Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito / Relações Internacionais

LUCA CISNEIROS GRADIM

ANÁLISE COMPARADA DA LEI GERAL DE PROTEÇÃO DE DADOS COM O REGULAMENTO EUROPEU SOBRE A PROTEÇÃO DE DADOS E A PROTEÇÃO DE DADOS NOS ESTADOS UNIDOS

BRASÍLIA
2020

LUCA CISNEIROS GRADIM

ANÁLISE COMPARADA DA LEI GERAL DE PROTEÇÃO DE DADOS COM O REGULAMENTO EUROPEU SOBRE A PROTEÇÃO DE DADOS E A PROTEÇÃO DE DADOS NOS ESTADOS UNIDOS

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito / Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Paulo Henrique Franco Palhares

BRASÍLIA
2020

LUCA CISNEIROS GRADIM

ANÁLISE COMPARADA DA LEI GERAL DE PROTEÇÃO DE DADOS COM O REGULAMENTO EUROPEU SOBRE A PROTEÇÃO DE DADOS E A PROTEÇÃO DE DADOS NOS ESTADOS UNIDOS

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito / Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Paulo Henrique Franco Palhares

BRASÍLIA, 27 DE SETEMBRO DE 2020

BANCA AVALIADORA

_____

Professor(a) Orientador(a)

_____

Professor(a) Avaliador(a)

AGRADECIMENTOS

Agradeço primeiramente a Deus pelo dom da vida, e à minha família por serem sua fundação, e por me ensinarem a ser uma pessoa melhor a cada dia. Agradeço ao meu professor orientador Paulo Palhares, que desde o início da pesquisa tem sido um excelente guia, e passado suas sugestões e correções com muita clareza, objetividade, e calma. Por fim, estendo meus agradecimentos ao professor Marlon Tomazette, e aos colegas e amigos Lucas Santos, Felipe Mattos, Henrique Bawden, e, em especial, ao amigo Thiago Moraes.

RESUMO

O presente trabalho acadêmico tem por objetivo analisar a Lei Geral de Proteção de Dados, diploma normativo que dispõe acerca das normas concernentes ao correto tratamento dos dados pessoais em âmbito nacional, comparando-o com as normas acerca da proteção de dados nos Estados Unidos da América, e com o Regulamento Geral sobre a Proteção de Dados, da União Europeia, que atualmente é o principal regulamento acerca da matéria.

Por meio dessa análise e comparação, a presente pesquisa se propõe a averiguar se a LGPD encontra-se apta a garantir aos titulares dos dados que recaem sob sua tutela a efetiva proteção contra o uso indevido de seus dados, e a submissão destes a tratamento irregular no contexto atual, onde o direito à privacidade e à proteção de dados representa um relevante desafio no âmbito jurídico.

Palavras-chave: privacidade. Proteção de dados. Lei Geral de Proteção de Dados. *General Data Protection Regulation*. *California Consumer Privacy Act*.

SUMÁRIO

INTRODUÇÃO

Nos dias de hoje, graças aos frequentes avanços do campo da tecnologia informacional, inúmeras operações são realizadas por meio eletrônico. Não apenas isso, mas os serviços oferecidos por meios virtuais já são tantos e tão importantes, que torna-se absurda a ideia de que exista algum indivíduo médio que não use nenhum aplicativo para fazer compras, ou não tenha conta em alguma rede social, ou que não se utilize, de alguma forma, de meios eletrônicos para realizar atividades cotidianas.

Todos esses serviços envolvem a troca e o tratamento de dados pessoais, pois estes são indispensáveis para que o que é proposto pelos fornecedores do serviço possam entregar o que é oferecido aos titulares dos dados. Justamente por isso, os dados pessoais passaram a ter alto valor no meio virtual, o que traz tanto a oportunidade de que sejam utilizados de forma indevida, como a necessidade de que sejam implementadas garantias aos seus titulares de que seus dados serão utilzziados apenas para fins lícitos e de forma segura. Essa garantia, logicamente, se concretiza por meio da criação de normas que rejam o tratamento dos dados, e disponham acerca dos direitos de quem os detêm e das obrigações de quem os maneja.

Diante desse cenário, países de todo o mundo têm posto de forma relevante em suas pautas a criação de leis e regulamentos que possam garantir aos seus cidadãos a proteção de sua privacidade e de seus dados pessoais. Nesse sentido, a presente pesquisa realiza um breve histórico de casos importantes para a história da tutela dos direitos dos titulares de dados no meio eletrônico, e posteriormente expõe e analisa os principais pontos do *General Data Protection Regulation*, o regulamento que dispõe acerca da proteção de dados na União Europeia, que é o principal diploma normativo a tratar de forma ostensiva e clara sobre o assunto. Após isso, é analisada e posta em comparação a Lei Geral de Proteção de Dados, que é a lei que dispõe acerca da proteção de dados pessoais em âmbito nacional. Por fim, é discutida a proteção de dados no âmbito dos Estados Unidos, e posta em comparação com as normas já apresentadas e discutidas.

Faz-se relevante tal discussão vez que a garantia da privacidade e da proteção de dados pessoais, no contexto atual, representa um dos maiores desafios jurídicos não só para o Brasil, mas também a nível internacional. Nesse contexto, Lei Geral de Proteção de Dados é muito recente, e cabe análise e comparação com outros diplomas normativos importantes acerca do assunto, para que se possa saber se a Lei nacional será ou não efetiva contra os desafios apresentados pelo contexto contemporâneo, onde a tecnologia da informação sofre avanços cada vez mais notáveis e com cada vez mais frequência.

1. BREVE HISTÓRICO DE PROTEÇÃO DE DADOS NO ÂMBITO INTERNACIONAL

No contexto em que vivemos, onde as plataformas digitais passaram a ser o padrão para interações de diversas naturezas, seja entre pessoas físicas, jurídicas, ou dos dois tipos entre si, a coleta e utilização de dados pessoais vem sendo cada vez mais comum, ao ponto em que tornou-se inviável a plena convivência em sociedade sem que haja esse compartilhamento.

E embora a questão da coleta, processamento, e acesso de dados pessoais tenha ganho visibilidade no Brasil por volta de 2010, ano no qual surgiu o anteprojeto da Lei de Proteção de Dados, esse tópico é objeto de interesse jurídico e político no âmbito internacional há tempos. Já na década de 1960, a possível criação de um banco unificado de armazenamento de dados gerou uma importante discussão política, nos Estados Unidos, que ficou conhecido como o caso do *National Data Center*. Ademais, no ano de 1970, no estado de Hesse, Alemanha, surgiu a primeira lei estadual acerca da proteção de dados pessoais, e, poucos anos depois, sobreveio no mesmo país a primeira lei federal versando sobre o assunto. Representa um marco de notável relevância, ainda, a decisão da Corte Constitucional da Alemanha, que teve papel importante no aperfeiçoamento da lei federal acerca da proteção de dados pessoais.

Posto isso, antes de adentrar na história da proteção de dados pessoais, cabe definir bem o que são os "dados", e porque há importância em sua proteção jurídica, e uma boa forma de fazê-lo é pondo em comparação os termos "dado" e "informação". O primeiro apresenta uma conotação mais primitiva e fragmentada do que o último. Ou seja, representa uma informação em potencial, antes de ser transmitida[1]. A informação, por sua vez, é o resultado que sem tem ao serem processados os dados, de modo que a matéria prima recebeu o devido tratamento, tornando-se o produto final. Vez que a coleta e tratamento de dados é o que nos leva às informações, e que, como dito anteriormente, o uso e compartilhamento de dados está cada vez mais intimamente relacionado aos mais diversos aspectos da vida cotidiana, maior se tornam sua utilidade e relevância, a ponto desses dados passarem a ser objeto de interesse do governo, e até mesmo de entes privados atuantes no mercado.

E, surgindo essa relevância e consequente interesse, passa também a existir a possibilidade de abuso desses dados, seja esse abuso na forma em que são coletados, como é

[1] DONEDA, DANILO. **Da privacidade à proteção de dados pessoais**, Rio de Janeiro. Editora Renovar. 2006. P. 152.

feito seu processamento, ou para quais fins serão utilizados. Daí a importância de tutela jurídica sobre os dados e informações, ainda mais no contexto cada vez mais informatizado e tecnológico em que vivemos. A essa tutela se dá o nome de "proteção de dados".

Logo, a proteção de dados no âmbito digital consiste na proteção dos dados pessoais, que podem ser coletados, armazenados, usados, e propagados online[2]. Feita essa necessária introdução, passamos aos casos que foram importantes para a criação e aperfeiçoamento dessa área que hoje possui grande relevância jurídica no Brasil.

1.1 O CASO DO *NATIONAL DATA CENTER*

O caso do *National Data Center* é importante para a história da tutela jurídica dos dados pessoais, tendo em vista que foi a primeira vez em que foi posto a debate, em um nível político significativo, o uso da tecnologia de informação para o armazenamento e processamento de dados. No ano de 1965, nos Estados Unidos, foi feita uma proposta ao *Bureau of Budget*, pelo *Social Science Research Council*, recomendando a criação de uma base de dados unificada, vez que a existência de diversos bancos de dados pelo país, que era o caso na época, consistia em uma alternativa menos eficiente de utilização dos dados, tanto pelas agências federais, quanto pelas organizações que não integravam o Estado[3]. A esse banco de dados seria dado o nome de *National Data Center*.

Por representar uma alternativa que aumentaria consideravelmente a eficiência da estrutura administrativa do país, a criação do *National Data Center* foi endossada pelo governo norte-americano. No entanto, embora a centralização do conteúdo dos diversos bancos de dados representasse um avanço significativo tanto para o governo quanto para pesquisadores, grande parte da população estadunidense se mostrou contra a concentração massiva de dados pessoais de indivíduos e o acesso a esse conteúdo por meio de uma só plataforma[4].

Com a ebulição desse debate envolvendo a opinião da comunidade científica e a opinião pública, foram realizadas diversas audiências pelo congresso norte-americano, a fim de destrinchar as questões atreladas à criação do *National Data Center*, e as implicações que o banco traria na vida dos norte-americanos. O congresso norte-americano acabou por não apoiar

---

[2] UNESCO, **Keynotes to Foster Inclusive Knowledge Societies: Access to Information and Knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet, United Nations Education, Scientific and Cultural Organization**. 2015. p. 56.

[3] SEAN CAWLEY. **The National Data Center and the Federal Information Network: A Paradox**. College of Arts and Science, Vanderbilt University, EUA. Volume 10. 2015.

[4] REBECCA S. KRAUS. **Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants**. EUA. 2011.

a iniciativa, temendo pela possibilidade do uso indevido dos dados, e recomendou que nada fosse feito para estabelecer uma plataforma de tal natureza sem que "a proteção da privacidade seja observada e garantida ao máximo nível possível para os cidadãos de cujas informações pessoais seja formado o banco de dados"[5].

Embora do intenso debate acerca do *National Data Center* não tenha sobrevindo nenhuma lei, ou sequer medida judicial, este foi o estopim para o debate acerca da necessidade de proteção da privacidade de dados pessoais no mundo.

1.2 O CENSO DE 1983 E A DECISÃO DA CORTE CONSTITUCIONAL DA ALEMANHA

Apesar de o caso do *National Data Center*, no ano de 1965, ter tido repercussões restritas ao âmbito político, a realização de um censo na Alemanha, anos depois, teve fortes consequências jurídicas no âmbito da proteção de dados. Como dito anteriormente, o primeiro marco legislativo acerca da proteção de dados ocorreu no estado de Hesse, na Alemanha, no ano de 1970. Embora o Ato de Proteção de Dados de Hesse tenha sido apenas uma lei estadual, outros estados alemães passaram a legislar sobre o assunto, e, poucos anos depois, sobreveio a primeira lei federal que tratava sobre a proteção de dados na Alemanha[6].

Dentro desse contexto, o governo alemão pretendia realizar um censo, o que se daria por meio da colheita de dados dos cidadãos, e posterior processamento eletrônico desse conteúdo. Ocorreu, no entanto, que surgiu certa desconfiança em diversos setores da sociedade alemã na época, tanto em relação ao método utilizado para a coleta de dados, quanto ao fim para o qual serviriam[7].

Dentre os pontos que fomentaram o ceticismo dos alemães, podemos contar: "a possibilidade de que os dados obtidos pelo censo fossem confrontados com os dados do registro civil para uma eventual retificação do próprio registro; a possibilidade destes mesmos dados, desde que não identificados com o nome de cada titular, poderem ser transmitidos às

---

[5] *The Computer and Invasion of Privacy*: Hearings Before a Subcommittee of the Committee on Government Operations, House of Representatives. U.S. Government Printing Office: Washington, 1966, p. 6.

