos, ensejarão a responsabilidade do controlador e operador, sem necessariamente haver uma quebra no contrato ou na relação negocial propriamente dita do agente e o titular, todavia, nada impede que os agentes sejam responsabilizados contratualmente quando violarem alguma cláusula preestabelecida no contrato. No entanto, antes de abordar outras questões, faz-se imperioso conhecer os elementos da responsabilidade civil.

---

[2] Entendido como o resultado da violação do dever jurídico originário, que em suma institui a obrigação de indenizar o prejuízo (Gonçalves, 2019).[3] Que preceitua a proibição da violação de um dever jurídico (Gonçalves, 2019).

PRESSUPOSTOS DA RESPONSABILIDADE CIVIL

Com base no artigo 186[4] do Código Civil, identificam-se quatro pressupostos para a configuração da responsabilidade civil, conforme a doutrina tradicional: ação ou omissão; culpa ou dolo do agente; relação de causalidade e o dano efetivamente experimentado pela vítima.

A ação ou omissão diz respeito à conduta do agente, que de modo voluntário, negligente ou imprudente viola um ou múltiplos direitos e causa danos a outrem (Código Civil, 2002). A ação, representada pela conduta comissiva, se manifesta quando o indivíduo atua e lesiona direitos de terceiros, um exemplo seria um indivíduo que atropela seu semelhante. A omissão, por sua vez, diz respeito a conduta omissiva, e é punida porque o agente deveria agir mas se abstem e, em virtude disso, ocorre o evento danoso. Flávio Tartuce (2018, p. 171) pontua que a omissão é comprovada por meio da existência de um dever jurídico de evitar o dano e a demonstração efetiva de que o dano poderia ter sido evitado caso a conduta tivesse sido praticada.

A noção de culpa abarca o dolo e a culpa em sentido estrito. A culpa stricto sensu engloba a imprudência, entendida como uma falta de cuidado somada a uma ação; a negligência, que decorre de uma falta de cuidado somada a uma omissão; e a imperícia, que por sua vez constitui a ausência de técnicas para o desempenho de uma função (Tarturce, 2018, p. 176). O dolo, conforme preceitua Carlos Roberto Gonçalves, é a violação deliberada, consciente, intencional, do dever jurídico (2019, n.p.). Faz-se mister mencionar que, quando se trata da indenização, a culpa em sentido estrito e o dolo são tratados igualmente, não havendo distinções. Em suma, conforme Paula Grecco Bandeira:

> Busca-se perquirir os elementos psicológicos do agente que viola o dever de conduta, verificando-se se tinha a possibilidade de prever os resultados danosos de sua atuação (culpa) ou se agiu com intenção de prejudicar (dolo). Assim, a culpa é tratada como elemento subjetivo ou psicológico do ilícito, razão de um juízo moral de condenação do sujeito. Note-se, portanto, que a noção de culpa psicológica reúne dois elementos essenciais, a saber: (i) a violação de um dever preexistente, resultado da manifestação de vontade livre e consciente do agente; e (ii) a previsibilidade do resultado danoso, 'pressuposto lógico e psicológico de sua evitação'." (2008, p. 2).

---

4 "Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito." (BRASIL, 2002).

A relação de causalidade é conceituada por Gonçalves como “a relação de causa e efeito entre a ação ou omissão do agente e o dano verificado.” (2019, n.p.). Nesse interím, por estabelecer um vínculo entre vítima, agente e dano, o nexo de causalidade se faz indispensável para a configuração do dever de indenizar. Esse elemento é analisado de modo objetivo, e pode ser desconsiderado, permitindo a não responsabilização do agente, quando o dano for fruto de força maior, caso fortuito ou culpa exclusiva da vítima, já que a relação de causa e efeito entre o resultado danoso e a culpa do agente é afastada (VENOSA, 2013, p. 54).

O dano, que pode ser tanto material, moral, individual ou coletivo, é indispensável para a configuração da responsabilidade civil. Acrescenta-se que, para ser ressarcível, é necessário que o dano seja “atual”[5] e “certo”[6] (GONÇALVES, 2019, n.p.). Conforme Venosa, quando há prejuízo no patrimônio da vítima, tem-se o dano material e, quando há afetação do ânimo moral e psíquico da vítima, vislumbra-se o dano moral (2013, p. 47). Segundo Tartuce, os danos morais coletivos são aqueles que atingem direitos individuais e homogêneos de vítimas determinadas ou determináveis ao mesmo tempo (2018, p. 337).

RESPONSABILIDADE CIVIL OBJETIVA E SUBJETIVA

O Brasil filiou-se à corrente dualista e, por consequência, compreende em seu Código Civil tanto a responsabilidade objetiva quanto a subjetiva. Nesta, para a responsabilidade se materializar, é necessário que o agente que praticara um ato danoso tenha agido com culpa, àquela, por sua vez, prescinde de culpa. É possível vislumbrar ambas as responsabilidades nos artigos 186 e no parágrafo único do 927[7] do Código Civil, respectivamente.

A responsabilidade civil objetiva, como já dito, não precisa do elemento culpa, satisfazendo- se apenas com a existência da conduta voluntária, do dano e do nexo de causalidade. Seu fundamento é a lei, quando esta é explícita, e o risco. Nesse sentido, faz-se mister abordar a teoria do risco, mais especificamente a teoria do risco criado, que preceitua que se uma atividade criar um risco de dano para terceiros, o responsável pela atividade é obrigado a

---

[5] Será atual o dano que já existia no momento da pretensão de ajuizamento da ação de responsabilidade. (GONÇALVES, 2019).

[6] Certo é o dano concreto (GONÇALVES, 2019).

[7] “Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, é obrigado a repará-lo.
Parágrafo único: Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem”. (BRASIL, 2002).

reparar o dano se este se concretizar, ainda que inexista culpa em sua conduta. O fundamento desta teoria se ampara na noção do exercício de atividade perigosa, pois conforme essa ótica poder-se-ia conceder maior proteção as vítimas que sofressem algum dano.

A responsabilidade subjetiva, por sua vez, se configura quando há a presença da ação ou omissão, da culpa, do dano e do nexo causal. Seu fundamento é a lei e o ato ilícito, este último conceituado como "uma conduta culposa que contraria o Direito e causa dano a outrem" (GONÇALVES, 2019, n.p.).

CONCEITOS E A RESPONSABILIDADE CIVIL NA LGPD

1.1. Conceituação: Os agentes de tratamento e os dados pessoais

A lei geral de proteção de dados pessoais trouxe em alguns de seus dispositivos, sobretudo nos primeiros, algumas conceituações para a melhor compreensão das demais regras. Nesse diapasão, antes de analisarmos os dispositivos que dispõem sobre a responsabilidade civil na LGPD, faz-se oportuno mencionar algumas dessas conceituações.

No artigo 5°, inciso IX, a Lei n° 13.709 preceitua:

> Art. 5º Para os fins desta Lei, considera-se:
>
> (...)
>
> V – titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
>
> IX - agentes de tratamento: o controlador e o operador;
>
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Logo, constata-se que é do controlador que emanam as ordens à respeito de como se dará o tratamento dos dados, instituindo políticas e parâmetros para que o operador, que se subordina a ele, execute concretamente aquilo que lhe fora ordenado.

Além disso, é oportuno apresentar outra conceituação referente aos dados pessoais, que é justamente o substrato da LGPD:

Art. 5º Para os fins desta Lei, considera-se:

- dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

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

- dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Diante da definição concedida pela lei, temos que se identificada, ou se existir a possibilidade de ser identificada a pessoa natural, a informação vinculada a ela é tida como um dado pessoal. Nesse interím, cookies de internet, email pessoal e até corporativo etc, que permitem a identificação de uma pessoa natural, enquadra-se no inciso supracitado.

A RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO

A Lei Geral de Proteção de Dados Pessoais trouxe uma Seção própria para tratar sobre a responsabilidade dos agentes de tratamento e o ressarcimento de danos causados aos titulares de dados, disciplinado entre o art. 42 e o 45 da Lei.

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
>
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
>
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
>
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso (BRASIL, 2018).

Com base no dispositivo retromencionado, depreende-se que a reparação pode ser feita em relação a um indivíduo apenas ou a uma coletividade, e não se concentra apenas no plano patrimonial. Além disso, do *caput* é possível extrair que a responsabilidade se concentra na figura do controlador ou operador. Nesse interím, dá-se ênfae na conjunção alternativa "ou", o que significa que embora o operador se subordine ao controlador e as suas respectivas ordens, cabe a ele realizar o tratamento de dados em consonância com a Lei e também tomar as medidas necessárias para que haja a segurança desses dados, principalmente porque a atividade exercida contém diversos riscos, e, na menor violação do estatuto do presente estudo, caberá a ele a o dever de reparar.

Todavia, o §1° do artigo em apreço traz em seus incisos exceções em relação a alternância presente no caput, tonando solidária a responsabilidade do operador e controlador quando as obrigações previstas na LGPD não forem observadas ou quando o controlador remeter ao operador uma ordem lícita e ele não a obedecer. Nesse caso, a submissão deste para com àquele é desconsiderada e ele equipara-se ao controlador.

Ademais, é indubitável que o tratamento de dados se dá através de uma cadeia produtiva, e que não necessariamente o cargo de operador e controlador são exercidos por pessoas singulares. Sob tal ótica, é possível que em certas situações exista uma multiplicidade de agentes, coexistindo mais de um controlador, por exemplo. Diante desse caso, o inciso II, §1°, do artigo 42, estipula que serão solidários todos os controlados envolvidos diretamente no tratamento que ocasionar danos ao titular dos dados. Não obstante, em razão da adoção desse instituto que permite que a obrigação seja cobrada de um ou de todos os controladores, aquele que cumpri-la não fica prejudicado no seu direito de ajuizar ação de regresso contra os demais responsáveis, "na medida de sua participação no evento danoso", observando-se a prevalência do princípio da proporcionalidade.[8]

Embora não esteja expressa a responsabilidade do encarregado[9], por participar da cadeia de produção, o professor Walter Aranha Capenema entende que, quando essa função for exercida por pessoa destacada do operador e controlador em uma relação consumerista, incidirá sobre ele também a responsabilidade solidária pelo dano causado (2020, p. 163). Acrescenta-se que a priori, por exercer uma função meramente consultativa, não recai sobre ele qualquer responsabilidade, todavia, em casos excepcionais, se tiver agido com dolo no intuito de

---

[8] Art. 42, §4°, da Lei Geral de Proteção de Dados.

[9] Art. 5°, VII, LGPD. "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);

induzir o controlador a adotar atividade contrária as regras do LGPD, restará a ele o dever de reparar o dano causado.

Insta dizer, ainda, que a adoção da solidariedade para esses casos se deu com o desiderato de “assegurar a efetiva indenização ao titular dos dados”, já que ao expandir o rol de responsáveis, o lesado poderá escolher àquele que apresentar maiores condições de reparar o dano sofrido. Não obstante, deve-se ter em mente que ambos os incisos supramencionados não instituem regras absolutas, pois se existente os “casos de exclusão previstos no art. 43” da LGPD, deixá-los-á de aplicá-los.

No que tange a produção de prova, embora em regra incumba ao autor o ônus probatório quanto aos fatos alegados, fora adotada pela legislação em apreço a teoria da distribuição dinâmica do ônus da prova, que admite a sua inversão de acordo com as peculiaridades do caso concreto, do direito alegado e das condições das partes envolvidas.A escolha dessa teoria pelo legislador explicita o seu reconhecimento pela relação de desigualdade existente entre o titular dos dados e os agentes de tratamento, já que em razão de seu conhecimento técnico e do seu acesso a todas as informações referentes a atividade, acaba se tornando mais fácil para estes a produção de provas. Destarte, o §2° estipula as situações que o juiz, a seu critério, poderá determinar essa inversão a favor do titular dos dados, quais são: a) quando for verossímil a alegação da ocorrência de dano; b) se o titular não gozar de recursos suficientes para a elaboração de prova e; c) mesmo que o titular tenha possibilidades de arcar com os custos da produção da prova, recairá sobre si uma excessiva onerosidade. A aludida teoria encontra-se presente no artigo 373 do Código de Processo Civil e também no artigo 6°, VII, do CDC, nesse último caso, exigindo menos requisitos.

Em relação às hipóteses de exclusão da responsabilidade civil dos agentes, dispõe a LGPD:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I – que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
>
> – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. BRASIL, 2018).

A reparação do dano deverá ser feita pelo agente que realizou o tratamento de dados pessoais. Logo, se houve um tratamento de dados, mas o agente não tem qualquer vínculo com esse tratamento que lhe fora atribuído, não há que se falar em responsabilidade, pois inexiste um

pressuposto fundamental para a sua configuração: o nexo causal, já visto nesse trabalho. Essa hipótese prevista no inciso I do artigo 43 visa proteger o agente que pode ser acusado indevidamente, o que não é tão incomum em razão da celeridade da vida contemporânea, à exemplo do fato de que as pessoas possuem o costume de usar os mesmos dados em diversas plataformas, logo, na ocorrência de algum vazamento, ela pode acabar ajuizando ação contra um agente que nada teve a ver com o dano ocorrido.

Ao revés da situação prevista no inciso I do referido artigo, no inciso II há a situação em que o agente de fato realizou o tratamento de dados que lhe é atribuído, o qual resultou em um evento danoso, mas, ainda sim, ele não será responsabilizado, porque em momento algum inobservou as normas determinadas pela legislação de dados e pala Autoridade Nacional de Proteção de Dados. Nesse caso, embora o titular se sinta constrangido e considere errada a tomada de decisão do agente, se este demonstrar que agiu com legítimo interesse[10], por exemplo, estará agindo em consonância com a lei. Um outro exemplo apresentado pelo professor Capanema, é quando há uma "decisão automatizada, baseada em critérios transparentes, informados (presentes em termos de uso) e sem viés, que negue um empréstimo a um possível consumidor" (2020, p 167), vislumbrando-se a observância das regras da LGPD.

A última hipótese que exime de responsabilidade o agente de tratamento é quando o dano ocorrido é produto da culpa exclusiva do titular ou de um terceiro, conforme inciso III do artigo 43. Essa situação ocorre quando o titular age de modo descuidado ou subestima os riscos da adoção de determinada medida, que podem fugir do controle dos agentes de dados. Para exemplificar, temos os chamados "sites espelhados", que apresentam designer idêntico ou muito semelhante ao do site oficial. Nesse caso, se um indivíduo disponibilizar seus dados ao site falso acreditando estar no site oficial, e posteriormente o estelionatário utilizar indevidamente os referidos dados pessoais, não caberá nenhuma responsabilidade aos agentes do verdadeiro site, porque inexiste relação de causalidade, uma vez que fora o fraudador que o induziu a erro. Do mesmo modo ocorre quando um cidadão recebe um email da Receita Federal requerendo seus dados e, sem antes analisar se o email é verídico, os envia.

---

[10] Art. 7° O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
(...)
IX - 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; o

Na ocorrência de algum dano, não tendo sido o Órgão o verdadeiro remetente, em nada será responsabilizado, já que não deu azo à lesão.

Em todas as hipóteses do supratranscrito artigo, com base no artigo 42, §2°, da LGPD, haverá a inversão do ônus da prova, cabendo aos agentes de processamento provarem que se enquadram em alguma das situações que permitem a exclusão de sua responsabilidade, vistas nos incisos do artigo 43. Tendo em vista o princípio de prestação de contas, o agente poderá fazer a sua prova pelos documentos que é obrigado a registrar.[11]

Em relação a irregularidade do tratamento de dados, a LGPD prevê:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
>
> – o modo pelo qual é realizado;
>
> – O resultado e os riscos que razoavelmente dele se esperam;
>
> – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
>
> Parágrafo úncio. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

A legislação em estudo apresenta duas hipóteses em que o tratamento de dados pessoais será considerado irregular: a) quando houver descumprimento das normas da LGPD e; b) quando o titular tiver suas expectativas frustradas em relação ao procedimento, já que se está diante de uma relação contratual em que se valoriza a transparência e a boa-fé. Embora à primeira vista a segunda hipótese possa parecer subjetiva, o legislador preocupou-se em lhe dar concretude, listando nos incisos do artigo 44 o que se deve levar em conta no momento de interpretá-la. Dentre as circunstâncias relevantes que devem ser levadas em consideração, o artigo supratranscrido se concentra no modo como o tratamento é realizado, nos riscos e resultados que razoavelmente dele se esperam e, também, no estado da técnica à época em que o tratamento fora realizado.

---

[11] Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Em relação ao inciso III, cabe trazer à tona uma discussão iniciada pelo professor Capanema. O referido discente disserta à respeito da vulneralibidade[12], afirmando que elas são documentadas e catalogadas como Common Vulnerabilities and Exposures – CVE quando descobertas, permitindo, assim, que àqueles que cuidam da "segurança da informação das empresas e órgãos públicos adotem medidas técnicas para prevenir tais incidentes" (2020, pág 167). O professor entende que, se a vulnerabilidade não for documentada, não seria admissível a responsabilização civil do agente, porque se desonhecida, não há como se exigir o dever de segurança, porque estaria-se desconsiderando o estado da técnica existente à época.

Além disso, o parágrafo único do aludido artigo responsabiliza os agentes de tratamento quando houver danos decorrentes da violação da segurança dos dados em razão da não adoção, pelo controlador e operador, das medidas de segurança presentes no artigo 46[13]. Esse dispositivo decorre do Princípio da Segurança, previsto no artigo 6°, VII, da Lei Geral de Proteção de Dados[14].

Recentemente, o Tribunal de Justiça do Distrito Federal e dos Territórios recebeu uma ação civil pública, com pedido de tutela de urgência, pelo Ministério Público (MP), requerendo que o portal Mercado Livre, que estava comercializando de forma maciça os dados pessoais de brasileiros presentes no seu banco de dados pelo valor de R$ 500,00 (quinhentos reais), suspendesse o respectivo anúncio e fornecimento dos dados cadastrais dos usuários da plataforma[15]. O Magistrado acolheu o pedido do MP, e motivou a sua decisão com base no princípio constitucional do sigilo de dados, insculpido no artigo 5°, XII, da Constituição Federal; como também no princípio da privacidade previsto no artigo 2°, I, da LGPD e, o que

---

12 Matéria pertencente à tecnologica, conceituada como a "condição que, quando explorada por um atacante, pode resultar em uma violação de segurança". (HOPERS; STEDING-JESSEN, 2014).

13 Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
§1° A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
§2° As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

14 Art. 6°, VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

15 Pje: 0733785-39.2020.807.0001.

nos interessa, no artigo 44 dessa lei, pois como o Mercado Livre não teve a anuência dos titulares dos dados para fornecê-los, acabou, portanto, fazendo um tratamento irregular ao não observar o artigo 7°, I, da referida Lei.

Além, disso, A LGPD dispõe no seu artigo subsequente:

> Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

Com base no aludido artigo, se estivermos diante de uma relação de consumo[16], aplicar-se-á o Código de Defesa do Consumidor, pois, além de favorecer o consumidor, ele se presta melhor ao papel de tutelar os direitos dele frente a superioridade econômica e informacional dos agentes da atividade.

Na seara desse tema, observa-se a compatibilidade entre a LGPD e o Código de Defesa do Consumidor, pois assim como aquele, este também prevê a solidariedade dos agentes em caso de produção de danos ao consumidor, como também a inversão do ônus da prova e o acesso a informações adequadas e claras.

Logo, nota-se a interdisciplinariedade entre a Legislação de dados com os diplomas legais já vigentes, reservando para si as matérias que lhe são afetas e delegando aos outros ramos do Direito aquilo que por eles receberão um cuidado mais específico, o que acaba tornando possível uma reparação mais efetiva e justa.

O DANO E A DEFINIÇÃO DO QUANTUM INDENIZATÓRIO

Conforme Cavalieri, o dano é a "subtração ou diminuição de um bem jurídico, qualquer que seja a sua natureza. (...) Dano é lesão de um bem jurídico (2005, pág. 95-96).

Nesse interím, é possível vislumbrar o dano como um produto da ocorrência de uma violação de dados pessoais, por exemplo. Nessa situação, temos como indispensável a existência de um dano para que seja admitida a indenização, pois, se a vítima nada sofreu, não há o que se reparar, caso contrário estaria-se diante de um enriquecimento ilícito desta. Nesse diapasão, quando observamos o nosso ordenamento jurídico, temos no artigo 944 do Código Civil que a "indenização mede-se pela extensão do dano". Sob tal ótica, o professor Capanema dispõe

---

16 Conceituada como "a relação que o direito do consumidor estabelece entre o consumidor e o fornecedor, conferindo ao primeiro um poder e ao segundo um vínculo correspondente, tendo como objeto um produto ou serviço" (DONATO, 1993, pág. 70).

que para se analisar a extensão do dano na seara da proteção de dados, deve-se levar em consideração os seguintes critérios: a) quantos dados pessoais foram afetados; b) qual a natureza dos dados pessoais violados, pois se for sensível, por exemplo, a indenização será maior; c) se a conduta do agente é reincidente; d) se o agente se omite ao adotar as medidas de segurança com vistas a diminuir o dano ou em atender o disposto pela Autoridade Nacional de Proteção de Dados; e) se o usuário é notificado da ocorrência do incidente e; f) se terceiros utilizaram os dados pessoais vazados. (2020, pág. 168).

Desse modo, será possível estipular-se uma indenização mais justa e coerente, de modo a reparar a lesão sofrida pela vítima em razão da violação de seus dados pessoais.

A RESPONSABILIDADE DOS AGENTES: OBJETIVA OU SUBJETIVA?

Já foi visto no presente trabalho o conceito de responsabilidade objetiva e subjetiva, e o que surge à tona nesse momento é a discussão a respeito da natureza da responsabilidade civil dos agentes de tratamento de dados, se objetiva ou subjetiva, já que a LGPD não expressa em seus dispositivos qual a forma adotada, demandando, portanto, uma tarefa dedutiva.

Gisela Sampaio e Rose Meireles entendem que a LGPD se filiou a teoria subjetiva, isto é, a culpa do agente no momento de sua conduta que resultou no evento danoso é indispensável. As referidas autoras defendem seu posicionamento com base: no *caput* do artigo 44, que responsabiliza o agente quando ele não fornece a segurança que o titular esperava em relação ao tratamento de dados e também quando ele inobserva a legislação de proteção de dados; e no *caput* do artigo 42, que prevê a responsabilização do controlador e operador quando eles violarem a LGPD.

Além disso, Sampaio e Meireles indicam que o Capítulo VI da Lei Geral de Proteção de Dados, que se concentra na indicação da conduta a ser seguida pelos agentes de tratamento de dados para “a segurança, sigilo, boas práticas e governança de dados” seria também um indício de que a LGPD aderiu a responsabilidade subjetiva. Outrossim, as autoras pontuam que o inciso II, do artigo 43 da LGPD, se assemelha as hipóteses de responsabilidade civil subjetiva ao dispor que, embora o agente contribua para a ocorrência do dano, se ele não violar a legislação, não há que se falar em responsabilidade. Isso porque elas entendem que a violação da lei seria um elemento subjetivo do dever de indenizar e também seria uma prova da conduta culposa do agente que trata dos dados pessoais. Logo, se o agente não inobsersou a legislação de proteção de dados e ainda sim ocorreu um dano, sua conduta não fora culposa e, portanto, ele não será responsabilizado civilmente.