[6] STEPANOVA, O., GROOTHUIS, F. **The privacy, data protection and cybersecurity law review**. 6 edição. 2019. Disponível em: https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210039/germany. Acesso em: 27 de maio de 2020.

[7] DONEDA, DANILO. **Da privacidade à proteção de dados pessoais**, Rio de Janeiro. Editora Renovar. 2006. P. 192.

autoridades federais e aos *Länder*[8]; a existência de uma multa pecuniária, relativamente elevada, para os que não respondessem, bem como um mecanismo de favorecimento àqueles que denunciassem tais pessoas."[9] Logo, junto a esses pontos presentes na lei que organizava o censo, sobreveio a preocupação de que os dados nele obtidos, que a princípio cumpririam finalidade meramente estatística, poderiam ser utilizados para fins administrativos (e.g. a já citada possibilidade de retificação do registro civil por meio do uso de dados obtidos pelo censo)[10].

Esses eventos motivaram numerosas reclamações à Corte Constitucional alemã, que eventualmente proferiu sentença suspendendo provisoriamente o censo, e declarando que a lei que o instituía era inconstitucional em relação a artigos da Lei Fundamental[11] que versavam acerca do direito geral da personalidade. Como consequência dessa decisão, foi promulgada, em 1985, uma nova lei, que instituía um novo censo, com a correção dos pontos que foram contestados. No novo censo, "os dados coletados para fins estatísticos eram separados das informações individuadas; o cidadão era cuidadosamente informado sobre as finalidades da coleta de dados e sobre sua obrigação de fornecê-las; a transferência de dados pessoas entre autoridades federais e regionais foi simplesmente vetada, entre diversas outras disposições"[12].

Cumpre destacar, ainda, três pontos que decorreram da sentença proferida, vez que são relevantes para a história da proteção de dados no mundo jurídico. O primeiro deles é o reconhecimento de que o estágio de desenvolvimento da tecnologia informática utilizada no processamento das informações recolhidas era um fator determinante a ser levado em conta[13]. Isso quer dizer que, o crescente avanço das tecnologias de informação era o que criava a possibilidade de que os dados colhidos no censo pudessem vir a causar danos aos indivíduos que os forneceram. O verdadeiro perigo, na verdade, não estava no ato de colher os dados, mas sim no seu processamento.

Por meio da tecnologia, seria viável o processamento dos dados e utilização das informações obtidas de forma discricionária pelo Estado, em uma capacidade quase ilimitada.

---

[8] A tradução de *länder* para o português é "país". Ou seja, o governo alemão poderia vir a compartilhar os dados processados com outros países.

[9] DONEDA, DANILO. **Da privacidade à proteção de dados pessoais**, Rio de Janeiro. Editora Renovar. 2006. P. 193.

[10] DONEDA, DANILO. **Da privacidade à proteção de dados pessoais**, Rio de Janeiro. Editora Renovar. 2006. P. 194

[11] A Lei Fundamental da Alemanha é o equivalente à nossa Constituição Federal, ou seja, o diploma normativo da mais alta hierarquia.

[12] DONEDA, DANILO. **Da privacidade à proteção de dados pessoais**, Rio de Janeiro. Editora Renovar. 2006. P. 196

[13] DONEDA, DANILO. **Da privacidade à proteção de dados pessoais**, Rio de Janeiro. Editora Renovar. 2006. P. 195

Como já dito, haveria inclusive a possibilidade de cruzamento com outras bases de dados estaduais e federais, o que aumentaria ainda mais o leque de possibilidades de como o estado poderia usar as informações obtidas. Daí podemos concluir que, quanto mais avançada a tecnologia, maior deve ser o cuidado com sua utilização, e mais sofisticados devem ser os mecanismos (inclusive jurídicos) que visam proteger os indivíduos de um potencial abuso dessa tecnologia.

O segundo ponto é a "desmistificação da noção de que o tratamento de certos tipos de dados pessoais seria irrelevante para a privacidade"[14]. Ou seja, não há nenhum tipo de dado que não seja importante, devendo todo tipo de dado receber a devida proteção. Essa questão da relevância dos dados está intimamente relacionada ao ponto anterior, vez que é o avançado estágio no qual se encontra a tecnologia da informação que permite que qualquer dado, aparentemente desimportante, torne-se relevante para determinada finalidade após receber o devido processamento.

Outrossim, nos termos da própria sentença proferida pela Corte Constitucional alemã: "não se pode levar em consideração apenas a natureza das informações; são determinantes, porém, a sua necessidade e utilização. Estas dependem em parte da finalidade para a qual a coleta de dados é destinada, e de outra parte, da possibilidade de elaboração e de conexão próprias da tecnologia da informação. Nesta situação, um dado que, em si, não aparenta possuir nenhuma importância, pode adquirir um novo valor; portanto, nas atuais condições do processamento automático de dados, não existe mais um dado 'sem importância'"[15].

O terceiro ponto é a "solidificação de um entendimento segundo o qual a proteção de dados pessoais requer um embasamento constitucional direto"[16]. Isso pois, não nos esqueçamos, o que impediu a realização do censo foi a incompatibilidade entre a lei que o autorizava e a Lei Fundamental.

Cumpre ressaltar, ainda, que os artigos da Lei Fundamental com os quais a lei original do censo eram incompatíveis eram artigos que serviam como "a base sobra a qual se estrutura o direito geral da personalidade"[17]. Logo, vemos que a privacidade dos dados pessoais faz parte do pleno exercício do direito da personalidade. Dessa forma, havendo proteção constitucional da personalidade, tem-se como consequência a tutela da proteção de dados.

---

[14] Idem.
[15] Idem.
[16] DONEDA, DANILO. **Da privacidade à proteção de dados pessoais**, Rio de Janeiro. Editora Renovar. 2006. P. 197
[17] DONEDA, DANILO. **Da privacidade à proteção de dados pessoais**, Rio de Janeiro. Editora Renovar. 2006. P. 194

Observa-se, então, que o a sentença proferida pela Corte Constitucional alemã serve como o primeiro importante marco na história da proteção de dados no âmbito jurídico.

1.3 A CONVENÇÃO Nº 108 DO CONSELHO DA EUROPA E O *DATA PROTECTION DIRECTIVE* DE 1995

Acerca da proteção de dados no âmbito da União Europeia, há de se observar que, em que pese a preocupação e pioneirismo de países como a Alemanha, Suécia, e França na legislação acerca da proteção de dados[18], surgiu a necessidade de legislar sobre o tema no âmbito supranacional, de forma que fosse promovida harmonização da matéria para todos os países-membros. Isso porque, ainda que as regras acerca da proteção de dados fossem similares em alguns países, problemas inevitavelmente surgiram no que tangia às leis em si, bem como em relação à aplicação dessas leis na prática[19].

No âmbito de um mercado interno complexo como o da União Europeia, para que houvesse a livre movimentação de bens, capital, serviços e pessoas, era necessária também que houvesse movimentação de dados, o que não poderia ser realizado sem que houvesse a uniformização da proteção desses dados entre os estados-membros[20].

Com esse fim, a Convenção nº 108 do Conselho da Europa foi o primeiro documento vinculante a nível internacional visando a harmonização das regras pertinentes à proteção de dados na União Europeia. Além de servir como exemplo de cooperação internacional para a solução de um notável desafio jurídico, a Convenção nº 108 representa importante marco na história da tutela de direitos relativos a dados pessoais e seu processamento. O documento uniformizou a nível internacional, por exemplo, requisitos a serem observados no processamento de dados[21], os direitos de indivíduos que têm seus dados processados[22],

---

[18] Além do já citado exemplo da Alemanha, na Suécia foi criada a *Datalagen*, em 1973, e a França adotou a *Loi relatif a l'informatique, aux fichiers et aux libertés*, no ano de 1977.

[19] UNIÃO EUROPEIA. **Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. European Treaty Series – No 108. Strasbourg, 1981. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434. Acesso em: 06 de junho de 2020.

[20] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, COUNCIL OF EUROPE. **Handbook on european data protection law**. Imprimerie Centrale. Luxemburgo. 2018. P. 29

[21] UNIÃO EUROPEIA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. 1981. Capítulo II, art. 5. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37. Acesso em: 06 de junho de 2020.

[22] UNIÃO EUROPEIA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. 1981. Capítulo II, art. 8. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37. Acesso em: 06 de junho de 2020.

exceções ao direito da proteção de dados[23], e mecanismos de cooperação entre países-membros para fins de cumprimento das normas contidas na Convenção[24].

Outro ponto merecedor de destaque é o Art. 11 do Capítulo II da Convenção, que dispõe que nenhuma das provisões presentes no documento devem ser interpretadas como limitantes, ou de modo a impedir que estados-membros aumentem a proteção dada aos indivíduos a quem os dados se referem[25]. Ou seja, a Convenção estabeleceu regras mínimas a erem seguidas. No entanto, em que pese a notável importância que a Convenção nº 108 teve na questão da uniformização legislativa, bem como a imposição de direitos, deveres, exceções à proteção de dados, e princípios a serem observados, era necessário que se criasse um sistema mais detalhado e compreensivo às particularidades do crescente avanço na tecnologia da informação.

Sobreveio, então, no ano de 1995, o *Data Protection Directive* (DPD), que além de refletir os princípios contidos na Convenção nº 108 do Conselho da Europa, os expandiu, aprimorando a tutela dos direitos relativos à proteção de dados[26]. O DPD aproveitou a possibilidade criada pelo Capítulo II, art. 11 da Convenção, e trouxe novos instrumentos de proteção. Além disso, foi um texto mais sofisticado acerca do assunto. O documento trouxe, por exemplo, critérios mais específicos para que o processamento de dados seja considerado legítimo[27], informações a serem dadas para indivíduos aos quais os dados se referem[28]. Entretanto, pela União Europeia se tratar de uma espécie de coligação de países que a formam, a legislação internacional deve ser observada, principalmente em uma situação como a descrita, cujo objetivo é a uniformização da legislação de diversos países para seguir um só molde. Ademais, apesar de ser uma solução mais sofisticada, como se buscava à época, por se tratar de uma diretiva, o *Data Protection Directive* não poderia ser aplicado diretamente, e deveria ser

---

[23] UNIÃO EUROPEIA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. 1981. Capítulo II, art. 9. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37. Acesso em: 06 de junho de 2020.

[24] UNIÃO EUROPEIA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. 1981. Capítulo IV. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37. Acesso em: 06 de junho de 2020.

[25] UNIÃO EUROPEIA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. 1981. Capítulo II, art. 11. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37. Acesso em: 06 de junho de 2020.

[26] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, COUNCIL OF EUROPE. **Handbook on european data protection law**. Imprimerie Centrale. Luxemburgo. 2018. P. 29.

[27] UNIÃO EUROPEIA. **Directive 95/46/EC of the european parliament and of the council – Data Protection Directive**. 1995. Capítulo II, seção II, art. 7. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5. Acesso em: 06 de junho de 2020.

[28] UNIÃO EUROPEIA. **Directive 95/46/EC of the european parliament and of the council – Data Protection Directive**. 1995. Capítulo II, seção IV. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5. Acesso em: 06 de junho de 2020.

transposto nas legislações nacionais de cada estado-membro, como dita o sistema jurídico da União Europeia[29].

Devido a essa questão, diversos países-membros da União Europeia acabaram por transcrever as normas da diretiva de uma forma diferente ao longo dos anos, restando frustrada a tentativa de se atingir uma harmonização completa da legislação acerca do tema. Além disso, deve ser levado em conta o crescente avanço no campo da tecnologia da informação que ocorreu na época, o que proporcionava o processamento cada vez mais veloz e sofisticado de dados pessoais. A junção das diversas interpretações que os países tiveram do conteúdo do DPD com a evolução tecnológica que se deu na época fez surgir a necessidade de mais uma reforma na legislação acerca da proteção de dados no âmbito da União Europeia.

Chegamos, finalmente, então, ao diploma normativo que é utilizado nos dias atuais, o chamado *General Data Protection Regulation*, que será analisado mais detalhadamente a seguir.

2. PRINCIPAIS ASPECTOS DA PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA – GENERAL DATA PROTECTION REGULATION (GDPR) E NOS ESTADOS UNIDOS

Tendo em vista o crescente avanço da tecnologia da informação, faz-se necessário um mecanismo mais sofisticado para tratar de questões acerca da proteção de dados. Para cumprir esse papel surgiu a GDPR, que é composta de 99 artigos e 173 enunciados. Na GDPR, são considerados pessoais os dados relacionados a uma pessoa identificada ou identificável. O que vem a tornar alguém identificável, segundo o diploma normativo, é a possibilidade daquele dado poder levar, direta ou indiretamente, à identificação do indivíduo[30]. Faz-se clara aqui a grande amplitude do conceito. Além de dados óbvios como o nome e sobrenome, endereço, data e local de nascimento, o regulamento cobre também dados eletrônicos como cookies, arquivos computadorizados, e outros elementos armazenados por meio de ferramentas de vigilância de tráfego na internet[31].Além disso, para o regulamento, a "esfera pessoal" do indivíduo engloba não só dados relacionados à sua vida privada, como também aspectos de sua

[29] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, COUNCIL OF EUROPE. **Handbook on european data protection law**. Imprimerie Centrale. Luxemburgo. 2018. P. 30.
[30] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 4, (1).
[31] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, COUNCIL OF EUROPE. **Handbook on european data protection law**. Imprimerie Centrale. Luxemburgo. 2018. P. 89.

vida pública, bem como profissional, entendimento sedimentado pelo Tribunal Europeu dos Direitos Humanos[32].

Tendo em vista a vastidão de elementos englobados pelo conceito de dados pessoais dentro da GDPR, principalmente no que concerne à quantidade de dados que tornam um indivíduo identificável (ou seja, os dados que podem levar à identificação de uma pessoa), o próprio regulamento diz que deve ser levada em consideração a tecnologia disponível no momento do processamento[33]. De fato, o crescente avanço tecnológico permite não apenas novas e mais eficientes formas de se processarem dados, como também novos tipos de dados, como por exemplo impressão digital, reconhecimento de íris, de voz, que são cada vez mais utilizados para se identificar indivíduos nos mais diversos contextos. Ressalta-se, no entanto, que para a GDPR, a tecnologia disponível para o processamento não precisa ser detida por quem coleta ou armazena os dados, basta que esses dados possam, por meio dessa tecnologia, levarem à identificação do indivíduo. Em outras palavras, importa para a legislação se é provável que esses meios de identificação (isto é, a tecnologia) estarão disponíveis e serão utilizados, ainda que por terceiros, em um futuro previsível[34]. Nesse sentido, dita o enunciado 26 da GDPR, que para "averiguar se há probabilidade razoável de que os meios sejam utilizados para identificar a pessoa física, devem ser levados em conta todos os fatores objetivos, como o custo e tempo necessários para a identificação, levando em consideração a tecnologia disponível no momento do processamento".

Por fim, dentro dos dados pessoais, há categorias especiais que necessitam de maior proteção, pela própria natureza dos dados, vez que seu processamento, ainda que realizado da forma devida, pode apresentar um risco para os sujeitos aos quais os dados se referem. Estes estão elencados no art. 9 da GDPR, e são: *a)* dados pessoais que revelem raça ou origem étnica; *b)* dados pessoais que revelam opiniões políticas, religião ou outras crenças, incluindo crenças filosóficas; *c)* dados que revelem filiações a sindicatos; *d)* dados genéticos e biométricos processados com o fim de identificar um indivíduo; *e)* dados pessoais acerca dsaúde, atividade sexual, e orientação sexual.

2.1 PRINCÍPIOS PRESENTES NA GDPR

[32] No caso *Amann v. Switzerland*, No. 27798/95, 16 de fevereiro de 2000, no §65 da decisão, o Tribunal dita que "não há razão para justificar a exclusão de atividades de natureza profissional, ou de negócios, da noção de 'vida privada'".
[33] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Enunciado 26.
[34] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Enunciado 26.

No artigo 5 do regulamento, são elencados os princípios que regem o processamento de dados pessoais. Por representarem as regras fundamentais a serem levadas em conta quando da realização dessa atividade, faz-se imprescindível que sejam estudados na presente pesquisa.

2.1.1 PRINCÍPIOS DA LEGALIDADE, FAIRNESS E TRANSPARÊNCIA DO PROCESSAMENTO DE DADOS

O artigo 5 (1) (a) do regulamento dita que os dados pessoais devem ser processados dentro de forma legal, justa e transparente com relação ao indivíduo aos quais os dados dizem respeito.

No que diz respeito à legalidade, isso quer dizer que deve haver fundamento legal para que os dados sejam processados. Esses fundamentos estão presentes no artigo 6 (1) do regulamento, e são: *a)* o consentimento do titular dos dados, *b)* quando o processamento dos dados for necessário para cumprimento de um contrato do qual o titular dos dados for parte, *c)* quando o processamento dos dados for necessário para o cumprimento de obrigação legal à qual o controlador estiver submetido; *d)* se necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa natural; *e)* para os fins de interesse público ou para o exercício de dever oficial do qual o controlador é incumbido; *f)* o processamento for necessário para a satisfação de interesse legítimo do controlador ou de terceiros. Nesta última hipótese, não deverá haver processamento se o titular tiver direitos que só poderão ser garantidos com o não processamento dos dados, principalmente se o titular for menor de idade[35].

A *fairness*, ou justeza do processamento, está intimamente relacionada ao princípio da legalidade e da transparência. Não foi à toa que os três princípios foram colocados juntos no diploma normativo. Segundo este em específico, os controladores devem notificar os titulares dos dados e o público em geral de que os dados serão processados respeitando os devidos princípios. Ademais, devem os controladores se encontrarem aptos a demonstrar que suas operações de processamento estão em conformidade com a GDPR[36].

O princípio da transparência, por sua vez, dita que os controladores devem tomar medidas de modo a manter os titulares dos dados cientes de como estes estão sendo utilizados, de forma concisa, transparente, e em linguagem clara e simples[37]. A transparência deve ser

[35] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 6 (1).
[36] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, COUNCIL OF EUROPE. **Handbook on european data protection law**. Imprimerie Centrale. Luxemburgo. 2018. P. 118.
[37] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 12 (1).

aplicada de forma ampla, devendo as informações necessárias estarem disponíveis para o titular, ou até mesmo que este seja informado diretamente, seja em momento anterior ao início do processamento dos dados[38], durante o seu processamento, ou após. Os titulares devem ser informados acerca do propósito para o qual seus dados serão processados no momento de sua coleta, por exemplo, quais procedimentos serão utilizados no processamento dos dados, bem como as ferramentas de proteção dos dados, e os riscos envolvidos no processo[39].

Em suma, o princípio da transparência vincula os controladores a comunicarem aos titulares dos dados todas as informações relevantes ao processamento dos dados, bem como os seus direitos, de forma clara, e permitir o acesso dos titulares a seus dados.

2.1.2 PRINCÍPIO DA DELIMITAÇÃO DE PROPÓSITO DO PROCESSAMENTO DE DADOS

De acordo com o princípio da delimitação de propósito do processamento, os fins que se visam alcançar com o processamento dos dados em questão devem ser definidos antes que este seja realizado. Outrossim, se o propósito do processamento dos dados está delineado de forma específica e clara o bastante, os envolvidos no processo sabem o que esperar, e o grau de transparência e legalidade aumentam consideravelmente[40]. Ou seja, não é permitido que haja processamento de dados sem um fim específico, de forma que a legitimidade do processamento depende diretamente da existência de um propósito explícito, específico, e legítimo[41].

Há ainda outro aspecto importante a ser observado, que é a relação guardada com o princípio da legalidade. Como já foi apontado, faz-se necessário um fundamento legal para que seja realizado o processamento de dados pessoais. Dessa forma, se algum controlador que, dentro dos conformes legais, e com um propósito específico, processa os dados pessoais de alguém, e então pretende realizar processamento posterior dos mesmos dados, mas para um propósito diferente, deve obter novamente fundamento legal (por exemplo, obter novamente o consentimento dos titulares dos dados).

Em resumo, segundo o regulamento, os dados que foram processados com base em um propósito específico e com o devido respaldo legal, não poderão passar por processamento

---

[38] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Arts. 13 e 14.
[39] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Enunciado 39.
[40] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, COUNCIL OF EUROPE. **Handbook on european data protection law**. Imprimerie Centrale. Luxemburgo. 2018. P. 122.
[41] Idem.

posterior para propósito incompatível com o original[42]. Seria necessário, para tanto, novo fundamento legal. Por consequência, tem-se a possibilidade de processamento posterior, desde que para um novo propósito que seja compatível com o original. O diploma normativo cita, inclusive, propósitos que seriam, a princípio, considerados compatíveis, como o arquivamento dos dados por motivos de interesse público, pesquisa científica ou histórica, e ainda por motivos de estatística, desde que, em qualquer dessas hipóteses, sejam implementadas ferramentas visando salvaguardar os direitos dos titulares dos dados[43].

O regulamento aponta, ainda, alguns pontos específicos aos quais o controlador deve atentar-se quando se encontrar na situação de análise de compatibilidade do posterior processamento. Por exemplo, deve-se levar em conta "qualquer ligação entre os propósitos originais e os propósitos do processamento posterior; o contexto no qual os dados pessoais foram coletados, em particular no que concerne às expectativas razoáveis dos titulares com base no seu relacionamento com o controlador; a natureza dos dados pessoais; as consequências que o processamento posterior terá para os titulares; e a existência de salvaguardas tanto nas operações de processamento originais quanto nas que se pretendem realizar"[44].

Por fim, o regulamento coloca a possibilidade de processamento posterior, ainda que não haja compatibilidade entre o propósito original e novo propósito, se essa continuidade de processamento for "uma medida necessária e proporcional visando defender importantes objetivos de interesse público"[45], desde que tenha havido consentimento dos titulares (o que é um fundamento legal), ou lei do estado-membro nesse sentido.

2.1.3 PRINCÍPIO DA MINIMIZAÇÃO DE DADOS

Intimamente relacionado com o princípio da delimitação de propósito do processamento, o presente princípio dita que devem ser processados apenas os dados necessários para a satisfação do objetivo delineado. Ou seja, deve haver a limitação de dados visando o cumprimento do propósito previamente delimitado, e nada além disso.

Nos termos do regulamento, os dados processados devem ser "adequados, relevantes e limitados ao que for necessário em relação aos propósitos para os quais serão processados"[46].

---

[42] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 5 (1) (b).
[43] Idem.
[44] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Enunciado 50.
[45] Idem.
[46] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 5 (1) (c)

Desse princípio podemos então depreender que, só deve haver o processamento de dados pessoais quando não for possível alcançar o objetivo almejado por outros meios[47].

2.1.4 PRINCÍPIO DA EXATIDÃO DE DADOS

Segundo o princípio da exatidão de dados, os dados processados devem ser fiéis à realidade, ou seja, devem estar alinhados à verdade dos fatos. Dessa forma, a depender da natureza dos dados, o status de uma situação pode mudar, o que torna necessária a retificação dos dados a ela relacionados. Outrossim, para a satisfação desse princípio, faz-se necessária a checagem periódica de determinados dados.

Clássico exemplo disso é quando há inscrição equivocada de alguém no serviço de proteção ao crédito. Enquanto permanecer a inscrição desse indivíduo no cadastro negativo, determinados negócios jurídicos (como por exemplo a realização de um empréstimo com uma instituição financeira) se tornarão inviáveis. Faz-se clara, portanto, a importância na exatidão dos dados, de modo que dados que não refletem a realidade devem ser apagados ou corrigidos imediatamente[48].

Para os fins de manutenção da exatidão dos dados, é importante que os mesmos sejam checados regularmente pelos controladores e operadores, bem como é imprescindível que seja dado aos titulares o fácil acesso aos seus dados, a fim de verificar se estes refletem a realidade dos fatos[49].

2.1.5 PRINCÍPIO DA LIMITAÇÃO DO ARMAZENAMENTO DE DADOS

Nos termos do artigo 5 (1) (e) da GDPR, os dados processados não devem permanecer em um estado que permita a identificação dos titulares por tempo maior do que for necessário para cumprir o propósito para o qual foram processados. Em outras palavras, os dados devem ser eliminados ou anonimizados quando tiverem cumprido seu propósito em relação ao seu processamento.

---

[47] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, COUNCIL OF EUROPE. **Handbook on european data protection law**. Imprimerie Centrale. Luxemburgo. 2018. P. 125.
[48] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, COUNCIL OF EUROPE. **Handbook on european data protection law**. Imprimerie Centrale. Luxemburgo. 2018. P. 127.
[49] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, COUNCIL OF EUROPE. **Handbook on european data protection law**. Imprimerie Centrale. Luxemburgo. 2018. P. 128.