Aliás, faz-se mister mencionar a posição de João Quinelato e Maria Celina Bodin de Moraes, que defendem que a LGPD adotou a teoria ativa ou proativa da responsabilidade civil. Essa teoria institui a necessidade dos agentes de tratamento sempre agirem com o fito de evitar a ocorrência de danos, surgindo o dever de indenizar como uma medida excepcional. Nesse sentido, a responsabilidade civil sendo vista de um ponto positivo, enseja a tutela proativa, ou seja, o tratamento dos dados pessoais deve ser feito de modo transparente, de modo que o titular tenha conhecimento de seu processo, finalidade e a destinação dos referidos dados. Nesse interím, é imperioso que os agentes tomem medidas rigorosas para que a promoção dos dados dos titulares sejam protegidos de forma realmente eficaz, já que entendem que os dados constituem conteúdo do direito à privacidade. Quinelato e Moraes apontam que a responsabilidade proativa encontra-se no art. 6°, X, da LGPD, que aborda o princípio da responsabilização e prestação de contas e obriga o controlador e operador a demonstrar todas as medidas adotadas com vistas a cumprir os dispositivos presentes da referida Lei, inclusive a proporção de sua eficácia.

Danilo Doneada e Laura Mendes, ao revés, entendem ter a LGPD adotado a responsabilidade objetiva, com base na teoria do risco. Isso porque os autores indicam que a atividade exercida pelos agentes de tratamento possui um risco intrínseco, já que há um risco eminente de dano na ocorrência de violação dos dados pessoais, considerados personalíssimos e fundamentais. Doneda e Mendes calcam seu posicionamento no artigo 6, III, que dispõe sobre a obrigatoriedade da utilização dos dados na medida do necessário, se limitando àqueles que são fundamentais à finalidade pretendida, sem excessos. Diante disso, os autores afirmam que o legislador pretendeu diminuir os riscos de dano, uma vez que já se está diante de uma atividade dotada de grande potencial para causar danos.

Outrossim, Danilo e Laura indicam que o princípio da prestação de contas explicita a necessidade dos agentes serem claros, sinceros e transparentes quando forem informar os titulares acerca do tratamento dos dados, devendo estes serem comunicados sobre a pretensão da adoção de qualquer medida pelos agentes. Dessa obrigação surge também o dever dos agentes de prestarem contas, expondo em um relatório[17] todas as medidas que foram e estão sendo tomadas, para ser possível a análise de compatibilização ou não com a legislação. O termo “mitigaçao de risco” presente no artigo 5°, VII, da LGPD, inclusive, conforme os autores, é um modo de evidenciar que o agente tem conhecimento prévio da capacidade de

[17] É o chamado relatório de impacto à proteção de dados pessoais, que nada mais é do que a “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.” (Art. 5°, VII, LGPD).

danos de determinada decisão, e, em razão disso, deve buscar evitá-los, exercendo, portanto, uma gestão dos riscos inerentes à atividade.

Além disso, para complementar, os referidos autores também se baseiam no artigo 44 da LGPD, que trata do tratamento irregular dos dados pessoais, como já fora visto. No entanto, eles suscitam uma questão no que tange a redação do aludido artigo, pois ele, diferente do artigo 42 que institui o dever de indenizar "em razão do exercício de atividade de tratamento de dados pessoais", impõe que a devida indenização seja feita em razão da "violação da segurança dos dados". Todavia, eles entendem que os danos resultados de um incidente de segurança estão relacionados ao risco intrísico à atividade desenvolvida pelos agentes. Logo, dispõem que os riscos são inerentes à atividade, enquadrando-o na hipótese de fortuito interno, que cria óbices a não responsabilização dos agentes de tratamento e a instituição da indenização devida.

Em suma, para Doneda e Mendes a responbilidade dos agentes de tratamento prescinde de culpa, logo, em caso de produção de danos, eles deverão indenizar os titulares dos dados. Os autores instituem que a responsabilidade na LGPD é objetiva, calcados na teoria do risco, pois entendem que o tratamento de dados é uma atividade que possui, de modo intríseco, riscos em relação aos direitos dos titulares e, por isso, não se faz necessário que o titular comprove a conduta culposa do agente, pois, havendo dano, surge daí o dever de reparação.

Diante das duas correntes já mencionadas, entendemos que a LGPD aderiu a responsabilidade objetiva, sob o fundamento da teoria do risco criado, conceituado por Facchini Neto como aquela que é:

> "Consequência inafastável da atividade em geral. (...) Sua aplicação não mais supõe uma atividade empresarial, a exploração de uma indústria ou de um comércio, ligando-se, ao contrário, a qualquer ato do homem que seja potencialmente danoso à esfera jurídica de seus semelhantes. Concretizando-se tal potencialidade, surgiria a obrigação de indenizar." (2010, p. 159).

Logo, tem-se que algumas atividades, em decorrência de sua natureza ou dos instrumentos utilizados, submetem o homem a diversos tipos de riscos e, em razão disso, faz surgir a obrigação de reparar os resultados advindos da respectiva atividade. Nesse diapasão, independentemente de imprudência, negligência ou imprudência, o agente que exerce uma atividade iminentemente arriscada deve ser responsabilizado e arcar com os danos decorrentes dela.

Adotamos tal posicionamento baseando-se nos pontos apresentados por Doneda e Mendes, já que de fato o legislador instituiu a necessidade da feitura de um "relatório de impacto", para analisar os processos tendenciosos a causar danos, e de antemão buscar mitigá-los. Além disso, também houve a previsão dos princípios da segurança e da prevenção, que demonstram o reconhecimento dos riscos inerentes à atividade, buscando, assim, evitá-los ao máximo. Outrossim, há admissão da teoria da distribuição dinâmica do ônus da prova, que é mais um sinal de que a atividade é demasiadamente complexa, guardando em si um risco eminente, logo, não seria coerente incubir à vítima o dever de provar a culpa do agente para que seu dano fosse reparado. Alias, nesse interím, vislumbra-se uma semelhança entre a redação do Código do Consumidor[18] e a da Lei Geral de Proteção de Dados e, sabendo que aquele se filiou à responsabilidade objetiva, seria mais um motivo para se presumir que o legislador desejou atribuir à LGPD o mesmo instituto. Desse modo, entendemos que não é necessário a existência de culpa para que os agentes de tratamento sejam responsabilizados, em razão da teoria do risco criado.

CONCLUSÕES

A Lei Geral de Proteção de Dados Pessoais foi um marco à legislação brasileira ao estabelecer diretrizes, regras e princípios no que tange ao tratamento de dados pessoais, regulando-o. Destarte, viu-se que outros diplomas legais antecederam a elaboração e publicação da referida Lei, tais como a Constituição Federal, o Código Civil e o Marco Civil da Internet, no entanto, por não serem criados com o fito de regular o tema em apreço, apresentavam diversas lacunas e não lograram êxito nesse ponto. Mencionou-se, ainda, a pretensão de dar status constitucional à proteção de dados pessoais, inserindo-o no rol do art. 5° da Constituição Federal, em razão da intríseca relação entre os dados pessoais e a própria identidade do indivíduo.

A responsabilidade civil, que surge sempre quando uma pessoa infringe uma norma, estabelece o dever do autor do evento danoso de repará-lo por meio de uma indenização destinada à vítima. Nesse interím, viu-se que a responsabilidade civil divide-se em contratual e extracontratual, e que ambas podem ser impostas contra os agentes de tratamento, a depender do fato que deu causa ao dano, se decorrente da inobservância da LGPD ou da

---

[18] Art. 6°, CDC. "São direitos básicos do consumidor:
(...)
VIII – a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências." (BRASIL, 1990).

quebra do contrato existente entre o agente e o titular. Aliás, dentro do tema de responsabilidade civil, foi apresentado os pressupostos essenciais para a configuração desta, os quais são: ação ou omisão; relação de causalidade, o dano e a culpa ou dolo do agente, sendo que este último requisito só se faz necessário na responsabilidade subjetiva, uma vez que a responsabilidade objetiva prescinde de culpa lato sensu.

Além disso, sabendo quem são os titulares, os agentes de tratamentos e os três tipos de dado pessoal conceituados na Lei, foi possível vislumbrar como se dá a responsabilização no âmbito civil dos agentes de tratamento, por meio da análise dos artigos 42 ao 45 da LGPD, que em seus dispositivos apresentam quais os motivos que ensejam a responsabilidade do controlador e operador, as hipóteses de solidariedade, de inversão do ônus da prova e também as excludentes que eximem os agentes de reparar o dano decorrente da violação dos dados pessoais de um ou mais titulares. Além disso, viu-se também quando o tratamento de dados pessoais se dá de forma irregular, e ainda, como os juízes têm decidido e os parâmetros que podem ser observados no momento de se estabelecer o quantum indenizatório.

Por fim, veio a tona a discussão doutrinária acerca da responsabilidade dos agentes de tratamentos, se objetiva ou subjetiva. Gisela Sampaio e Rose Meireles entendem que a LGPD se filiou a teoria subjetiva, com base no art. 42, 44 e outros presentes na aludida Lei. Logo, para essas autoras, a aferição de culpa é indispensável para que seja possível responsabilizar o agente de tratamento que deu causa a um dano. João Quinelato e Maria Celina, por outro lado, acreditam que a LGPD se filiou a teoria proativa da responsabilidade civil, baseando-se na necessidade instituída pela Lei de proteger os dados pessoais através de medidas eficazes que deverão ser explicitadas, em razão do art. 6°, X. Por sua vez, Danilo Doneda e Laura Mendes entendem ter a LGPD adotado a responsabilidade objetiva, com base na teoria do risco, isso porque a atividade exercida pelos agentes de tratamento um risco intrínseco que torna a ocorrência de dano um risco eminente. Os referidos autores calcam seu posicionamento no art. 6°, III, art. 5°, VII, 42 e 44, desse modo, por seguirem essa corrente, entendem que para que recaia sobre o controlador e o operador a responsabilidade civil, não é necessário a existência de culpa em suas ações.

Com base no exposto, entendemos que a responsabilidade civil dos agentes de tratamento é objetiva, já que por diversos motivos, muitos apresentados por Doneda e Mendes, como também vistos no presente trabalho, o legislador preocupou-se em instituir diversos princípios e regras a serem seguidas pelos controladores, já antevendo que em razão da natureza da

atividade, que é de risco intríseco e eminente, surgiriam muitos danos decorrentes da violação dos dados pessoais, e, com tal posicionamento, poderia mitigá-los.

REFERÊNCIAS:

BANDEIRA, Paula Greco. **A Evolução do Conceito de Culpa e o Artigo 944 do Código Civil**. Revista da EMERJ, [s. l.], v. 11, n. 42, 2008. Disponível em: http://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista42/Revista42_227.pdf. Acesso em: 2 de novembro de 2020.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF: Senado, 1988.

Lei n° 10.406, de 10 de janeiro de 2002. Institui o **Código Civil**. Diário Oficial da União: Brasília, DF.

_____ Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. [S. l.], 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 01 de novembro de 2020.

_____ Lei n°. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais** (LGPD). (Redação dada pela Lei n° 13. 853, de 2019). [S.I.], 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 de novembro de 2020.

CAPANEMA, Walter Aranha. **A responsabilidade civil na Lei Geral de Proteção de Dados**. Direito digital e proteção de dados pessoais. São Paulo. 2020.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. Malheiros Editores, 2005.

DONATO, Maria Antonieta Zanardo. **Proteção ao consumidor: conceito e extensão**. São Paulo: Revista dos Tribunais, 1993.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 2011.

FACCHINI NETO, Eugênio. **Da responsabilidade civil no novo Código**. 2010.

GARCIA, Rebeca. **Marco Civil da Internet no Brasil: repercussões e perspectivas**. Revista dos Tribunais, [s. l.], v. 964, 16 fev. 2017. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.964.06.PDF. Acesso em: 02 de novembro de 2020.

GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. Saraiva Educação SA, 2019.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. **Término do tratamento de dados**. IN: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. Lei Geral de Proteção de Dados Pessoais. Editora RT: São Paulo, 2019.

HOPERS, Cristine; STEDING-JESSEN, Klaus. **Fundamentos de Segurança da Informação**. [S.L.]: Escola de Governança da Internet no Brasil. 2014. Disponível em: https: //bit.ly/2unOasd. Acesso em: 05 de novembro de 2020.

MENDES, Laura Schertel; DONEDA, D. **Comentário à nova Lei de Proteção de Dados (Lei 13. 709/2018), o novo paradigma da proteção de dados no Brasil**. REVISTA DE DIREITO DO CONSUMIDOR, v. 120, 2018.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. **Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD**. IN: Cadernos Adenauer, volume 3, 2019.

PINHEIRO, P. P. **Proteção de Dados Pessoais: Comentários à Lei nº 13.709/2018**. 1. ed. São Paulo: Saraiva Educação, 2018.

RODOTÀ, Stefano. **A vida na sociedade de vigilância – a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

TARTUCE, Flavio. **Manual de Responsabilidade Civil**. Rio de Janeiro: Forense, 2018. V. único.

VENOSA, Silvio de Salvo. **Direito Civil: Responsabilidade civil**. 13. ed. São Paulo: Atlas, 2013. v. 4.

APLICAÇÃO E CONCEITO DA LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE DAS DISPOSIÇÕES PRELIMINARES

Giovanna Corrêa Kiuchi

Luiz Augusto Barcelos Inácio

Resumo: O presente artigo pretende explicar o porquê da Lei Geral de Proteção de Dados integrar o ordenamento jurídico do Brasil, por meio da exposições de problemas correlacionados ao tratamento de dados pessoais. Pretende-se examinar os seis artigos iniciais da referida Lei, de modo a apresentar as suas hipóteses de aplicação e comentar os conceitos nela expostos.

Palavras-chave: Lei Geral de Proteção de Dados, Tratamento de dados e Dados Pessoais.

INTRODUÇÃO

Com o advento da Lei Geral de Proteção de Dados, o Direito Privado sofreu alterações expressivas, posto que as atividades desempenhadas, tanto no ambiente virtual quanto físico, correlacionadas ao tratamento de dados pessoais terão de observar o disposto nesta Lei. Caso contrário, sanções expressivas hão de ser aplicadas às pessoas jurídicas e físicas que descumpram os seus dispositivos.

Diante disso, caberá à Autoridade Nacional de Proteção de Dados (ANPD) fiscalizar e aplicar as referidas sanções, que serão traduzidas em advertências ou multas de até 2% do faturamento total da empresa.

Por conseguinte, de maneira a compreender a razão do bem tutela na referida Lei se apresentar tão relevante para o direito brasileiro, visto que as penalidades previstas são significativas, faz-se necessário que sejam traçados alguns pontos na esfera social, jurídica e política que justifiquem a existência da LGPD.

Acrescenta-se, que as hipóteses de aplicação da Lei e os seus conceitos também serão abordados, uma vez que investigados os motivos estruturais para a publicação da LGPD se apresenta elementar o estudo das circunstâncias em que ela será empregada. À vista disso, tratar-se-á, também, dos conceitos apresentados nas Disposições Preliminares da Lei para que a exposição seja satisfeita. Mediante o exposto, nas seguintes páginas serão comentados e contextualizados os artigos 1° ao 6°, de modo a contribuir com o entendimento dessa Lei tão

importante e debatida na sociedade brasileira, que terá projeções, até mesmo, para fora do território nacional.

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS DENTRO DO ORDENAMENTO JURÍDICO BRASILEIRO

De início, a Lei aqui referenciada normalizara a respeito do tratamento de dados pessoais da pessoa natural, conforme disposto em seu primeiro artigo. Vale ressaltar, no entanto, que a realidade contemporânea é marcada por uma explosão de leis, um verdadeiro Big Bang Legislativo nas palavras de Ricardo Lorenzetti. Nesse sentido, realmente precisamos da Lei Geral de Proteção de Dados em nosso ordenamento jurídico? As leis e os códigos que a precedem já não seriam suficientes para a tutela dos bens jurídicos nela elencados?

Diante do exposto, faz-se fundamental uma rápida explanação da Lei n° 12.965/2014, do Código de Defesa do Consumidor e da Lei do Cadastro Positivo, na medida em que nelas já estariam manifestados alguns dispositivos correlacionados à privacidade e dados pessoais, sendo possível, portanto, uma associação à LGPD.

Reconhecida como a Lei que inaugurou uma norma específica para os direitos e garantias dos cidadãos na internet (Bioni, 2019, p. 186), a Lei do Marco Civil da Internet abarcará em seu artigo 3°, especificamente nos incisos II e III, que a disciplina do uso da internet no Brasil possui como princípio a proteção da privacidade e a proteção dos dados pessoais. Isto posto, nota-se uma interseção com o conteúdo da LGPD, no entanto, esta não será aplicada unicamente no ambiente eletrônico tal qual o MCI, aqui a aplicabilidade da norma será nos diferentes meios. Ademais, a LGPD assume um papel de complementar a citada Lei para a formação de um sistema coeso, já que brevíssimas descrições foram feitas no tocante ao tratamento de dados.

Em relação ao Código de Defesa de Consumidor, estará disposto em seu artigo 43 que o consumidor terá acesso às informações em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. Nesse sentido, observará Bioni (2019, p.184) que o objetivo do legislador ao elaborar o dispositivo exposto foi alcançar todo e qualquer banco de dados que atinja o livre desenvolvimento da personalidade do consumidor. Por conseguinte, tanto no CDC como na LGPD será levantado a necessidade do consentimento do titular de dados e o respeito à finalidade para que seja feita a obtenção de dados, além de ser possibilitado a correção destes. Em relação a este último ponto, a LGPD

complementará tal direito possibilitando que o titular acesse todos os dados pessoais que estão sendo coletados e tratados pelo controlador, desse modo, toda informação tratada em desconformidade com esta Lei poderá ser excluída ou cancelada a pedido do titular.

A última explanação refere-se a Lei do Cadastro Positivo, em que será disciplinado acerca da formação e consulta a banco de dados com informações de adimplementos, seja de pessoas físicas ou jurídicas, para formação de histórico de crédito, em consonância com disposto no artigo 1° desta Lei. De maneira convergente com a LGPD, a Lei acima possibilita ao cadastrado, mediante requerimento, a exclusão de informações inseridas no cadastro a qualquer momento, além disso, ambas guardarão semelhança pela valorização da finalidade para a qual os dados foram coletados (MINASSE e RIBEIRO,2019). Tal como demonstrado anteriormente, os dados pessoais serão tratados de modo específico na LGPD, desse modo, serão presentes algumas diferenças entre as Leis tratadas neste parágrafo. Nesse viés, destaca- se que na Lei do Cadastro Positivo as informações referentes ao cancelamento do cadastro não são detalhadas de maneira clara, não há informações para o titular ter acesso, de modo fácil, às informações sobre o tratamento de seus dados, além disso, não há uma autoridade competente para a fiscalização do cumprimento desta Lei (MINASSE e RIBEIRO,2019).

Findado esse pequeno esclarecimento a respeito do CDC, MCI e da Lei do Cadastro Positivo, evidenciou-se, por meio de referências aos dispositivos destas normas e o porquê de elas integrarem o ordenamento jurídico, que os dados pessoais são, de fato, referenciados em seus textos. Apesar disso, a LGPD dispõe do tratamento de dados de forma mais completa e guarda em seus artigos instruções e obrigações a serem cumpridas neste tratamento, de modo a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, tal como estabelecido no art. 1°.

Nessa toada, de modo a compreender o porquê de a discussão ao redor do tratamento de dados pessoais ganhar tamanha proeminência na atualidade, seja na esfera econômica, política, social ou jurídica, é crucial a demonstração de problemáticas causadas pelo não cumprimento de direitos fundamentais basilares, especialmente aqueles que se relacionam aos fundamentos da disciplina de proteção de dados dispostos no art. 2° desta Lei, sendo estes;

> 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.

Assim sendo, destacam-se três casos que ilustram as questões sublinhadas acima.

O primeiro exemplo será da empresa *Red Cross Blood Service*, que realiza coleta e doação de sangue na Austrália. Em 2016, dados referentes ao comportamento sexual dos doadores foram expostos na internet por conta da transferência de arquivos para um local não seguro (MULHOLLAND, 2018).

A segunda situação ocorreu em 2017 quando a empresa *Standard Innovation* disponibilizou um vibrador que colhiam informações relacionados ao seu uso, no entanto, não havia a indicação em nenhum termo acerca da colheita de dados (MULHOLLAND, 2018).

O último caso será do denominado sistema de crédito social ("*social scoring*") adotado na China, por meio do qual ocorre a categorização e taxação do comportamento dos cidadãos, informações que serão, futuramente, utilizadas pelo Estado para indicar quais políticas públicas os indivíduos terão acesso (MULHOLLAND, 2018).

À vista disso, serão perceptíveis diferentes tipos de violações no tratamento de dados, no primeiro exemplo ocorrerá a violação no dever de segurança dos dados, no segundo uma violação do princípio da finalidade, e no terceiro a violação do princípio da não discriminação. Acrescente-se, que os dados referenciados possuem capacidade de serem utilizados de forma discriminatória pelo Estado e pelo mercado, tratando-se, portanto, de dados sensíveis (MULHOLLAND, 2018).

Nesse viés, é claro-evidente que as situações expostas infringem, de modo incisivo, os direitos e garantias fundamentais, na medida em que a intimidade e a vida privada, salvaguardadas no art. 5° da CF/88, são afrontadas pela exposição de dados pessoais sem a ciência e consentimento de seus titulares. Nessa linha, defenderá Stefano Rodotá (2008, p.92, apud MULHOLLAND, 2020, p.49) que a proteção da privacidade será "o direito de manter o controle sobre as próprias informações", posto que na sociedade da informação em que os indivíduos estão

inseridos é necessária uma releitura da privacidade, pois o simples “direito a ser deixado só”, defendido por Warren e Brandeis em 1890, não salvaguardaria o indivíduo, na medida em que cada vez mais os titulares de dados possuem suas informações compartilhadas, especialmente no meio digital. Por esse ângulo, “o reconhecimento de que “nós somos as nossas informações” impõe que sejamos capazes de obter meios para controlar a circulação de nossos dados pessoais (MULHOLLAND, 2020, p.8),

Por consequência, tendo em vista as inovações tecnológicas cada vez mais constantes em nossa sociedade e a capacidade destas de potencializarem a não observância de direitos fundamentais, apresentou-se essencial a edição de um marco legal que diminuísse o descompasso entre este meio e o tratamento de dados. Vale ressaltar, que um cidadão brasileiro chega a passar, em média, 3 horas e meia por dia navegando na internet (WEARESOCIAL, 2020) , desse modo, a LGPD é indispensável para a proteger aquilo que seria o corpo eletrônico do indivíduo, uma vez que a utilização deste ambiente pressupõe, em algum momento, que seja realizado o tratamento de dados, sendo este “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”; (art. 5, X).

No campo político, pode-se relacionar o interesse na aprovação da LGPD em 2018 com o intuito do governo brasileiro em pleitear sua entrada na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que possui como requisito a vigência de uma regulamentação sobre o tema de proteção de dados pessoais. Nesse cenário, a construção do texto normativo da Lei aqui tratada tem como forte inspiração o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), posto que esta norma entrou em vigor em maio de 2018, sendo assim, uma espécie de norte para a LGPD, que no período destacado, ainda estava em construção.

CONDIÇÕES PARA A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Neste momento, prosseguir-se-á para as hipóteses de aplicação da LGPD, posto que as razões e motivos que a fundamentam foram apresentadas anteriormente. Nesse viés, urge que seja feito um destaque ao artigo 3°, na medida em que o texto normativo prescreverá que a

LGPD será aplicada a qualquer operação de tratamento de dados pessoais, tenha ela sido realizada por pessoa física ou por pessoa jurídica de direito público ou privado. Além disso, discorrerá o artigo que independentemente do meio utilizado ela será empregada, englobando tanto os meios virtuais quanto os físicos. Além disso, dispõe sua parte final que independentemente do país sede da pessoa que realiza o tratamento ou do país onde estejam localizados os dados, a Lei será aplicada na condição de haver uma operação de tratamento de dados. Portanto, a aplicação da Lei ocorre mesmo na hipótese de os dados estarem localizados em outro local diverso do Brasil, no entanto, deverão ser presentes pelo menos um dos requisitos destacados abaixo;

> - a operação de tratamento seja realizada no território nacional;
> - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

À face do exposto, os três requisitos referenciados possuem como denominador comum o fato de relacionarem o tratamento de dados com o território nacional, assim sendo, para que a LGPD seja aplicada o tratamento deverá ser realizado no Brasil ou os dados tratados são de indivíduos localizados no território nacional, ou os dados pessoais tenham sido coletados no Brasil.