O próprio diploma normativo aponta, ainda, que, "a fim de garantir que os dados pessoais não sejam mantidos por mais tempo que o necessário, deve haver fixação de prazo para eliminação dos dados, ou para realização de uma revisão periódica"[50], com a finalidade de averiguar a necessidade (ou inexistência desta) de que os dados sejam mantidos.

Por fim, de forma similar como é feita ao princípio da delimitação de propósito do processamento de dados, é permitido que os dados sejam armazenados por período maior do que o necessário, desde que o processamento ao qual será submetido tenha fins relevantes ao interesse público, ou para fins de pesquisa histórica ou científica, desde que sejam implementadas medidas a fim de salvaguardar os direitos dos titulares dos dados[51].

Nos termos da lei, as medidas implementadas podem ser de natureza técnica ou organizacional, mas sua implementação é indispensável.

2.1.6 PRINCÍPIO DA INTEGRIDADE E CONFIDENCIALIDADE DOS DADOS

Tratando-se de proteção de dados, aspectos como a segurança e confidencialidade dos dados são indispensáveis para garantir que os direitos dos titulares dos dados não sejam violados. Com o objetivo de assegurar essa proteção, dita o princípio da integridade e confidencialidade dos dados, que devem ser implementadas medidas técnicas ou organizacionais de modo a impedir processamento não autorizado ou ilegal, bem como a perda dos dados, sua destruição, ou dano[52]. Segundo o regulamento, tanto o controlador quanto o operador devem levar em conta "o nível da tecnologia envolvendo o processamento dos dados, seu custo de implementação, bem como sua natureza, margem, contexto e seus propósitos"[53]. Também devem ser levados em conta os riscos aos direitos e liberdades dos titulares dos dados, incluindo a probabilidade de violação desses direitos e a severidade dessa possível violação[54].

Exemplos de medidas de segurança citados pelo regulamento são a encriptação dos dados, ou sua pseudonimização, bem como a testagem regular dos mecanismos de proteção aplicados aos dados a fim de averiguar sua eficácia. No entanto, as técnicas utilizadas a fim de salvaguardar os direitos dos titulares dos dados podem (e devem) variar, a fim de melhor se adequarem a cada situação.

---

[50] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Enunciado 39.
[51] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 5 (1) (e).
[52] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 5 (1) (f).
[53] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 32 (1).
[54] Idem.

2.1.7 PRINCÍPIO DA PRESTAÇÃO DE CONTAS

Segundo o princípio de prestação de contas, o controlador deve tomar medidas a fim de não apenas se certificar de que os dados estão sendo processados da devida maneira, mas também demonstrar que está agindo dentro dos moldes do regulamento. Outrossim, os operadores dos dados também têm obrigações próprias, vez que seu papel e o do controlador estão intimamente relacionados.

O próprio diploma normativo explicita formas por meio das quais os operadores podem fazer com que o processamento dos dados pessoais se dê em conformidade com o regulamento, como por exemplo: *a)* a manutenção de registros das atividades de processamento dos dados a fim de que as autoridades possam consulta-las a qualquer momento[55]; *b)* designar um funcionário específico para supervisionar a proteção dos dados, nas hipóteses descritas nos artigos 37 a 39 da GDPR; *c)* avaliar o impacto que possivelmente será acarretado aos titulares dos dados quando o processamento envolver altos riscos aos seus direitos[56]; *d)* atuar utilizando medidas técnicas e organizacionais, de modo a garantir que a proteção máxima dos dados seja o procedimento padrão[57]; *e)* garantir, por meio da utilização as devidas ferramentas e implementação de plataformas, que os titulares possam exercer seus direitos relacionados aos dados[58]; *f)* aderir aos códigos de conduta e mecanismos de certificação de segurança presentes nos artigos 40 e 42 do regulamento.

Vez que a GDPR explicita obrigações específicas para os operadores dos dados, e, levando também em conta seu óbvio e forte vínculo com os controladores, resta claro que ambos devem ter atuação positiva visando o cumprimento dos requisitos postos no que tange à prestação de contas, e não apenas aguardar que os titulares dos dados ou autoridades supervisoras os inquiram acerca da observância dos requisitos no decorrer do desenvolvimento da atividade.

2.2. DIREITOS DOS TITULARES DOS DADOS

O estudo dos princípios nos permite ter uma clara ideia dos principais pontos acerca da GDPR. No entanto, há aspectos mais específicos do diploma normativo que devem ser

[55] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 30.
[56] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 35.
[57] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 25.
[58] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 12 e 20.

observados, inclusive para fins de comparação com a LGDP em momento posterior da pesquisa. Nesse diapasão, vez que o espírito do regulamento é a proteção dos direitos e liberdades dos titulares dos dados, cabe analisar mais a fundo o que a GDPR traz acerca destes.

2.2.1 DIREITOS DE INFORMAÇÃO DO TITULAR E DE ACESSO AOS DADOS

Segundo o diploma normativo, os controladores e processadores têm a obrigação, antes de iniciar o processamento dos dados, de informar ao titular acerca do recolhimento de seus dados, e sobre sua intenção de processá-los, sendo dispensado requerimento por parte do titular[59]. Outrossim, como ditado pelo princípio da transparência no processamento, os titulares devem ser informados acerca da identidade do controlador, dos seus direitos com relação ao processamento, quais dados serão processados, de que forma o processamento se dará, assim como os riscos envolvidos e as medidas para preveni-los[60].

Mais especificamente, segundo o artigo 15 da GDPR, o controlador deve permitir que os titulares dos dados possam acessá-los a qualquer momento, bem como informar-lhes acerca: *a)* do propósito do processamento; *b)* das categorias de dados que serão utilizadas; *c)* de quem mais terá conhecimento acerca dos dados; *d)* do período de tempo pelo qual os dados permanecerão armazenados/em processamento; *e)* da prerrogativa detida pelo titular de determinar que o controlador retifique ou apague seus dados, bem como do seu direito de restringir os dados que serão processados, ou mesmo de se opor ao processamento; *f)* do seu direito de reclamação a autoridades supervisoras do processamento.

Outras informações relevantes a serem informadas ao titular dos dados incluem a identidade e informações para contato com *Data Protection Officer*, nos casos em que tal figura esteja presente no processamento dos dados[61]. Esta medida em particular demonstra a preocupação da GDPR em garantir, efetivamente, que os titulares dos dados tenham seus direitos respeitados, vez que, podendo entrar diretamente em contato com o *DPO*, torna-se mais eficiente a tomada de medidas preventivas ou repressivas no que diz respeito ao mau uso dos dados.

---

[59] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, COUNCIL OF EUROPE. **Handbook on european data protection law**. Imprimerie Centrale. Luxemburgo. 2018. P. 207.
[60] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Enunciado 39.
[61] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 13.

2.2.2 DIREITO À EXCLUSÃO DOS DADOS

Como dito anteriormente, o rol de direitos dos titulares inclui o de requisitar que seus dados sejam apagados, o que é essencial para a boa prática do processamento, vez que o objetivo da lei é salvaguardar os direitos dos titulares. Ademais, além de garantir a prerrogativa do titular de não ser mais parte do processamento, o direito de exclusão de dados guarda relação com o princípio da minimização de dados, que dita que devem ser usados apenas os dados necessários para o propósito do processamento, e nada mais.

Deve-se observar que a GDPR determina ainda que, uma vez requisitada, a exclusão dos dados deve se dar "sem atrasos desnecessários". Existem ainda hipóteses nas quais o controlador deve excluir os dados sem que haja manifestação de seus titulares. Outrossim, o artigo 17 do regulamento elenca as seguintes hipóteses nas quais os dados deverão ser excluídos: *a)* quando os dados pessoais não forem mais necessários para os propósitos do processamento; *b)* quando o titular dos dados revogar seu consentimento, e o consentimento for a base legal para que seja efetuado o processamento (o consentimento como base legal encontra-se presente nos artigos 6 (1) (a), e 9 (2) (a) da GDPR); *c)* quando os dados tiverem sido processados de forma ilegal; *d)* quando a exclusão dos dados for obrigatória para o cumprimento de obrigação legal decorrente de normas da União Europeia ou do estado-membro ao qual o controlador se submete. *e)* pelo responsável do titular de fato dos dados, quando o consentimento tiver sido dado por aquele, em virtude do titular de fato ser menor de 16 anos.

Em casos nos quais o controlador original tenha tornado os dados públicos, e houver manifestação do titular no sentido de exclusão dos dados, ou caso qualquer das outras hipóteses de exclusão se concretizar, deverá o controlador notificar os atuais controladores dos dados (ou seja, quem está processando os dados que agora são públicos) de que o titular dos dados requisitou sua exclusão, devendo os atuais controladores atendê-lo.

Por fim, há exceções a serem observadas ao direito de exclusão de dados. Segundo a GDPR, ainda que as hipóteses acima descritas se concretizem, os dados não deverão ser excluídos quando o seu processamento for necessário: *a)* para o exercício da liberdade de expressão e de acesso à informação; *b)* para o cumprimento de obrigação legal que determine o processamento dos dados pela União Europeia ou estado-membro ao qual o controlador se submete; *c)* para o cumprimento de tarefa de interesse público; *d)* para o exercício de dever oficial do qual o controlador é incumbido; *e)* por razões de interesse público, ou para propósitos de pesquisa científica ou histórica (desde que observadas as devidas medidas de salvaguarda de

demais direitos dos titulares); *f)* para o ingresso de ação judicial visando garantia de um direito, ou ainda para o exercício ou defesa de um direito.

2.2.3 DIREITO À RESTRIÇÃO AO PROCESSAMENTO DOS DADOS

Como exposto no direito de informação do titular, este tem a prerrogativa de restringir o uso de seus dados no seu processamento, nos termos do artigo 18 da GDPR. Nesse sentido, cabe comentar acerca do que seria e como se daria a restrição dos dados. A restrição pode ser vista como uma alternativa mais branda à exclusão, vez que é dotada de caráter temporário. Uma das hipóteses que ensejam a restrição é, inclusive, quando há o processamento ilegal dos dados, podendo o titular pedir tanto pela exclusão dos dados, como já apontado, quanto pela restrição de uso dos dados no processamento[62]. Ou seja, o controlador ainda terá os dados armazenados, mas não poderá utilizá-los para fins de processamento. Outrossim, quando a exatidão dos dados for contestada pelo titular, este poderá requerer a suspensão do processamento de seus dados até que seja averiguada a fidelidade dos dados à realidade[63].

As outras duas hipóteses previstas para a restrição do uso de dados pelo titular são *a)* quando os dados não forem mais necessários para o propósito do processamento, mas o titular precisar deles para o ingresso de ação judicial visando garantia de um direito, ou ainda para o exercício ou defesa de um direito[64]; e *b)* quando o titular se opor ao processamento de seus dados, e o controlador resistir à oposição (hipótese descrita no artigo 21 (1) da GDPR), o processamento deverá ser suspenso até que se decida qual dos dois tem maior legitimidade de ter seu direito atendido.

Dita ainda o artigo 18 (2), que no caso de restrição ao processamento de dados, só poderá voltar a haver processamento: *a)* com o consentimento do titular; *b)* se o processamento for necessário para o ingresso de ação judicial visando garantia, exercício, ou defesa de um direito de terceiro que seja pessoa natural; ou *c)* por razões de interesse público da União Europeia ou de qualquer estado-membro[65].

Por fim, se for o caso de fim da suspensão do processamento em virtude da restrição, o titular dos dados deverá ser notificado antes que ocorra futuro processamento[66].

---

[62] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 18 (1) (b).
[63] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 18 (1) (a).
[64] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 18 (1) (c).
[65] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 18 (2).
[66] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 18 (3).

2.2.4 DIREITO À OPOSIÇÃO AO PROCESSAMENTO DOS DADOS

Dentre os direitos dos titulares dos dados, encontra-se o a prerrogativa de se opor ao processamento destes. No entanto a oposição ao processamento não pode ocorrer em qualquer situação, sendo elencadas hipóteses nas quais o titular poderá exercer esse direito. Outrossim, a GDPR, em seu artigo 21 (1), determina que poderá o titular se opor ao processamento de seus dados, desde que este esteja baseado no interesse público/exercício de dever oficial do qual o controlador é incumbido (base legal definida pelo artigo 6 (1) (e) do regulamento), ou ainda para a satisfação de interesse legítimo de controlador ou de terceiros (base legal definida pelo artigo 6 (1) (f) do regulamento).