No primeiro requisito, a Lei será aplicada dentro das fronteiras do Brasil desde que ocorra alguma operação de tratamento, termo previsto no art. 5°, X, da LGPD e já tratado no texto atual.

No segundo a LGPD será aplicada na circunstância do destinatário final de oferta ou fornecimento de bens ou serviços ou de tratamento de dados ser indivíduo localizado no território nacional. Aqui, encontra-se um desafio, na medida em que a pessoa física ou jurídica de direito privado não necessariamente possuirá representação no Brasil, logo, a aplicabilidade da Lei estará sujeita à fatores próprios das relações internacionais. Tal como preconizado por Kelsen (1999, p.201), “o chamado território do Estado apenas pode ser definido como o domínio espacial de vigência de uma ordem jurídica estadual”, dessa forma, a jurisdição do Estado Brasileiro não poderá ser exercida prontamente no território estrangeiro no qual foi observado as atividades supracitadas e elencadas no art. 3°.

O último requisito tratará, de forma semelhante ao primeiro, de ação praticada no território nacional, entretanto, aqui, o dispositivo levantará a hipótese de aplicação da LGPD

por conta de coleta de dados pessoais ocorrida no território nacional. Acrescente-se, que não há necessidade de o titular dos dados ser domiciliado ou residentes no Brasil, ou ainda ter nacionalidade brasileira, o que basta é que o indivíduo se encontre no território brasileiro no momento da coleta.

Em contrapartida, a Lei também elencará os casos em que não caberá a sua aplicação integral. De modo popular, muito se repete aquele velho ditado que "a diferença entre o veneno e o remédio é a dose", nesse caminho, já que a LGPD foi concebida, essencialmente, para proteger uma gama de direitos fundamentais da pessoa natural, tais como a privacidade, liberdade e livre desenvolvimento, uma aplicação absoluta, desmedida e irrestrita da Lei reverberaria retrocessos expressivos no ordenamento jurídico, prejudicando, em verdade, o destinatário desta norma. Em conformidade com o abordado, acerca da importância do equilíbrio normativo exemplifica-se que;

> A lei brasileira de direitos autorais (Lei n° 9.610/98, LDA) conta com um capítulo chamado "Limitações aos direitos autorais", que é de grande importância para a construção de um sistema jurídico equilibrado. Afinal, se não há qualquer dúvida sobre a necessidade de se protegerem as criações intelectuais, também é evidente que esta proteção não pode ser absoluta, gerando para os titulares de direitos autorais exclusividades tão amplas que servissem de obstáculo ao desenvolvimento artístico, técnico e educacional. (MULHOLLAND, 2020, p.23)

Diante disso, o art. 4° levantará uma série de hipóteses, em seus incisos, nas quais ocorrerá o tratamento de dados pessoais, mas a LGPD não será aplicada.

O primeiro inciso discorrerá que o tratamento de dados pessoais feito por pessoa física não estará no escopo da LGPD quando realizado para fins exclusivamente particulares e não econômicos. Observa-se, que não há justificativas para o Poder público ser envolvido aqui, já que a hipótese trata da atividade privada, sem intuito econômico.

Em seguida, o inciso II fará ressalvas para as condições em que o tratamento de dados pessoais seja realizado para fins exclusivamente jornalísticos e artísticos ou acadêmicos. De forma semelhante, o Regulamento Geral de Proteção de Dados aplicado na União Europeia também tratará em seu artigo 85, 1, a respeito destas atividades.

> Os Estados-Membros conciliam por lei o direito à proteção de dados pessoais nos termos do presente regulamento com o direito à liberdade de expressão e de informação, incluindo o tratamento para fins jornalísticos e para fins de expressão académica, artística ou literária

No ordenamento jurídico brasileiro alguns desafios serão encontrados quanto ao limite das exceções dispostas no inciso II. No mais, deve ser feita uma interpretação abrangente do

disposto, de modo a não restringir as liberdades individuais. Por fim, para encetar o questionamento da matéria, anote-se o seguinte trecho;

> O que caracteriza uso jornalístico, especialmente levando em consideração que no Brasil o exercício do jornalismo independe de diploma? Ou, ainda, o que caracteriza fins acadêmicos? É necessário estar vinculado a um programa formal escolar ou universitário, por exemplo? Ou qualquer pesquisa pode ser considerada acadêmica? (MULHOLLAND, 2020, p.25)

No tocante à terceira hipótese de não aplicação da LGPD, o inciso III abordará que quando o tratamento de dados pessoais for realizado para fins exclusivos de segurança pública ou defesa nacional ou segurança do Estado ou atividades de investigação e repressão de infrações penais não haverá que se falar no emprego desta Lei. Desse modo, foi feita uma ponderação pelo legislador a respeito dos direitos individuais e o interesse público e decido que a segurança do corpo social deve ser privilegiada.

Acrescente-se, que o tratamento de dados pessoais previstos acima será regido por legislação específica que conterá medidas proporcionais e estritamente necessárias, as quais observarão os princípios gerais de proteção e os direitos do titular previstos nesta Lei. Por óbvio, essas exceções do inciso III não serão aplicadas às pessoas de direito privado, excetuada as hipóteses nas quais estas estejam em procedimentos sob tutela de pessoa jurídica de direito público, circunstância que será informada à autoridade nacional, ainda assim, não poderá ser tratada a totalidade dos dados pessoais dos bancos de dados. Ademais, a Autoridade Nacional de Proteção de Dados Pessoais será responsável por emitir opiniões técnicas e recomendações no tocante às hipóteses que excepcionam a aplicabilidade da LGD no inciso III, cabendo a esta autoridade nacional também solicitar aos respectivos relatórios de impacto à proteção de dados pessoais.

Na última hipótese prevista no artigo 4°, a LGPD não será aplicada ao tratamento de dados pessoais provenientes de fora do Brasil e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência dos dados. Vale ressaltar, que o país de origem dos dados pessoais necessita ter, no mínimo, um grau de proteção proporcional ao propiciado pela LGPD.

CONTEXTUALIZAÇÃO DOS TERMOS DEFINIDOS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Quanto aos conceitos utilizados ao longo de toda a LGPD, estarão presentes no artigo 5° da referida Lei as definições e significados dos termos empregados no texto normativo, diminuindo possíveis desencontros interpretativos e uniformizando o entendimento ambicionado pela norma.

As definições tratadas no artigo 5° são agrupadas de acordo com o assunto versado, de modo que o primeiro grupo se relaciona ao dado pessoal, ao dado pessoal sensível, dado anonimizado e ao banco de dados. O segundo grupo expõe acerca das definições da pessoa jurídica, pessoa física de direito público e de direito privado que a proteção de dados no Brasil implica. O terceiro grupo traz à luz as definições que se referem tanto aos dados quanto aos indivíduos envolvidos no tratamento de dados, qualificando, então, as ações praticadas pelos indivíduos quanto aos dados pessoais. O quarto e último grupo concebe três disposições de improba compilação, que se encontram sob uma única intitulação por se tratar de institutos distintos.

Primeiramente, vale destacar que o artigo 5° categoriza e tutela, de maneira diferenciada, os dados pessoais e os dados pessoais sensíveis. Os dados pessoais são compostos por informações relacionadas à pessoa natural identificada ou identificável e, os dados pessoais sensíveis aludem à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, de acordo com o inciso II do artigo 5°.

De acordo com o conceito de dados sensíveis abordado no parágrafo anterior, vale constatar a potencialidade discriminatória no tratamento de dados pessoais, ou seja, a limitação a qual se desdobraria a fim de que o tratamento de dados se concretizasse em prol da proibição de seu uso, de modo a gerar uma discriminação, com um uso abusivo e não igualitário de dados.

Nessa mesma perspectiva, Danilo Doneda (2003, p.160-161) concebe que os dados sensíveis são “determinados tipos de informação que, caso sejam conhecidas e processadas, prestar-se-iam uma potencial utilização discriminatória ou particularmente lesiva (apud MULHOLLAND, 2020, p. 138).”. A partir dessa concepção, pode-se perceber que para Doneda os dados sensíveis são determinados a partir do efeito do seu tratamento em relação aos demais dados pessoais. Assim, de acordo com o autor tem-se que a igualdade material estaria em um patamar acima da permissibilidade de o titular dos dados exercerem seus direitos de maneira autônoma, sem que houvesse qualquer limitação abusiva ou indevida. Portanto, o dado em si, não é nem perigoso nem discriminatório, mas pode ser de acordo com

o uso que se faz. Portanto, o dado em si não é nem perigoso nem discriminatório, mas pode ser de acordo com o uso que se faz, podendo-se, então, concluir que "o conceito de dados sensíveis deve ser funcionalizado de acordo com o tratamento que é concedido a eles" (MULHOLLAND, 2020, p. 139).

Além disso, vale ressaltar que um dado trivial pode vir a ser transmudado em um dado sensível, dando enfoque aqui as *big datas*, que permitem que haja a correlação de dados para que comportamentos e acontecimentos sejam previstos. Um grande exemplo para tal é o caso utilizado por Bioni (2018, p. 85, apud MULHOLLAND, 2020, p. 138) para demonstrar como um "dado trivial" pode também se transmudar em um dado sensível, em que o Facebook foi utilizado como objeto de estudo, em que a Universidade de Cambridge utilizou as "curtidas" como pilar para a identificação de aspectos sensíveis dos usuários da rede. Ou seja, a partir de um dado trivial, nesse caso as curtidas, foi conseguido que fosse transformado em um dado sensível, uma vez que identificou dados de natureza personalíssima e de potencial discriminatório.

A terceira definição trazida pelo artigo 5° da LGPD é o de dados anonimizados que, são dados que impedem que o indivíduo a ele associado venha a ser reconhecido, ou seja, é incapaz de revelar a identidade da pessoa a qual o dado se refere. É importante que se perceba que os dados anonimizados não fazem parte do rol de dados pessoais, entretanto, caso ocorra um processo de reversão da anonimização, os dados se tornarão, então, dados pessoais.

Os bancos de dados são a quarta definição que o artigo 5° elucida. Os bancos de dados são o conjunto estruturado de dados pessoais, estabelecido em um ou vários locais, de modo que, a importância trazida a luz se mostra presente no conceito do termo "estruturados" mostrando que para que seja considerado um banco de dados é necessário que os dados estejam organizados conforme uma lógica interna e não apenas dados em conjuntos sem qualquer espécie de organização ou lógica.

O titular, primeira pessoa de que trata o segundo grupo do artigo 5°, é a pessoa natural a quem se referem os dados pessoais nos quais são objeto de tratamento. Desse modo, pode-se perceber que os dados protegidos nos termos da LGPD apenas as pessoas físicas.

O controlador, definição trazida pelo inciso VI do artigo 5°, é a quem compete as decisões referentes ao tratamento de dados pessoais, independentemente de ser pessoa natural ou jurídica, de direito público ou privado, ou seja, pode-se perceber que, então, as atividades de controlador podem ser exercidas tanto por pessoa física quanto por pessoa jurídica tendo a função de tomar as decisões quanto ao tratamento dos dados pessoais.

Nessa mesma linha, o operador é quem realiza o tratamento dos dados pessoais em nome do controlador, ou seja, a diferença presente entre o controlador e o operador é que o operador é quem detém o poder de decisão. Já o operador pode realizar o tratamento dos dados,

mas somente a partir das ordens de um controlador, que, por sua vez, apresenta-se como dono ou responsável por essas informações, estando o controlador, dessa forma, no topo da cadeia de tratamento de dados.

Vale ressaltar que a LGPD não discorre acerca de o operador ser ou não empregado do controlador, de modo que, pode ser contratado para atuar enquanto operador, como um terceiro contratado. Dessa forma, é importante que se fale acerca do encarregado, que é o canal de comunicação entre o controlador, os titulares de dados e o governo. Ou seja, todas as conclusões e instruções do encarregado devem ser levadas ao conhecimento dos mais altos escalões hierárquicos do controlador, tendo em vista o poder decisório daquele e dos riscos envolvidos em caso de inequação à LGPD. Assim, o encarregado não pode ter nenhuma ingerência sobre as atividades do controlador pois em razão de sua independência deve apenas orientar, cabendo a gestão exclusivamente ao respectivo controlador.

O tratamento, tratado no inciso X do artigo 5°, é qualquer atividade que utilize um dado pessoal na execução da sua operação, figurando como um elemento central. Vale salientar que a definição de tratamento é deveras abrangente, de modo que engloba todas as atividades a que se relaciona.

O consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma determinada finalidade, sendo fundamental para o sistema de proteção de dados da LGPD. O consentimento mostrou sua visibilidade desde o Marco Civil da Internet, sendo a hipótese mais abrangente e com maior incidência prática. Vale ainda destacar que o consentimento visa a garantia de que ele foi obtido por meio da manifestação livre, informada e inequívoca, nos termos da LGPD.

O bloqueio é a suspensão temporária de qualquer operação de tratamento mediante guarda do dado pessoal ou do banco de dados. O bloqueio é outro termo no qual o Marco Civil da Internet já havia se referido, entretanto, a LGPD traz à tona uma definição mais detalhada e abrangente.

A eliminação é a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado. No que tange a eliminação, tanto a LGPD quanto o Marco Civil tratam como a exclusão de dados pessoais (BUCAR, 2013, apud MULHOLLAND, 2020, p. 37).

A transferência internacional de dados é a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro. Vale ressaltar que a transferência internacional de dados busca condicionar o fluxo internacional de dados pessoais dos cidadãos brasileiros a países que possuam níveis de proteção e privacidade e de dados pessoais equiparáveis, dando ênfase à transparência sobre acordos internacionais, bilaterais ou regionais que versem sobre o tema e ao incentivo à adoção de padrões contratuais internacionalmente conhecidos.

Além disso, tem-se o uso compartilhado de dados, a última definição do terceiro grupo. O uso compartilhado de dados é definido como comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados, de forma que relaciona-se com a atuação de entes públicos ou privados, nacionais ou estrangeiros.

Dando início à primeira definição do quarto grupo, tem-se o relatório de impacto à proteção de dados pessoais, que é um instrumento de responsabilidade do controlador, pelo qual, em qualquer operação que envolva o tratamento de dados pessoais que possa gerar riscos às liberdades civis e aos direitos fundamentais, será realizada a descrição dos processos para mitigação de riscos e concomitantemente, de responsabilidades. O relatório de impacto se relaciona diretamente a atividade da Autoridade Nacional, que de acordo com o artigo 10,

§3° pode demandá-lo ao controlador que quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

O Órgão de Pesquisa, de acordo com o inciso XVIII é quem é legitimado a conduzir o tratamento de dados, sob a condição de que na realização dos estudos, a anonimização dos dados seja preservada.

A autoridade nacional é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. Vale acentuar

que, a autoridade nacional é o órgão da administração pública federal, integrante da Presidência da República. Além disso, a autoridade nacional é o órgão que sanciona e fiscaliza o cumprimento da Lei Geral de Proteção de Dados.

PRINCÍPIOS NORTEADORES DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Além das definições trazidas a luz do artigo 5°, a LGPD elencou em seu artigo 6° os dez princípios que conduzem as atividades de tratamento de dados pessoais. O primeiro princípio elencado é o Princípio da Finalidade, que fixa que o tratamento dos dados deve ter propósitos legítimos, específicos, explícitos e informados previamente ao titular (FEDERAL TRADE COMISION. Internet of things: Privacity & Security in a Connected World. *FTC Staff Report*, 2015, p.21-22 apud MULHOLLAND, 2020 p. 57). A partir desse princípio, de acordo com Doneda, pode-se estruturar "um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria a abusividade)" (DONEDA, 2010, p.46, apud MULHOLLAND, 2020, p.54)

O princípio da finalidade traz à tona a junção de todos os princípios elencados no artigo 6° para que ocorra o melhor tratamento dos dados pessoais. Por propósitos legítimos se refere uma finalidade movida pelo bom senso, pela razão, legitimidade, bons costumes, boa- fé, distanciando-se, portanto, da iniciativa subalterna, de má fé. Por meio dos propósitos específicos são enfatizados a preocupação de que o tratamento se volte, certeiramente, para um objetivo determinado ou relevante para o ser. Os propósitos explícitos procuram enfatizar os aspectos únicos do tratamento, ou seja, admitindo a equivocidade ou ambiguidade. Tendo o objetivo previamente delineado, não permite que dúvidas possam surgir após ser especificado o seu conteúdo. Assim, todos os objetivos integradamente conformam a finalidade admitida pelo normativo, devendo, então, serem informadas ao titular, que concordará e delimitará o objeto de tratamento, domínio esse que não poderá ser subsequentemente alterado, salvo se a nova específica e expressa concordância for obtida desse titular.

O princípio da adequação dispõe que o tratamento de dados deve ser compatível com a finalidade, devendo os dados coletados serem usados apenas a partir do ponto em que forem necessários a fim de alcançar os objetivos previamente informados, consoante com o contexto do tratamento. O princípio da adequação se refere a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. Nessa linha, a adequação se refere ao nexo de pertinência lógica de conformidade que se estabelece entre o tratamento e a finalidade objetivada, tal como previamente informada ao titular.O princípio da necessidade dispõe que devem ser tratados apenas os dados mínimos necessários, pertinentes,

proporcionais e não excessivos em relação às finalidades do tratamento. O princípio da necessidade tem sua unificação quando da limitação da realização do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Dessa forma, tem-se que é necessário sempre questionar o porquê se faz necessária a coleta de determinados dados, devendo a resposta ser o mais rutilante possível.

O princípio do livre acesso e transparência, dispostos no inciso IV e VI, dispõe que os titulares podem consultar gratuita e facilmente a forma, duração de tratamento e a integridade de seus dados pessoais. A resposta da consulta, há de ter seu acesso fácil sobre a realização dos agentes de tratamento, da maneira mais clara e precisa possível. O princípio do livre acesso garante que ao momento que desejam as pessoas possam vir a acessar os próprios dados. Dessa forma, tendo acesso a uma maneira de consulta gratuita dos dados coletados e que tiveram o tratamento dispensado.

O princípio da qualidade dos dados dispõe que os dados devem ser exatos, claros e adequados, de acordo com a necessidade e para o cumprimento da finalidade. De acordo com esse princípio, os dados a serem colhidos e posteriormente disponibilizados devem ser verídicos e que condigam com a maneira na qual os objetos foram utilizados e inter- relacionam-se com a tecnologia. Além disso, tal princípio reclama que os dados estejam atualizados. Ou seja, a partir desse princípio, tem-se que os dados armazenados devem ser fiéis à realidade, além de que devem estar atualizados, completos e relevantes (BRASIL, 2010, p.46 apud MULHOLLAND, 2020, p.57)

O princípio da segurança e prevenção (incisos vii e viii) dispõe que devem ser utilizadas medidas técnicas e administrativas para prevenir acidentes, como por exemplo o vazamento de dados ou invasão por hackers. A partir do princípio da segurança, deve sempre ocorrer a atualização das medidas técnicas e administrativas, a fim de proteger os dados de acesso não autorizados. O princípio da prevenção discorre acerca dos métodos preventivos que abarcam as medidas técnicas que lhe cabem a fim de evitar que ocorram danos desinentes do tratamento de dados.

O princípio da não discriminação dispõe que o tratamento não pode ser realizado para fins discriminatórios ilícitos ou abusivos. O princípio da não discriminação determina que os dados colhidos não podem vir a manejar os dados de maneira discriminatória nem mesmo em direção à fins discriminatórios. Nessa linha, se tem o exemplo da Internet das Coisas que, por intermédio dos objetos conectados, permite a classificação dos consumidores de maneira meticulosa. O autor Scott Peppet (2014, p. 117-120 apud MULHOLLAND, 2020, p.59) exemplifica a discriminação por meio da Internet das Coisas através da situação em que os empregadores podem vir a avaliar os dados dos candidatos de determinada vaga de emprego e tomar as decisões a partir desses dados. Além disso, expõe que apesar de não aparentar, tudo mostra tudo – do inglês *everything reveals everything* (PEPPET, 2014, p.121 apud MULHOLLAND, 2020, p.59). Nessa linha, é válido que dois pontos sejam analisados e o sensor fusion é o primeiro deles. O sensor fusion é uma maneira de obtenção de dados por meio de uma técnica de cruzamento de dispositivos distintos, ou seja, os dados coletados podem vir a ser coletados para conclusões mais complexas. O segundo ponto é a *big data*, em que as informações fisiológicas, físicas sobre os usuários sejam coletadas por meio de dispositivos e, com a aplicação de algoritmos, se faz possível a inferência sobre o estado físico, fisiológico e comportamental das pessoas (DONEDA, 2016, p. 2-5 apud MULHOLLAND, 2020, p.60)

Ainda, dentro do princípio da não discriminação, é importante que se mencione acerca do setor de seguros. Uma vez que o princípio da não discriminação versa acerca da impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos. Dessa forma, percebe-se que a discriminação que a LGPD veda é a referente a fins ilícitos ou abusivos. Nessa linha, tem-se que a seleção de riscos realizada com a finalidade ética legalmente válida fica protegida de ser considerada ilegal à vista da LGPD. Nesse contexto, um exemplo clássico e relevante é o da precificação de seguros tanto residencial quanto de automóvel, a partir dos dados do CEP de residência do segurado. Tal exemplo não é uma exemplificação de discriminação social, entretanto, se adequa a um exemplo de seleção de risco com o objetivo legalmente válido pelo fato de a realidade que alguns locais são estatisticamente mais sujeitos à prática de violência que outros.

O princípio da responsabilização e prestação de contas dispõe acerca da efetividade dessas medidas técnicas e administrativas deve ser demonstrada. Tal princípio requer do agente a capacidade de demonstração da eficácia das medidas adotadas para o cumprimento das normas de proteção de dados pessoais.

CONSIDERAÇÕES FINAIS

A partir do evidenciado, pode-se perceber que o tratamento dos dados pessoais se realiza de modo específico e diferenciado na Lei Geral de Proteção de Dados. Além do mais, com base no explanado, salienta-se que apesar da existência prévia do CDC, do MCI e da Lei do Cadastro Positivo na composição do ordenamento jurídico de maneira a referenciar os dados pessoais, foi a partir da LGPD que o tratamento desses dados pessoais passou a ser tratado de maneira mais completa e passou a dispor acerca das obrigações a serem cumpridas. No mais, com base nos exemplos fáticos referenciados no corpo deste artigo, os quais permeiam tanto a esfera social quanto a jurídica e política, percebe-se tamanha importância da LGPD, uma vez que expostos os dados pessoais sem o consentimento de seus titulares a intimidade e a vida privada são expostas, levando ao descumprimento dos direitos fundamentais, sendo necessária , então, uma Lei que regule tais fatos, de modo a proteger os dados pessoais que trazem à luz sua natureza personalíssima e seu potencial discriminatório.

Portanto, não se envidam dúvidas acerca da importância da LGPD, já que as Leis que a antecedem não abordam, de maneira plena, o tratamento de dados pessoais. Por fim, ao direcionar sua atuação para esta atividade, faz-se presente uma norma que protegerá os direitos fundamentais de liberdade e de privacidade e, ainda, garante o livre desenvolvimento da pessoa natural.

REFERÊNCIAS:

BIONI, Bruno Ricardo. Proteção De Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense Ltda, 2019.

BRANDEIS, L. e WARREN, S. (1890). The right to privacy. Harvard Law Review,
4.