Percebe-se, então, que nessas duas hipóteses que ensejam a oposição, há o conflito entre o direito do titular em manter seus dados livres de processamento, e o direito (ou dever, no caso da hipótese descrita no artigo 6 (1) (e) da GDPR) do controlador em processa-los. Diante disso, recai sobre o controlador o ônus de demonstrar argumentos legítimos fortes a ponto de serem sobrepostos aos direitos do titular dos dados[67].

O regulamento ainda estabelece mais três cenários envolvendo o direito do titular à oposição do processamento de seus dados. Um deles é quando os dados estiverem sendo usado para fins diretos de marketing. De forma clara e simples, a GDPR deixa claro que o titular tem o direito de, a qualquer momento, a qualquer momento, se opor ao uso de seus dados para fins de marketing, incluindo *profiling*[68]. Uma vez manifestada a oposição do titular, o controlador deverá cessar o processamento dos dados para esse fim[69]. O regulamento dispõe, ainda, que o direito de manifestar oposição deverá ser informado pelo controlador de forma clara e destacada ao titular dos dados[70].

Outro cenário é quando o processamento de dados se der para fins de *information society services*[71]. Nesse caso, os controladores que oferecem estes serviços devem também oferecer, por meios eletrônicos e automatizados, as ferramentas necessárias para que o titular dos dados possa manifestar sua oposição ao processamento de seus dados[72]. Exemplo cotidiano da

---

[67] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 21 (1).
[68] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 21 (2).
[69] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 21, (3).
[70] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Enunciado 70.
[71] A definição de *information Society services*, segundo a Diretiva 98/48/EC é "qualquer serviço normalmente prestado por remuneração, à distância, por meio de equipamentos eletrônicos para o processamento e armazenamento de dados, e a pedido de quem recebe o serviço". Exemplo disso são lojas online ou serviços de *streaming*.
[72] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 21 (5).

implementação dessas ferramentas é a prerrogativa de bloquear o uso de *cookies* que nos é dada por determinados sites no âmbito da internet.

Por fim, quando seus dados estiverem sendo processados para fins de pesquisa cietífica, histórica, ou para fins estatísticos, o titular poderá se opor ao processamento, salvo se este for necessário para servir fins de interesse público[73].

2.2.5 DIREITO À PORTABILIDADE DE DADOS

Nos termos do enunciado 68 da GDPR, visando fortalecer o controle sobre seus próprios dados, e quando o processamento dos dados for realizado de forma automatizada (ou seja, de forma não manual), o controlador deverá disponibilizar ao titular os dados a ele referentes de forma estruturada, comumente usada, e em formato que possa ser facilmente operado por outras plataformas e outros controladores. O propósito desse direito é dar ao titular dos dados o poder de, a qualquer momento, transferir diretamente de um controlador para outro os seus dados, quando for viável de um ponto de vista técnico[74]. Ademais, o controlador não deve oferecer óbices a essa transferência, devendo apenas realizar o pedido do titular, nos termos do artigo 20 (1) da GDPR.

Para fins de concretização desse direito, o regulamento encoraja os controladores a desenvolverem formatos de processamento de dados que sejam interoperáveis[75]. O diploma normativo ressalta o fato de que a portabilidade de dados só será possível quando a base legal para o processamento dos dados for o consentimento do titular (presente nos artigos 6 (1) (a), e 9 (2) (a), tratando-se de dados sensíveis), ou o cumprimento de um contrato (presente no artigo 6 (1) (b) do regulamento).

Deve-se observar, ainda, que a vontade do titular de transferir seus dados de um controlador para outro pode vir acompanhada da vontade de que o controlador original exclua seus dados, de modo que sequer permaneçam por ele armazenados. Nesse caso, o controlador original deverá realizar as duas operações. Ou seja, o direito à portabilidade não deve prejudicar o direito à exclusão[76].

2.3 A PROTEÇÃO DE DADOS NOS ESTADOS UNIDOS

[73] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 21 (6).
[74] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 20 (2).
[75] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Enunciado 68.
[76] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 20 (3).

Preliminarmente, faz-se necessário destacar que não há, nos EUA, uma lei federal uniformize a tutela da privacidade no âmbito da proteção de dados do consumidor. Há o chamado *Privacy Act of 1974*, cujas normas limitam-se a dados dos cidadãos, coletados pelo governo estadunidense[77]. Além desse diploma, existem diversas leis tratando da proteção de dados em diferentes setores, como a DPPA, que dispõe acerca da transferência de dados pessoais coletados pelos departamentos de veículos automotivos do país[78], ou há poucos estados com suas próprias leis que tutelam a proteção de dados, como é o caso do estado de Illionis, que possui uma lei que regulamenta o uso de dados biométricos e estabelece sanções em caso de eventuais violações às previsões legais[79].

Apesar da existência de diversos diplomas normativos, as normas, em diversos casos, não se encontram aptas a defender, efetivamente, os direitos dos titulares dos dados, no formato em que estão. Além de que, poucos são os estados com leis que dispõem acerca da proteção de dados pessoais em vigor[80]. A lei estadual mais apta a lidar com os desafios contemporâneos apresentados pelo crescente avanço de tecnologia informática é a lei do estado da California, chamada de *California Consumer Privacy Act* (CCPA)[81]. Como o próprio nome sugere, é uma lei voltada para a proteção de dados do titular na qualidade de consumidor, apresentando nítida semelhança ao viés do regulamento europeu, que, como pudemos observar, também influenciou nossa Lei Geral de Proteção de Dados.

O CCPA trouxe novas obrigações às empresas que realizam tratamento de dados pessoais, como por exemplo a de informar aos titulares quais categorias de dados serão coletadas, e o propósito de cada uma[82], e o dever de disponibilizar aos titulares dois ou mais meios a serem utilizados com o propósito de que esses possam entrar em contato com as empresas, caso queiram obter informações acerca de seus dados, como estão sendo usados, e para quais terceiros estão sendo repassados[83]. Também foram introduzidos direitos aos titulares

---

[77] GREEN, ANDY. Complete Guide to Privacy Laws in the US. Estados Unidos, 29 de março de 2020. Varonis. Disponível em: https://www.varonis.com/blog/us-privacy-laws/. Acesso em 23 de setembro de 2020.
[78] ESTADOS UNIDOS. **Driver's privacy protection act**. 1994.
[79] ESTADOS UNIDOS. **Illinois Biometric Information Privacy Act**. 2008.
[80] GREEN, ANDY. Complete Guide to Privacy Laws in the US. Estados Unidos, 29 de março de 2020. Varonis. Disponível em: https://www.varonis.com/blog/us-privacy-laws/. Acesso em 23 de setembro de 2020.

[81] COLOCAR REFERÊNCIA DOA RIGO. Link: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (acesso em: 23/09/2020).
[82] ESTADOS UNIDOS. **California Consumer Privacy Act**. 2018. Seção 1, (b).
[83] ESTADOS UNIDOS. **California Consumer Privacy Act**. 2018. Seção 7, (a), (1).

dos dados, como o de obter acesso aos dados fornecidos[84], de requerer sua exclusão[85], ou o de se opor à venda/compartilhamento de seus dados para com terceiros[86].

Em que pese a garantia de diversos direitos básicos necessários no contexto em que se vive atualmente, fato é que a lei californiana não é tão abrangente quanto o Regulamento Geral sobre a Proteção de Dados europeu, e tampouco quanto a LGPD. Evidencia-se esse desfalque, por exemplo, na ausência de dispositivo que explicite a necessidade do fornecimento de consentimento para a coleção de dados, como é o caso da GDPR e da LGPD (ou seja, os consumidores precisam ser notificados acerca da coleta de seus dados, e podem requerer sua exclusão, mas seu consentimento não é necessário para que os dados sejam coletados). Além disso, tanto a GDPR quanto a LGPD possuem previsão de aplicação de sanções diretamente pelas autoridades responsáveis pela proteção de dados[87]. No caso do CCPA, é necessário o ingresso no judiciário a fim de que seja aplicada sanção[88], o que traz mais morosidade à aplicação da penalidade.

Além disso, não se pode olvidar que as prerrogativas trazidas pelo CCPA aplicam-se somente aos residentes e empresas do estado da Califórnia, vez que não há lei federal nos EUA que uniformize a matéria dos direitos e obrigações essenciais relativas ao tratamento de dados. Fato é que a garantia da segurança dos dados pessoais e o fortalecimento do direito à privacidade representam, nos dias atuais, um dos maiores desafios jurídicos em escala global, em especial no contexto de como empresas coletam e utilizam os dados pessoais de consumidores. Como já restou demonstrado, a União Europeia tem demonstrado pioneirismo e inovação com relação à tutela desses direitos, e, felizmente, o Brasil demonstra interesse e compromisso com a garantia dos mesmos direitos em seu território, sendo a LGPD cristalino exemplo disso. No caso dos EUA, a ausência de uma lei federal com o intuito de concretizar esses direitos essenciais, bem como uniformizar a matéria a nível nacional, demonstram desinteresse do governo no que diz respeito à questão de como empresas realizam o tratamento dos dados de seus consumidores, e de como utilizam esses dados.

---

[84] ESTADOS UNIDOS. **California Consumer Privacy Act**. 2018. Seção 1, (a).
[85] ESTADOS UNIDOS. **California Consumer Privacy Act**. 2018. Seção 2, (a).
[86] ESTADOS UNIDOS. **California Consumer Privacy Act**. 2018. Seção 5, (a).
[87] Na LGPD a previsão se encontra no artigo 55-J, IV. Na GDPR encontra-se no artigo 83, (1).
[88] ESTADOS UNIDOS. **California Consumer Privacy Act**. 2018. Seção 12, (b).

Por fim, a GDPR ressalta que a transferência que seria possível com a portabilidade de dados não poderá ocorrer caso o processamento sendo feito pelo controlador seja em virtude de interesse público, ou para exercício de dever oficial do qual o controlador é incumbido[89].

3. A PROTEÇÃO DE DADOS NO BRASIL DE ACORDO COM A LGPD

Feita a análise dos principais diplomas normativos acerca da proteção de dados no exterior, cabe agora analisar a LGPD, e comparar as três leis escolhidas, a fim de tirar conclusões acerca do tema.

3.1 ESCOPO DA LGPD

De início, cumpre destacar que a LGPD, assim como o regulamento europeu, é destinada à tutela dos dados pessoais de pessoas naturais, não recaindo sob sua proteção dados de pessoas jurídicas. Outra semelhança entre os dois diplomas normativos é a possibilidade de aplicação extraterritorial.

Nos moldes da Lei nacional, independentemente dos meios utilizados para se realizar o tratamento dos dados, o país sede do controlador e processador, ou o país onde estejam localizados os dados, os controladores e processadores devem se adequar às normas da LGPD[90]. Isso, desde que, a operação de tratamento dos dados se dê no âmbito do território nacional, que os titulares dos dados estejam localizados em território nacional, ou ainda que os dados tenham sido coletados no Brasil[91]. Nos termos do §1º do art. 3º da LGPD, consideram-se coletados no Brasil os dados que foram obtidos de titular que se encontrava em território nacional no momento da coleta. Não se sujeita à aplicação da LGPD o tratamento de dados pessoais realizado por pessoa natural, desde que para fins particulares e não econômicos, ou ainda para fins exclusivamente jornalísticos e artísticos[92]. A exceção também se aplica ao tratamento de dados para fins puramente acadêmicos, desde que observadas as bases legais necessárias para seu processamento, presentes nos artigos 7º e 11 da Lei[93]. Ainda, quando o tratamento dos dados for realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, nos termos do artigo 4º, III.

---

[89] Idem.
[90] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 3º, *caput*.
[91] Idem, Art. 3º, incisos I, II, e III.
[92] Idem, Art. 4º, I, e art. 4º, II, a).
[93] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 4º, II, b).

Por fim, em seu inciso IV, o supramencionado artigo dispensa a aplicação da Lei para o tratamento de dados 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, desde que este proporcione grau de proteção de dados pessoais adequado ao da LGPD.

3.2 CONCEITOS NA LGPD

De início, cumpre destacar que, em essência, os conceitos envolvendo os principais aspectos da LGPD são idênticos aos do regulamento em vigência na União Europeia. Não obstante, há algumas diferenças, como por exemplo a figura da ANPD. Os conceitos da Lei nacional aos quais refere-se aqui estão elencados no artigo 5º.

Dados pessoais são os dados relacionados a pessoas identificadas ou identificáveis, e há também a categoria de dados pessoais sensíveis (chamadas de categorias especiais de dados especiais na GDPR), para os quais há regras específicas acerca do tratamento de dados. Os dados pessoais sensíveis são definidos como dados acerca da "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".