DIGITAL 2020: global digital overview. Wearesocial, 2020. Disponível em: https://wearesocial.com/digital-2020. Acesso em: 08/12/2020.

KELSEN, Hans. Teoria Pura do Direito. 6. ed. São Paulo: Livraria Martins Fontes Editora Ltda, 1998.

MINASSI, Elton e RIBEIRO, Yuri Camelo. Interface entre a nova lei do cadastro positivo e a Lei Geral de Proteção de Dados. MachadoMeyer, 2019. Disponível em:

https://www.machadomeyer.com.br/pt/inteligencia-juridica/publicacoes- ij/tecnologia/interface-entre-a-nova-lei-do-cadastro-positivo-e-a-lei-geral-de-protecao-de- dados. Acessado em: 10/12/2020.

MULLHOLAND, Caitlin Sampaio. Dados pessoais e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei. 13.709/18), 2018.

MULHOLLAND, Caitlin. A LGPD e o novo marco normativo no Brasil. 1ª edição. Arquipélago, 05 de junho de 2020.

DOS DIREITOS DO TITULAR NA LGPD E NA GDPR

Juliana Soave dos Reis

INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD) foi implementada no Brasil em 2018 mas só entrou em vigor em agosto de 2020, é portanto uma norma muito nova e que gera diversas incertezas e inseguranças na sua implementação. Na Europa, a GDPR foi implementada em maio de 2018 revogando a Diretiva Europeia 95/46/CE sobre proteção de dados pessoais. Por já possuir jurisprudências e seu texto ser, de certa forma, similar ao da Lei implementada no Brasil, a General Data Protection Regulation auxilia no entendimento e julgamento de casos brasileiros.

O presente artigo tem por objetivo estabelecer uma análise dos direitos dos titulares de dados pessoais presentes na Lei Geral de Produção de Dados por meio do destrinchamento de seus artigos e comparação com a GDPR européia.

DOS DIREITOS DO TITULAR NA LGPD

Na parte oral das apresentações que precederam o presente artigo, dentre os diversos temas que poderiam ser abordados sobre a LGPD, escolhi o tópico dos direitos dos titulares de dados pessoais e, portanto, este é o objeto de estudo deste artigo. Esse instituto que passaremos a ver está previsto do artigo 17 ao 22 da Lei 13.709/2018 e tem alguns pontos coincidentes com os artigos referentes ao tratamento dos dados, por exemplo o art. 9º que fala sobre o acesso facilitado às informações sobre o tratamento de seus dados e o art. 15, inciso III, que prevê a possibilidade de revogação do consentimento pelo titular, que também é um dos direitos que veremos aqui.

O art. 17, inicia tratando da questão de quem são os titulares dos dados, nesta seara podemos aferir que a pessoa natural é e sempre será titular de seus dados, independente do tipo de autorização que for dada para tratamento dos dados, sendo-lhe garantido os direitos fundamentais de liberdade, intimidade e privacidade.

No art. 18 e seus incisos estão elencados mais especificamente os direitos do titular que são basicamente o acesso, a retificação, o cancelamento e a oposição. Isso significa que o titular poderá ter acesso aos seus dados, requerer cópia detalhada do que está sendo armazenado, solicitar correção ou complementação de algum dado ou ainda a exclusão ou anonimização do mesmo, este último quando os dados forem 1) desnecessários para a finalidade que justifica a realização do tratamento; 2) excessivos em relação ao necessário para alcance da finalidade ou 3) caso não estejam

sendo tratados para finalidades específicas ou o tratamento não seja justificável por nenhuma base legal.

Em muitos quesitos a lei é autoexplicativa, os parágrafos do art.18 trata da forma de acesso a esses dados pelo titular, senão vejamos:

> § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
> § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
> § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
> § 4º Em caso de impossibilidade de adoção imediata da providência de que trata o 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
> - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
> - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
> § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
>
> § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.
>
> § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
>
> § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

O art. 19 começa tratando sobre a forma que deve ser fornecidas as informações solicitadas pelo titular.

> Art.19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:
> - em formato simplificado, imediatamente; ou
>
> - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.
>
> **Então, esses relatórios não podem ter uma linguagem muito técnica porque eles precisam ser compreendidos pelas pessoas físicas que são as titulares, mesmo as declarações completas, precisam ser em uma linguagem clara e simples. Seguindo...**

> § 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.
> § 2º As informações e os dados poderão ser fornecidos, a critério do titular:
> I - por meio eletrônico, seguro e idôneo para esse fim; ou
> II - sob forma impressa.
> § 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.
> § 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

O art.20 trata de uma questão bem interessante e atual que são as decisões automatizadas por machine learning, inteligência artificial e outras formas de inteligências mecanizadas, em que o titular poderá solicitar a revisão das decisões.

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Por fim, o art 21 esclarece que o uso de dados pessoais só poderá ser realizado para os fins consentidos pelo titular e para cumprimento de obrigações regulatórias do controlador, não podendo haver prejuízos à imagem, à segurança ou à integridade do titular.

Além disso, o art. 22 admite o ajuizamento de ação individual ou coletiva com demais titulares que tenham se sentido prejudicados pelo mesmo controlador.

Portanto, terminada a breve exposição e explicação dos artigos que compõem a LGPD, passaremos a expor a GDPR explicando suas cláusulas e apresentando um caso concreto para análise.

DOS DIREITOS DO TITULAR NA GDPR

A General Data Protection Regulation, é considerada a lei mais completa sobre proteção de dados no mundo, dada sua ampliação dos direitos dos usuários e maior responsabilização das organizações e empresas que realizam o processamento de dados. Nela, os direitos dos titulares são tratados do art.12 ao art. 23 e está dividido entre direito ao acesso, direito à retificação, direito à exclusão ou esquecimento, direito à oposição e restrição de processamento, direito à portabilidade de dados, direito à informação e direito à notificação.

O art. 12 é dividido em 8 partes e trata especificamente do fornecimento de informações aos titulares. Esse fornecimento dos dados deve ser realizado de forma clara, como que para uma criança, ou seja, sem vocabulário técnico que dificulte a compreensão; por via escrita, oral ou eletrônica, a depender de como foi realizado o pedido; no prazo de 1 mês podendo ser estendido por mais 2 meses; de forma gratuita ou com uma taxa razoável caso o pedido seja repetitivo, infundado ou excessivo; o controlador deve confirmar a identidade do titular antes de passar os dados.

O art.13 possui 4 números e aborda a informação que deve ser dada aos titulares no momento do colhimento dos dados pelo controlador.

> Artigo 13 - Informações a serem fornecidas quando os dados pessoais são coletados do titular dos dados
> Quando os dados pessoais relativos a um titular dos dados são coletados do titular dos dados, o responsável pelo tratamento deve, no momento em que os dados pessoais forem obtidos, fornecer ao titular dos dados todas as seguintes informações:
>
> a identidade e os dados de contato do responsável pelo tratamento e, quando aplicável, do representante do responsável pelo tratamento;
>
> os dados de contato do responsável pela proteção de dados, quando aplicável;
>
> os fins do tratamento a que se destinam os dados pessoais, bem como a base jurídica para o tratamento;
>
> sempre que o tratamento se baseie no artigo 6.º, n.º 1, alínea f), os interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros;
>
> os destinatários ou categorias de destinatários dos dados pessoais, se houver;
>
> quando aplicável, o facto de o responsável pelo tratamento pretender transferir dados pessoais para um país terceiro ou organização internacional e a existência ou ausência de uma decisão de adequação por parte da Comissão, ou no caso de transferências referidas nos artigos 46.º ou 47.º, ou o segundo parágrafo do artigo

> 49.º, n.º 1, referência às salvaguardas apropriadas ou idôneas e aos meios para obter uma cópia das mesmas ou ao local onde foram disponibilizadas.
>
> Além das informações referidas no n.º 1, o responsável pelo tratamento deve, no momento da obtenção dos dados pessoais, fornecer ao titular dos dados as seguintes informações adicionais, necessárias para garantir um tratamento justo e transparente:
>
> o período durante o qual os dados pessoais serão armazenados ou, se isso não for possível, os critérios usados para determinar esse período;
>
> a existência do direito de solicitar ao responsável pelo tratamento o acesso e a retificação ou apagamento dos dados pessoais ou a restrição do tratamento do titular dos dados ou de oposição ao tratamento, bem como o direito à portabilidade dos dados;
>
> quando o tratamento se baseia na alínea a) do artigo 6.º, n.º 1, ou na alínea a) do artigo 9.º, n.º 2, a existência do direito de retirar o consentimento a qualquer momento, sem afetar a legalidade do tratamento com base no consentimento antes sua retirada;
>
> o direito de apresentar queixa a uma autoridade de supervisão;
>
> se o fornecimento de dados pessoais é um requisito legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular dos dados é obrigado a fornecer os dados pessoais e as possíveis consequências do não fornecimento desses dados;
>
> a existência de tomada de decisão automatizada, incluindo criação de perfis, referida no artigo 22.º, n.ºs 1 e 4 e, pelo menos nesses casos, informações significativas sobre a lógica envolvida, bem como o significado e as consequências previstas de tal tratamento para o titular dos dados

Além disso, o nº 3 do art. 13 prevê que, caso o controlador queira utilizar os dados para fim diverso do original, deve informar ao titular.

O art.14 garante o direito de ser informado quando os dados não forem obtidos pelo titular de dados. Sendo assim, algumas das informações que devem ser dadas são: categorias dos dados pessoais em questão, identidade e dados de contato do responsável pelo tratamento e os fins do tratamento a que se dedicam os dados, bem como a base legal. Além disso, o nº 2 do artigo apresenta mais algumas informações que devem ser fornecidas ao titular, como o direito de retirar seu consentimento para o tratamento dos dados, o direito ao acesso, retificação, apagamento e portabilidade dos dados, bem como o período pelo qual esses dados serão armazenados.

Em sequência, o art. 15 discorre sobre o direito de acesso do titular e remonta muito aos arts. 12 e 14 previamente analisados. Assim se dá a redação do nº1 do art. 15:

> 1. O titular dos dados terá o direito de obter do responsável pelo tratamento a confirmação se os dados pessoais que lhe dizem respeito estão a ser processados e, se for o caso, o acesso aos dados pessoais e às seguintes informações:
>
> as finalidades do processamento;
>
> as categorias de dados pessoais em questão;
>
> os destinatários ou categorias de destinatários aos quais os dados pessoais foram ou serão divulgados, em particular destinatários em países terceiros ou organizações internacionais;
>
> sempre que possível, o período previsto de conservação dos dados pessoais ou, se não for possível, os critérios utilizados para determinar esse período;
>
> a existência do direito de solicitar ao responsável pelo tratamento a retificação ou o apagamento dos dados pessoais ou a restrição do tratamento dos dados pessoais relativos ao titular dos dados ou de se opor a esse tratamento;
>
> o direito de apresentar queixa a uma autoridade de supervisão;
>
> caso os dados pessoais não sejam recolhidos do titular dos dados, qualquer informação disponível quanto à sua fonte;
>
> a existência de tomada de decisão automatizada, incluindo criação de perfis, referida no artigo 22.º, n.ºs 1 e 4 e, pelo menos nesses casos, informações significativas sobre a lógica envolvida, bem como o significado e as consequências previstas de tal tratamento para o titular dos dados.

Ainda no art. 15, o nº 3 apresenta a possibilidade do titular receber uma cópia dos dados em tratamento, ficando facultada ao controlador a cobrança de uma taxa razoável baseada nos custos administrativos para quaisquer outros tipos de cópias solicitadas.

O art.16 conta somente com o caput que diz respeito ao direito de retificação dos dados, tal qual existe na LGPD, dos dados inexatos sobre sua pessoa. Aduz ainda o artigo que tendo em conta a finalidade do tratamento, o titular dos dados tem direito ao preenchimento incompleto dos dados.

Em continuidade ao exposto, o art.17 infere o direito ao esquecimento já conhecido no mundo jurídico. Esse direito garante ao titular poder solicitar que seus dados sejam apagados, se assemelhando em muito ao que diz a Legislação brasileira sobre anonimização em seu art.

Portanto, o apagamento dos dados pode ser solicitado quando: 1) os dados não forem mais necessários para os fins aos quais foram coletados ou de outra forma processados; 2) quando retirado o consentimento pelo titular; 3) quando houver oposição do titular ao tratamento e não havendo motivos imperiosos para o tratamento; 4) quando os dados pessoais tiverem sido processados ilegalmente; 5) quando houver obrigação legal que determine que os dados sejam

apagados; 6) quando os dados pessoais tiverem sido colhidos em relação à oferta de serviços da sociedade, em relação à crianças de, no mínimo 13 anos.

Em seu art.18, a GDPR trata sobre as restrições ao processamento que podem ser impostas ao controlador pelo titular. Sendo assim, as situações cabíveis de restrição são:

> O titular dos dados terá o direito de obter do controlador as restrições de processamento, quando se aplicar uma das seguintes opções:
>
> a exatidão dos dados pessoais é contestada pelo titular dos dados, por um período que permite ao controlador verificar a exatidão dos dados pessoais;
>
> o tratamento é ilegal e o titular dos dados opõe-se ao apagamento dos dados pessoais e solicita a restrição da sua utilização;
>
> o responsável pelo tratamento já não necessita dos dados pessoais para efeitos do tratamento, mas são exigidos pelo titular dos dados para o estabelecimento, exercício ou defesa de ações judiciais;
>
> o titular dos dados opôs-se ao tratamento nos termos do artigo 21.º, n.º 1, enquanto se aguarda a verificação de que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

O art.19 por sua vez determina a obrigação em informar sobre a retificação ou apagamento dos dados pessoais ou sobre a restrição de processamento. Dessa forma, os destinatários a quem os dados foram divulgados devem ser informados caso haja alguma das hipóteses previstas nos arts. 16, 17 ou 18, quais sejam, retificação, apagamento ou restrição de processamento dos dados.

Se aproximando do fim da parte de direitos dos titulares na GDPR temos o art.20 que aborda o tema da portabilidade de dados. Este direito garante ao titular a oportunidade de portar seus dados de um controlador para outro quando o trâmite for tecnicamente viável. Impende destacar que este processo se dará com o consentimento do titular e por meios automatizados.

O direito de objetar é apresentado nos 6 números do art.21, conferindo ao titular de dados a possibilidade de se opor ao tratamento de dados, salvo quando for necessário para cumprimento de tarefa de interesse público.

No art.22 estão colacionados os direitos de tomada de decisão individual automatizada. Esse tópico, refere-se, assim como a Lei Geral de Proteção de Dados em seu art. 20, às decisões realizadas por *machine learning* ou inteligências artificiais.

Assim determina o artigo:

> O titular dos dados tem o direito de não ser sujeito a uma decisão baseada exclusivamente no tratamento automatizado, incluindo a criação de perfis, que produza efeitos jurídicos a seu respeito ou o afete de forma semelhante.

O número 2 do mesmo artigo traz ainda as hipóteses de exceção, nas quais não serão admitidas o uso da decisão individual de não submissão às decisões de dados automatizados, quais sejam:

> O parágrafo 1 não se aplica se a decisão:
>
> é necessária para a celebração ou execução de um contrato entre o titular dos dados e um controlador de dados;
>
> está autorizado pela legislação da União ou dos Estados-Membros a que o responsável pelo tratamento está sujeito e que estabelece também as medidas adequadas para salvaguardar os direitos e liberdades e os interesses legítimos do titular dos dados; ou
>
> baseia-se no consentimento explícito do titular dos dados.

Por fim, o artigo 23 da GDPR colaciona as restrições que podem ser realizadas por normas da União ou do Estado-membro. Nesse sentido dispõe:

> A legislação da União ou do Estado-Membro a que o responsável pelo tratamento ou processador de dados está sujeito pode restringir, por meio de medida legislativa, o âmbito das obrigações e direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º, na medida em que as disposições correspondem aos direitos e obrigações previstos nos artigos 12 a 22, quando tal restrição respeita a essência dos direitos e liberdades fundamentais e é uma medida necessária e proporcional em uma sociedade democrática para salvaguardar:
> segurança nacional;
> defesa;
> segurança Pública;
> a prevenção, investigação, detecção ou repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública;
> outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo questões monetárias, orçamentais e fiscais, saúde pública e segurança social;
> a proteção da independência judicial e dos procedimentos judiciais;
> a prevenção, investigação, detecção e repressão de violações de ética para profissões regulamentadas;
> uma função de controlo, fiscalização ou regulação ligada, ainda que ocasionalmente, ao exercício da autoridade oficial nos casos referidos nas alíneas a) ae) eg);

a proteção do titular dos dados ou dos direitos e liberdades de terceiros;
a execução de ações de direito civil.
Em particular, qualquer medida legislativa referida no n.º 1 deve conter disposições específicas, pelo menos, se for caso disso, no que diz respeito a:
as finalidades do processamento ou categorias de processamento;
as categorias de dados pessoais;
o alcance das restrições introduzidas;
as salvaguardas para evitar o abuso ou acesso ou transferência ilegal;
a especificação do controlador ou categorias de controladores;
os períodos de armazenamento e as salvaguardas aplicáveis, tendo em conta a natureza, âmbito e objetivos do processamento ou categorias de processamento;
os riscos para os direitos e liberdades dos titulares dos dados; e
o direito das pessoas em causa de serem informadas sobre a restrição, a menos que isso possa ser prejudicial para a finalidade da restrição.
o direito das pessoas em causa de serem informadas sobre a restrição, a menos que isso possa ser prejudicial para a finalidade da restrição.

TABELA DE EQUIVALÊNCIA DOS ARTIGOS DA LGPD E GDPR

Princípio	LGPD	GDPR
Direito de acesso aos dados	Art. 18, II	Art. 15
Direito de retificação	Art. 18, III	Art. 16
Direito de eliminação	Art. 18, VI	Art. 17
Direito à portabilidade	Art. 18, V	Art. 20
Tomada de decisão individual automatizada	Art. 20	Art. 22

A única diferença visível no tema do direito do titular de dados é o prazo para fornecimento das cópias solicitadas por esse titular ao controlador. Enquanto na LGPD o prazo é de 15 dias, na GDPR o prazo é de 30 dias podendo ser prorrogado por mais 2 meses.

É notória que a GDPR é bem mais completa e profunda uma vez que, enquanto utiliza um artigo inteiro para tratar de cada assunto, a LGPD legisla em breves incisos, o que, pode ser prejudicial dada a ampla interpretação possível.

CASO CONCRETO

Como já mencionado, devido sua entrada em vigor em maio de 2018, a GDPR possui diversas jurisprudências que servem como norte para os futuros julgados da LGPD. A fim de ilustrar e exemplificar, será apresentado um caso concreto de Portugal para posterior análise de acordo com a LGPD.

DOS FATOS

Nos dias 3 e 16 de julho e 8 de agosto de 2018 o titular de dados solicitou à ré via email cópia das gravações das chamadas telefônicas que efetuou ao callcenter da ré, tendo recebido:

Chamada dos serviços da requerida para o titular dos dados efetuada em 29 de junho de 2018;

Chamada efetuada pelo titular dos dados para os serviços da requerida no dia 8 de agosto de 2018;

O autor não recebeu resposta escrita acerca de seus pedidos.

Posteriormente, o titular de dados foi contactado por telefone pelos serviços da empresa ré de quem recebeu informações de que as cópias solicitadas só poderiam ser fornecidas mediante decisão judicial.

Em 24 de agosto de 2018, o titular apresentou queixa à Comissão Nacional de Proteção de Dados relativo à negativa de fornecimento das cópias das gravações.

Em 22 de outubro de 2018 a empresa ré foi notificada pela CNPD para se manifestar acerca do ocorrido.

Em email recebido em 2 de novembro de 2018 a requerida, por meio de seu Encarregado de Proteção de Dados, informou que contratou uma outra empresa para prestação de serviços de callcenter, a qual atua em seu nome e em cumprimento de suas ordens. Além disso, informou que deu instruções à empresa de callcenter para que somente viabilizasse cópias das chamadas telefônicas "mediante ordem judicial ou pedido de alguma entidade ou organismo oficial, como o CNPD, órgão de polícia, etc.". Ainda informou que por suas ordens, a empresa só deveria manter a gravação das chamadas por 90 dias, e após, que fossem eliminadas. Sendo assim, as gravações solicitadas pelo autor já haviam sido eliminadas, exceto as gravações dos dias 8 e 24 de agosto e de 30 de outubro de 2018 que foram conservadas até ser proferida a decisão pela CNPD, tendo-as posteriormente facultadas ao autor em cumprimento à deliberação da CNPD nº1154/2018, de 18 de dezembro.

A ré sabia que deveria fornecer ao autor o acesso aos seus dados pessoais, bem como Às chamadas telefônicas por ele solicitadas, mediante cópia ou transcrição das mesmas.

A requerida atuou de forma livre, voluntária, consciente e sabendo que a sua conduta é proibida e punida por lei.

A DECISÃO

Pela Comissão Nacional de Proteção de Dados foi entendido que houve violação ao nº1 do art. 35 da Constituição da República Portuguesa, ao nº1 do art.15 da GDPR e do art, 83, nº5, alínea b) da GDPR. Sendo assim, a empresa ré foi condenada ao pagamento de multa no valor de €20.000,00 (vinte mil euros).

Atendo-se à matéria cerne do presente trabalho, qual seja o direito dos titulares de dados pessoais, o art. 15, nº1 da GDPR que fora violado no presente caso concreto diz respeito ao titular possuir o direito de ter acesso aos seus dados, bem como obter cópias que devem ser fornecidas pelo controlador.

No tocante à LGPD, o artigo aplicado à essa infração seria o art.18, II que aduz:

> Art18.O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> II - acesso aos dados; que é a cópia dos dados

A condenação estabelecida pela Comissão Nacional de Proteção de Dados baseou-se na própria GDPR que tem previsão em seu art.8, nº 5, de punição monetária limitada a

€20.000.000,00 (vinte milhões de euros), ou, no caso de empresas, a 4% do volume de negócios anual. A Lei Geral de Proteção de Dados prevê em seu art. 52, II, uma multa pecuniária à pessoa jurídica de direito privado o correspondente a 2% do seu faturamento no exercício anterior, limitada a R$50.000.000,00 (cinqüenta milhões de reais).

CONCLUSÃO

Dado todo o exposto, é possível notar as grandes semelhanças que cercam a Lei Geral de Proteção de Dados e a General Data Protection Regulation. Ambas as leis possuem conteúdo muito similar, ainda que a GDPR seja mais extensa e detalhada, a LGPD aborda muito bem também os direitos do titular de dados.

A exposição do caso concreto nos leva a analisar um pouco mais profundamente as leis trabalhadas, tendo em vista as diferenças existentes, é possível perceber que ambas seriam capazes de punir o réu.

Assim, com a recente entrada em vigor da LGPD, pode-se dizer que terá um grande efeito na sociedade pois, ao mesmo tempo em que visa garantir ao titular de dados uma maior proteção, fomenta o desenvolvimento tecnológico, econômico e a inovação.

REFERÊNCIAS:

“European General Data Protection Regulation”. ActiveMind.Legal, https://www.activemind.legal/legislation/gdpr/. Acessado em 2 de dezembro de 2020.

GDPR Enforcement Tracker - list of GDPR fines. https://www.enforcementtracker.com. Acessado em 2 de dezembro de 2020.

“General Data Protection Regulation (GDPR) – Official Legal Text”. General Data Protection Regulation (GDPR), https://gdpr-info.eu/. Acessado em 2 de dezembro de 2020.

L13709.http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acessado em 2 de dezembro de 2020.

https://www.cnpd.pt/home/decisoes/Delib/DEL_2019_21.pdf. Acessado em 2 de dezembro de 2020.

https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf. Acessado em 2 de dezembro de 2020.