Também estão presentes as figuras do controlador e do operador, definidos em conjunto como agentes de tratamento. O tratamento de dados, por sua vez, é a denominação utilizada na Lei pátria ao procedimento que no regulamento europeu é chamado de "processamento de dados".

Dados anonimizados, assim como na GDPR, não recaem sob a tutela da Lei pátria. No entanto, se o processo de anonimização ao qual foram submetidos for revertido, ou quando, com esforços razoáveis, puder ser revertido[94]. Ademais, caso os dados anonimizados sejam utilizados para a formação de perfil comportamental (*profiling*) de pessoa natural, e esse tratamento possa levar à identificação do titular dos dados, a lei passa a incidir sobre esses dados, ainda que anonimizados[95].

3.3 PRINCÍPIOS DO TRATAMENTO DE DADOS NA LGPD

[94] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 12.
[95] Idem. Art. 12, §2º.

A Lei Geral de Proteção de Dados é guiada por princípios, presentes em seu artigo 6º, que regem as normas de como deve se dar o tratamento de dados pessoais. Muitos desses princípios assemelham-se aos princípios presentes na GDPR. Cabe, então, analisa-los a fim de melhor compreender o diploma normativo.

3.3.1 PRINCÍPIO DA FINALIDADE

O princípio da finalidade dita que o tratamento de dados deve ocorrer para propósitos legítimos, específicos, explícitos, e informados ao titular, sem possibilidade de tratamento posterior incompatível com essas finalidades. Nota-se, aqui, grande semelhança ao princípio da legalidade, justiça e transparência do processamento de dados existente na GDPR. Outrossim, para que ocorra em virtude de propósitos legítimos, deve-se observar as bases legais para o tratamento de dados, que são as hipóteses que permitem o tratamento.

As bases legais elencadas pela LGPD encontram-se no artigo 7º do diploma normativo. Nos termos postos pelo artigo, o tratamento de dados pessoais só poderá será realizado: (i) com o consentimento do titular, que é a base legal por excelência para o tratamento de dados pessoais, tanto na legislação pátria quanto no regulamento europeu. Via de regra o consentimento será fornecido por escrito, mas outras formas são admitidas, nos termos do artigo 8º da Lei, e, em caso de consentimento por escrito, deverá haver cláusula em destaque no contrato celebrado entre as partes[96]. Ressalta-se que o consentimento deverá se referir ao propósito específico estipulado para o tratamento dos dados em questão, sendo nulas autorizações genéricas[97]. Percebemos aqui grande semelhança com o princípio da delimitação de propósito do processamento de dados, presente no regulamento de proteção de dados europeu. O mesmo pode ser visto no §6º do art. 8º da LGPD, que, dentre outras providências, dita que havendo alteração na finalidade específica do tratamento, esta deverá ser informada ao titular, podendo este então revogar ou não o seu consentimento.

Cumpre salientar que o consentimento poderá ser revogado a qualquer momento pelo titular, ao qual deve ser oferecido procedimento gratuito e facilitado para tal[98]. Importante notar que a revogação de consentimento não implica na eliminação do tratamento até então realizado

[96] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 8º, §1º.
[97] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 8º, §4º.
[98] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 8º, §5º.

nos dados, devendo haver requerimento expresso com esse fim[99]. A expressa previsão da disponibilidade de um "procedimento gratuito e facilitado" para o titular nos remete ao princípio da transparência, presente na GDPR, outra semelhança entre esta e o diploma normativo pátrio. Cabe ainda destacar que, em alinhamento com a dinâmica do ônus da prova em favor da parte menos capaz de produzi-la, presente, por exemplo, no Código de Defesa do Consumidor[100], cabe aos controladores o ônus de provar que o consentimento do titular foi obtido em conformidade com a Lei[101]. Por fim, nos resta apontar que é vedado o tratamento de dados mediante vício de consentimento[102].

A segunda base legal que enseja o tratamento de dados é (ii) quando o tratamento for necessário para o cumprimento de obrigação legal ou regulatória pelo controlador, situação similar à descrita do artigo 6 (1) (c), do regulamento europeu. O tratamento de dados pessoais também poderá ser realizado (iii) pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios, ou instrumentos congêneres, observadas as regras de tratamento de dados pelo poder público. Vemos aqui uma diferença entre a Lei nacional e a GDPR, vez que nesta não há a previsão de tratamento de dados diretamente pela Administração Pública como base legal.

Há, na GDPR, a hipótese do art. 6 (1) (e), em que o tratamento seria necessário "para os fins de interesse público ou para o exercício de dever oficial do qual o controlador seja incumbido", à qual poderia ser feita comparação, vez que, tratando-se das hipóteses previstas no art. 7º, III, LGPD, certamente estaria presente o interesse público, e seria o caso de execução de dever oficial de incumbência do controlador (tendo em vista que este seria a própria Administração Pública). No entanto, não se trata aqui de normas equivalentes, vez que a Lei Geral de Proteção de Dados não apenas aponta, expressamente, a Administração Pública como controladora, como também estabelece regras específicas para o tratamento de dados pessoais pelo Poder Público, em seu capítulo IV.

O próximo item que constitui base legal para o tratamento de dados pessoais é (iv) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais. O tratamento de dados para fins de pesquisa também é contemplado pelo regulamento europeu, embora não seja feita a recomendação específica de anonimização dos

---

[99] Idem.
[100] BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Art. 6º, VIII.
[101] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 8º, §2º.
[102] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 8º, §3º.

dados, mas sim que sejam postas medidas visando salvaguardar os direitos e liberdades dos titulares dos dados (a anonimização, no entanto, é uma técnica utilizada nesse contexto)[103].

Há de se observar ainda que, na LGPD, em caso de pesquisa relacionada à saúde pública, os dados em questão deverão ser mantidos em ambiente controlado e seguro, e seu tratamento deverá ocorrer exclusivamente dentro do órgão de pesquisa, com a finalidade estrita de realização de estudos e pesquisas[104]. Nesse caso, são recomendadas como medidas de segurança a anonimização ou a pseudonimização dos dados[105].

Cabe, aqui, apontar mais uma semelhança entre a legislação pátria e o regulamento da União Europeia, vez que há, no inciso II do artigo 16 da LGPD, previsão de conservação dos dados, para fins de estudo por órgão de pesquisa (sendo expressamente citada, mais uma vez, a anonimização dos dados). Já na GDPR, há disposição considerando que a continuidade do tratamento visando o arquivamento dos dados, para fins de pesquisa científica, histórica, e estatística, são considerados compatíveis com o propósito original, desde que sejam implementadas medidas visando salvaguardar os direitos e liberdades dos titulares[106]. O mesmo se aplica para dados pessoais sensíveis[107].

Dando continuidade, os dados pessoais também poderão ser submetidos a tratamento: (v) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados, de forma equivalente ao disposto no artigo 6 (1) (b) da GDPR; (vi) para o exercício regular de direitos em processo judicial, administrativo ou arbitral; (vii) para a proteção da vida ou incolumidade física de titular ou de terceiro, tal como também disposto no art. 6 (1) (d) da GDPR; (viii) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (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, de forma equivalente ao disposto no art. 6 (1) (f) da GDPR. (x) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

3.3.2 PRINCÍPIOS DA ADEQUAÇÃO E NECESSIDADE

[103] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 5 (1) (b).
[104] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 13.
[105] Idem.
[106] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 5 (1) (b).
[107] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Art. 9 (2) (j).

Os presentes princípios vêm complementar o princípio da finalidade, que dispõe acerca do propósito dado ao tratamento dos dados pessoais. O princípio da adequação, então, traz que os meios utilizados devem ser adequados ao fim que foi traçado inicialmente. Em outras palavras, o tratamento dos dados deve ser adequado ao propósito informado aos titulares, dentro do seu contexto[108].

Já o princípio da necessidade dita que os dados não deverão ser submetidos a tipos de tratamento que não sejam necessários para que se atinja o propósito delimitado. Deverão os dados ser submetidos tão somente aos procedimentos necessários para que se atinja o fim informado previamente ao titular, e nada mais. O princípio da necessidade ainda dispõe que o tratamento deve ser realizado "com abrangência dos dados pertinentes, proporcionais, e não excessivos em relação às finalidades do tratamento de dados"[109]. Ou seja, devem ser utilizados apenas os dados necessários. Esse aspecto em particular está em total sincronia com o princípio da minimização de dados, previsto no art. 5 (1) (c) do regulamento europeu.

3.3.3 PRINCÍPIOS DO LIVRE ACESSO, DA QUALIDADE DOS DADOS, E DA TRANSPARÊNCIA

Os presentes princípios têm por escopo trazer garantias fundamentais aos titulares dos dados, devendo então os controladores se certificarem de que essas garantias serão atendidas. Por se tratar de princípios acerca serviços que devem ser diretamente fornecidos aos titulares pelos controladores, serão os três estudados em conjunto.

Dispõe o princípio do livre acesso que deve ser disponibilizada aos titulares dos dados a consulta facilitada e gratuita acerca a forma e duração do tratamento ao qual os dados estão sendo submetidos, bem como o acesso aos dados em si[110].

O princípio da qualidade dos dados dita que os dados devem ser condizentes com a realidade[111], de forma equivalente ao princípio da exatidão dos dados, presente na GDPR. Além de determinar a exatidão dos dados, o princípio da qualidade dos dados determina que os dados devem ser organizados com clareza, e serem atualizados periodicamente, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento[112].

---

[108] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 6º, II.
[109] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 6º, III.
[110] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 6º, IV.
[111] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 6º, V
[112] Idem.

Por sua vez, segundo o princípio da transparência, devem os controladores informarem os titulares acerca da realização do tratamento, bem como dos agentes do tratamento, de forma clara, precisa, e facilmente acessível[113]. Em outras palavras, segundo esse princípio, os titulares têm o direito de saber não apenas como está sendo realizado o tratamento de seus dados, como também quem está realizando o tratamento, assim como ocorre no regulamento europeu.

3.3.4 PRINCÍPIOS DA SEGURANÇA E PREVENÇÃO

Assim como ocorre na GDPR, a Lei Geral de Proteção de Dados criou um princípio explícito visando garantir a máxima segurança quando do processamento de dados pessoais. Interessante notar, ainda, o destaque dado para a prevenção, vez que não há princípio unicamente dedicado para esse fator no regulamento europeu, sendo esse aspecto englobado pelo princípio da segurança de dados no referido diploma normativo.

Outrossim, o princípio da segurança na legislação pátria muito se assemelha com o seu equivalente no regulamento europeu, dispondo que devem ser utilizadas medidas tanto de natureza técnica, quanto administrativa, visando a proteção dos dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, ou difusão[114].

Poderíamos, nesse princípio, considerar como englobada também a prevenção, vez que é claro que o principal intuito da Lei é prevenir possíveis danos aos dados, embora haja também medidas repressivas, direcionadas aos titulares que não operarem de acordo com a lei[115]

Não obstante, o legislador optou por criar o princípio da prevenção, que, como é de se imaginar, dispõe que devem ser adotadas medidas com intuito de impedir a ocorrência de danos aos dados, em virtude de seu tratamento[116].

3.3.5 PRINCÍPIO DA NÃO DISCRIMINAÇÃO:

O princípio da não discriminação determina que o tratamento de dados não pode, sob hipótese alguma, ter finalidade discriminatória ilícita ou abusiva[117].

---

[113] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 6º, VI.
[114] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 6º, VII.
[115] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Capítulo VI, seção III, e capítulo VIII.
[116] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 6º, VIII.
[117] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 6º, IX.

Outrossim, podemos afirmar que o respeito a esse princípio deve ser redobrado quando do tratamento de dados pessoais sensíveis, pela sua própria natureza, vez que informações como a convicção religiosa, etnia, e vida sexual do indivíduo podem facilmente incitar referida discriminação, se o tratamento não for realizado de forma correta.

3.3.6 PRINCÍPIO DA RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

O último princípio elencado na Lei Geral de Proteção de dados cria, de forma similar ao princípio da prestação de contas presente no regulamento europeu, a obrigação de proatividade dos agentes de tratamento visando a boa técnica e a responsabilidade no que tange o processamento de dados pessoais.

Nesse contexto, os agentes de tratamento devem demonstrar que implementam medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção dos dados, bem como devem demonstrar a eficácia dessas medidas[118].

3.4 DOS DIREITOS DOS TITULARES DOS DADOS

Podemos perceber, até então, diversas semelhanças entre a Lei Geral de Proteção de Dados e o *General Data Protection Regulation*, não só em diversos pontos específicos de ambos os diplomas normativos, como também no principal propósito por eles compartilhado: o da proteção dos direitos dos titulares dos dados, principalmente em virtude do seu processamento em um contexto de mercado. Nesse diapasão, vez que a legislação pátria, tal qual o regulamento vigente na União Europeia, tem como cerne a defesa dos direitos dos titulares, tanto em caráter preventivo como repressivo, faz-se imperioso estudo mais detalhado acerca de sua defesa, assim como foi feito com o regulamento europeu na presente pesquisa.

Os direitos do titular estão elencados no capítulo III da LGPD, que em seu artigo 17 faz menção aos direitos fundamentais de liberdade, intimidade, e privacidade, cuja previsão decorre da Lei Maior.

Merece destaque, aqui, a importância de que seja disponibilizado um canal de comunicação eficiente entre o titular dos dados e os agentes de tratamento, vez que o exercício de suas prerrogativas, a si conferidas pela legislação, por parte do titular, só podem ser feitos mediante requisição, preferencialmente direcionada ao controlador. Aqui diz-se

[118] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 6º, X.

preferencialmente, pois o titular dos dados poderá direcionar a requisição tanto à ANDP[119], quanto a organismos de defesa do consumidor[120], embora o ideal é que haja relação transparente e harmoniosa entre o controlador e o titular. A legislação determina também que pode o requerimento ser realizado por representante legalmente constituído para tal[121].

Outrossim, segundo o artigo 18 da LGPD, poderá o titular requerer, a qualquer momento, a confirmação da existência de tratamento dos seus dados, bem como o acesso aos próprios dados, e a retificação de tais dados, caso estejam incorretos, incompletos, ou desatualizados[122]. Tanto a confirmação de existência dos dados quanto o acesso aos mesmos poderão ser providenciados em formato simplificado[123], ou por meio de um relatório completo acerca dos dados e seu tratamento, respeitados os segredos industrial e comercial[124]. Caso seja enviado o relatório completo, o controlador terá o prazo de 15 dias para fornecê-lo. Na hipótese do formato simplificado, o envio deverá ser imediato. Na hipótese de realização desse requerimento perante a ANPD, os prazos poderão ser diferentes, não havendo especificação de prazo pela lei[125]. Com o fim de que sejam cumpridos os prazos, a Lei determina que o armazenamento dos dados seja feito em formato que favoreça o envio desses relatórios[126]. Cabe ainda ao titular escolher se os receberá de forma eletrônica ou impressa[127].

Também detém o titular a prerrogativa de requerer a anonimização, bloqueio, ou eliminação de dados que sejam desnecessários ao propósito do processamento, de alguma forma excessivos, ou que estejam sendo submetidos a tratamento em desconformidade com a lei[128]. Caso o processador tenha compartilhado os dados com terceiros, deverá notifica-los do requerimento feito pelo titular, a fim de que sua vontade seja cumprida[129]. Ressalta-se que a eliminação de dados não depende dessas razões para ser requisitada, podendo o titular fazê-lo a qualquer momento[130].

Outrossim, declarada a vontade do titular mediante requerimento, os dados deverão ser eliminados, salvo se estiverem sendo conservados para (i) o cumprimento de obrigação legal

---

[119] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, §1º.
[120] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, §8º.
[121] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. §3º.
[122] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, incisos I, II, e III.
[123] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 19, I.
[124] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 19, II.
[125] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 19, §4º.
[126] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 19, §1º.
[127] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 19, §2º, incisos I e II.
[128] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, inciso IV.
[129] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, § 6º.
[130] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, inciso VI.

ou regulatória pelo controlador[131]; (ii) estudo por órgão de pesquisa, sendo anonimizados sempre que possível[132]; (iii) transferência a terceiro, respeitadas as regras da LGPD acerca do tratamento[133]; ou (iv) uso exclusivo do controlador, desde que anonimizados, e vedado seu acesso por terceiros[134].

O direito à portabilidade dos dados também está presente[135], não sendo abrangidos pela portabilidade dados já anonimizados[136]. É interessante a presença desse direito, tanto na LGPD quanto na GDPR, vez que a portabilidade de dados não é algo muito comum, pelo fato de depender da existência de plataformas interoperáveis, bem como da implementação destas pelos controladores dos dados. A presença desse instituto como direito dos titulares dos dados certamente serve como estímulo às empresas para colocarem em prática essa cooperação, o que é interessante do ponto de vista do consumidor, que terá mais liberdade para escolher a quem confiar o tratamento de seus dados, pois poderá trocar de agente com facilidade. Isso também aumenta o grau de controle que o titular tem sobre seus próprios dados, o que é um avanço benéfico.

Os titulares têm, ainda, o direito de saber com quais entidades o controlador compartilhou seus dados, sejam essas entidades públicas ou privadas[137]. A Lei nacional deixa expresso, ainda, que deve ser informado aos titulares que eles têm a opção de não fornecer seu consentimento para o tratamento dos dados, bem como possíveis consequências negativas que o tratamento poderá trazer[138].

Por fim, consta nos direitos dos titulares dos dados a possibilidade de revogação do consentimento[139].

O descumprimento de qualquer das prerrogativas das quais gozam os titulares dos dados enseja a oposição dos titulares ao tratamento de seus dados, inclusive contra os tratamentos baseados em alguma das hipóteses de dispensa de consentimento[140]. Ainda nesse contexto, caso o controlador não possa realizar a providência requerida pelo titular, deverá informa-lo da razão

---

131 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 16, inciso I.
132 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 16, inciso II.
133 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 16, inciso III.
134 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 16, inciso IV.
135 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, inciso V.
136 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, §7º.
137 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, inciso VII.
138 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, inciso VIII.
139 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, inciso IX.
140 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, §2º.

que o impede de fazê-lo[141], ou, caso quem tenha recebido o requerimento não seja o controlador, deverá informar o titular, e, quando possível, indicar quem é o agente[142].

No tocante à tomada de decisões baseada exclusivamente no tratamento automatizado de dados pessoais, o artigo 20 da Lei Geral de Proteção de Dados confere ao titular dos dados o direito de solicitar a sua revisão, inclusive decisões relacionadas ao seu *profiling*, ou seja, decisões destinadas a definir o perfil do titular, seja esse perfil no âmbito profissional, de consumo, crédito, ou de aspectos de sua personalidade. É importante a atenção ao direito dos titulares nesses casos, vez que, por ser um processo completamente automático, o grau de sofisticação do algoritmo utilizado, bem como a lógica aplicada ao processo, e outros fatores de ordem tecnológica, serão as ferramentas usadas para o tratamento, que, em alguns casos, poderá ter efeitos significantes para os titulares.

Tendo em vista que os aspectos supracitados possam nem sempre ser os mais refinados, ou, ainda que o sejam, possam ser utilizados de forma inadequada (ou até discriminatória), a LGPD dá aos titulares o direito de que haja intervenção humana no processo, que, no caso em tela, se concretiza na revisão que será feita pelo controlador.

Outrossim, sempre que lhe for solicitado, o controlador deverá fornecer informações no tocante aos critérios e procedimentos utilizados na tomada dessa decisão puramente automatizada, respeitados os segredos comercial e industrial[143]. Sendo o caso de impossibilidade de fornecimento dessas informações em virtude de segredo comercial e/ou industrial, poderá ser realizada auditoria, pela ANPD, a fim de que se verifique a presença ou não de aspectos discriminatórios no tratamento automatizado em questão[144].

O tópico da tomada de decisões com base apenas em operações automatizadas também é abordado no regulamento europeu[145], havendo, de forma similar, a possibilidade de intervenção humana, bem como do fornecimento de informações acerca do processo da tomada de decisões, permitindo que o titular entenda mais claramente a que tipo de procedimento seus dados estão sendo submetidos.

Por fim, dispõe o artigo 21 do diploma normativo brasileiro que os dados pessoais do titular referentes ao regular exercício de seus direitos não poderão ser utilizados em seu prejuízo, e, no artigo 22, há a previsão de dos interesses e direitos dos titulares em juízo.

---

[141] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, §4º, II.
[142] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 18, §4º, I.
[143] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 20, §1º.
[144] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 20, §2º.
[145] UNIÃO EUROPEIA. **General data protection regulation**. 2016. Arts. 12, 13 (2) (f), 15 (1) (h), e 22.

3.5 DOS DEVERES DOS AGENTES DE TRATAMENTO

Como encarregados pelo tratamento dos dados pessoais, recai sobre as figuras do controlador e do operador a responsabilidade para que esse se dê de forma responsável e segura, levando também em conta a segurança dos dados. Visando garantir o correto tratamento dos dados pessoais, a Lei Geral de Proteção de Dados estabelece obrigações específicas a essas duas figuras, bem como sanções para o caso de sua não observância. Por exemplo, o tratamento dos dados pelo operador é vinculado às instruções dadas pelo controlador, não podendo se dar de forma diversa da que foi determinada por este[146].

Devem tanto o controlador e o operador, ainda, manter registro das operações de tratamento de dados realizadas, em especial quando a base legal utilizada para o tratamento seja o legítimo interesse do controlador ou de terceiro[147]. O controlador também deverá elaborar um relatório de impacto à proteção dos dados sob tratamento, se assim determinar a Autoridade Nacional de Proteção de Dados[148]. No caso de elaboração desse relatório, o mesmo deverá explicitar "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"[149]. Também detém a ANPD a prerrogativa de dispor acerca de padrões de interoperabilidade para fins de portabilidade, assim como padrões de livre acesso aos dados, segurança, tempo de guarda dos registros, levando em conta os princípios da necessidade e transparência[150].

O controlador deve também indicar quem será o encarregado específico pelo tratamento dos dados, de forma que sua identidade e informações de contato sejam divulgadas publicamente, preferencialmente no site do controlador, visando o fácil acesso dos titulares dos dados às mesmas, nos termos do artigo 41, §1º, da LGPD. Dessa forma, os titulares dos dados poderão exercer suas prerrogativas legais, devendo o encarregado ao tratamento de seus dados prestar esclarecimentos sempre que requisitado, bem como aceitar eventuais reclamações e comunicações dos titulares, e adotar as providências necessárias para retificar qualquer situação que se apresente[151]. Da mesma forma, se requisitado pela ANPD, o encarregado deverá adotar as providências necessárias[152]. Também deve o encarregado orientar os demais colaboradores

[146] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 39.
[147] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 37.
[148] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 38.
[149] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 38, parágrafo único.
[150] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 40.
[151] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 41, §2º, I.
[152] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 41§2º, II.

da entidade que realizará o tratamento dos dados acerca das práticas a serem tomadas visando a sua proteção, nos termos do artigo 41, §2º, III.

Ressalta-se que, conforme a natureza e porte da entidade que realizará o tratamento dos dados, ou ainda levando em conta o volume de operações de tratamento, poderá a ANPD dispensar a indicação do encarregado específico, ou ainda estabelecer normas complementares sobre sua definição e suas atribuições, caso não haja dispensa de sua indicação[153].

Acerca da segurança e do sigilo dos dados pessoais, devem ser adotadas, desde a fase de concepção do produto[154], medidas de natureza técnica e administrativa, de modo a proteger os dados pessoais de qualquer destruição, perda, alteração, comunicação, ou tratamento inadequado, sejam essas situações de natureza acidental ou ilícita[155]. Ressalta-se que, essas medidas devem ser adotadas não apenas pelo controlador e operador, mas também por qualquer pessoa que venha a intervir em alguma das fases do tratamento dos dados. Nos termos do artigo 47 da LGPD, esse terceiro fica obrigado a garantir a segurança da informação, mesmo após o término do tratamento.

Caso haja falha na segurança dos dados, o controlador deverá entrar em contato com a ANPD[156]. O contato deverá ser imediato, ou o mais brevemente possível, sendo necessária justificativa quando este for o caso[157]. Nos termos da lei, na comunicação feita à agência nacional, deverão constar, pelo menos, a descrição da natureza dos dados afetados; informações acerca dos titulares; a indicação das medidas utilizadas para a proteção dos dados; os riscos relacionados ao incidente; as medidas que serão adotadas mata reverter ou mitigar os efeitos decorrentes da falha[158]. Nessa situação, deverá ser averiguado se foram adotadas as medidas de segurança adequadas visando salvaguardar os dados[159]. A ANPD poderá, ainda, determinar medidas a serem tomadas visando reverter ou mitigar os efeitos do prejuízo sofrido, ou até impor a ampla divulgação do fato em meios de comunicação.

É importante destacar que, embora o operador esteja subordinado ao controlador, pode equiparar-se a esse para fins de reparação de danos (sejam estes patrimoniais, morais, individuais ou coletivos[160]), quando não seguir as instruções do controlador, ou descumprir a

---

[153] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 41, §3º.
[154] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 46, §2º
[155] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 46.
[156] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 48
[157] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 48, §1º, V.
[158] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 48, §1º, I, II, III, IV, e VI.
[159] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 48, §3º.
[160] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 42, caput.

legislação[161]. Da mesma forma, se os controladores estiverem diretamente envolvidos no tratamento que acarretou danos ao titular dos dados, serão obrigados a repara-los, de modo que há solidariedade entre o controlador e o operador[162]. Como é de praxe nas hipóteses legais de solidariedade em nosso ordenamento jurídico, aquele que reparar o dano causado terá direito de regresso com relação aos demais responsáveis[163].

A LGPD apresenta, em seu artigo 43, as hipóteses nas quais os agentes de tratamento não serão responsabilizados pelo dano sofrido pelo titular dos dados. Nos termos do diploma normativo, para que não haja responsabilização, deve ser comprovado que o tratamento do qual decorreram os danos não foi realizado pelo agente acusado, ou que, embora tenha sido realizado por este, não houve violação à legislação de proteção de dados. Também não será responsabilizado o agente quando o dano decorrer de culpa exclusiva do próprio titular dos dados, ou ainda de terceiro.

Em suma, o tratamento deve se dar dentro dos parâmetros legais, levando-se em conta os resultados e os riscos que dele razoavelmente se esperam, o modo em que é realizado, e as técnicas de tratamento disponíveis à época de sua realização. A inobservância de qualquer desses aspectos tornará o tratamento irregular, e passível de responsabilização[164].

3.6 DAS BOAS PRÁTICAS E DA GOVERNANÇA

A Lei Geral de Proteção de dados dá aos agentes do tratamento a prerrogativa de que elaborem, de forma individual ou por meio de associações, e sempre dentro de sua competência, normas visando não apenas o cumprimento dos dispositivos legais, mas também a sofisticação do tratamento dos dados pessoais sob seu cuidado[165]. A essas normas, a legislação deu o nome de regras de boas práticas e de governança.

Naturalmente, as regras de boas práticas e de governança devem estar alinhadas com as exigências legais, devem ser aplicadas a todos os dados pessoais que estejam sob controle dos agentes de tratamento[166], devem conter mecanismos próprios de salvaguarda aos dados, planos

[161] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 42, §1º, I.
[162] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 42, §1º, II.
[163] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 42, §4º.
[164] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 44 caput, e incisos I, II, e III.
[165] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 50.
[166] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 50, §2º, I, b).

de resposta e remediação a incidentes[167], e devem também ser atualizados continuamente, de modo que os dados estejam protegidos da melhor forma possível[168].

Ademais, poderá a ANPD realizar pedido de comprovação de eficácia do programa de boas práticas e governança do controlador, ficando este obrigado a demonstrar que suas regras são, de fato, efetivas[169].

Nota-se, com a previsão da criação dessas normas, uma preocupação do ordenamento jurídico brasileiro com a qualidade da proteção dos dados pessoais, vez que representam um claro estímulo às entidades que realizam o tratamento dos dados no sentido de refinarem suas técnicas para realização da atividade.

3.7 DAS SANÇÕES ADMINISTRATIVAS

Vistas as obrigações e competências dos agentes responsáveis pelo tratamento de dados, cabe agora discorrer acerca das sanções administrativas previstas na Lei Geral de Proteção de Dados para os casos nos quais as normas na lei dispostas não forem observadas.

As sanções estão elencadas no artigo 52 da referida lei, e mais branda entre elas é a advertência, que virá acompanhada de prazo dentro do qual deverá ser corrigida a desconformidade com a lei. Há também previsão de multa simples, com limite de até 2% do faturamento da pessoa jurídica no seu último exercício, não podendo a quantia exceder a cinquenta milhões de reais. O mesmo limite se aplica para o caso da sanção de multa diária. A ANPD também poderá publicizar a infração cometida, efetuar bloqueio dos dados pessoais relacionados à infração até que a situação seja regularizada, ou simplesmente eliminar os dados.

Havendo imposição de ao menos uma das sanções supracitadas[170], poderão ser aplicadas, também, as sanções de suspensão parcial do funcionamento do banco de dados referente à infração, ou a suspensão do exercício da atividade de tratamento dos dados referentes à infração, ambos por seis meses, havendo possibilidade de prorrogação por igual período. Há, ainda, a previsão de proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados pela entidade que os realizava.

---

[167] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 50, §2º, I, g).
[168] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 50, §2º, I, h).
[169] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 50, §2º, II.
[170] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 52, §6º.

Ressalta-se que não serão impostas sanções sem que haja o devido procedimento administrativo que possibilite a ampla defesa do infrator, nos termos do parágrafo 1º do artigo 52 da LGPD.

No referido procedimento, serão levadas em conta a gravidade da infração e dos direitos pessoais dos titulares afetados, bem como sua natureza, a boa-fé, a condição econômica, e a vantagem auferida ou pretendia pelo infrator, o grau do dano sofrido, eventual reincidência, a cooperação do infrator, e se foram ou não adotados mecanismos e procedimentos capazes de minimizar o dano sofrido[171]. Também será observado se os agentes possuíam políticas de boas práticas e governança, se prontamente adotaram medidas corretivas com relação à falha, e será auferida a proporcionalidade entre a gravidade da falta e a intensidade da sanção[172].

3.8 DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

Outra novidade trazida pela Lei Geral de Proteção de Dados é a figura da ANPD, entidade dotada de competência regulatória, fiscalizatória, e punitiva[173] acerca da matéria da proteção de dados pessoais no Brasil. Nos termos do artigo 55-A da Lei, a autoridade nacional é órgão da administração pública federal, e integra a Presidência da República. O parágrafo primeiro do mesmo artigo prevê a possibilidade de transformação da ANPD em entidade da administração pública federal indireta, submetida a regime autárquico especial, porém permanecendo vinculada à Presidência da República. Essa mutabilidade da natureza jurídica da autoridade nacional poderá ocorrer no prazo de dois anos a serem contados a partir da entrada em vigência da LGPD[174].

A criação da Autoridade Nacional de Proteção de Dados representa avanço para a tutela dos direitos relativos à privacidade em âmbito nacional, vez que será a entidade responsável, por exemplo, pela uniformização da interpretação da Lei Geral de Proteção de Dados[175]; pela aplicação das multas previstas no artigo 52 da Lei nacional, nos casos em que haja tratamento irregular de dados pessoais[176]; por elaborar diretrizes para a Política Nacional de Proteção de Dados e da Privacidade[177]; e por informar a população acerca das políticas públicas e normas

[171] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 52, §1º, incisos I a VIII.
[172] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 52, §1º, incisos IX, X, e XI.
[173] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 55-J, §4º
[174] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 55-A, §2º.
[175] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 55-J, XX.
[176] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 55-J, IV.
[177] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 55-J, III.

concernentes à proteção de dados pessoais[178]. Percebe-se, logo, a preocupação do Estado com a especialização e aprofundamento no tema, bem como com a informação dos cidadãos acerca da matéria, o que é extrema importância, visto que são esses os titulares dos dados e detentores dos direitos.

Outro aspecto importante da legislação é a previsão de promoção de ações de cooperação com órgãos internacionais acerca da proteção de dados[179], o que, além de proporcionar a troca de conhecimento e tecnologia entre autoridades especializadas, tende a aumentar a participação do Brasil no panorama mundial da proteção dos dados pessoais. É válido ressaltar, inclusive, que a própria criação da ANPD traz ao Brasil mais credibilidade no cenário internacional, vez que sua existência e bom funcionamento torna o país mais próximo aos padrões de adequação perante as normas europeias de proteção de dados[180].

Essa cooperação também deverá estar presente a nível nacional. Isso porque, uma vez que a autoridade nacional será o órgão central responsável por uniformizar a interpretação, bem como definir normas e diretrizes para a implementação da LGPD, será necessária a articulação entre a ANPD e outras autoridades reguladoras públicas, como por exemplo a ANATEL e o CADE, hipótese inclusive estabelecida pelo inciso XXIII, do artigo 55-J do diploma normativo.

Tendo em vista o vasto elenco de competências instituídas à Autoridade Nacional de Proteção de Dados, bem como a seriedade do tema, é imprescindível que o órgão goze de autonomia e independência, a fim de que sua atuação visando garantir a integridade dos direitos dos titulares de dados possa se concretizar livre de impedimentos burocráticos, ou até ideológicos. Nesse sentido, é preocupante a excessiva vinculação da autoridade nacional e de seus membros à presidência, situação que é diversa da ideia inicial presente no Projeto aprovado pelo Senado em 2018[181].

---

[178] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 55-J, VI.

[179] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 55-J, IX.

[180] TEFFÉ, CHIARA SPADACCINI DE. Por que precisamos de uma Autoridade Nacional de Proteção da Dados? Brasil, 07 de janeiro de 2020. Jota. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/por-que-precisamos-de-uma-autoridade-nacional-de-protecao-de-dados-07012020. Acesso em 21 de setembro de 2020.

[181] TEFFÉ, CHIARA SPADACCINI DE. Por que precisamos de uma Autoridade Nacional de Proteção da Dados? Brasil, 07 de janeiro de 2020. Jota. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/por-que-precisamos-de-uma-autoridade-nacional-de-protecao-de-dados-07012020. Acesso em 21 de setembro de 2020.

CONSIDERAÇÕES FINAIS

Diante da pesquisa realizada, percebe-se que a Lei Geral de Proteção de Dados se espelhou, em muitos aspectos, na *General Data Protection Regulation*, que é o diploma normativo pioneiro na regulamentação do regular e seguro tratamento de dados pessoais. São englobados pela LGPD todos os elementos essenciais como os direitos dos titulares dos dados, as bases legais que ensejam o processamento dos dados, as obrigações dos agentes de tratamento, bem como as sanções caso as normas dispostas não sejam observadas. Representa um grande avanço a criação da Autoridade Nacional de Proteção de Dados, com o intuito de simplificar a uniformização da interpretação e aplicação das normas dispostas na LGPD, aplicação de multas, e de promover avanços no âmbito da tutela da proteção de dados pessoais no Brasil. Cabe apenas ressaltar que deve a ANPD gozar de maior autonomia, e de ampla independência, a fim de que possa exercer de forma plena suas prerrogativas. Nesse sentido, seu atual regime, de integração da Presidência da República vai de encontro a essa independência, e, apesar de haver previsão de mudança de sua natureza jurídica, permanece previsto em lei seu vínculo à Presidência da República, o que, para os fins de autonomia, não é algo desejável.

REFERÊNCIAS

BRASIL. Lei nº 8.078, de 11 de setembro de 1990.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018.

CHABINSKY, STEVEN., PITTMAN, F. PAUL. USA: Data Protection Laws and Regulatioins 2020. Inglaterra, 06 de julho de 2020. Disponível em: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa. Acesso em: 23 de setembro de 2020.

DONEDA, DANILO. **Da privacidade à proteção de dados pessoais**, Rio de Janeiro. Editora Renovar. 2006

ESTADOS UNIDOS. California Consumer Privacy Act. 2018.

ESTADOS UNIDOS. Driver's privacy protection act. 1994.

ESTADOS UNIDOS. Illinois Biometric Information Privacy Act. 2008.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, COUNCIL OF EUROPE. Handbook on european data protection law. Imprimerie Centrale. Luxemburgo. 2018

GREEN, ANDY. Complete Guide to Privacy Laws in the US. Estados Unidos, 29 de março de 2020. Varonis. Disponível em: https://www.varonis.com/blog/us-privacy-laws/. Acesso em 23 de setembro de 2020.

REBECCA S. KRAUS. Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants. EUA. 2011

SEAN CAWLEY. The National Data Center and the Federal Information Network: A Paradox. College of Arts and Science, Vanderbilt University, EUA. Volume 10. 2015

STEPANOVA, O., GROOTHUIS, F. The privacy, data protection and cybersecurity law review. 6 edição. 2019. Disponível em: https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210039/germany.

TEFFÉ, CHIARA SPADACCINI DE. Por que precisamos de uma Autoridade Nacional de Proteção da Dados? Brasil, 07 de janeiro de 2020. Jota. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/por-que-precisamos-de-uma-autoridade-nacional-de-protecao-de-dados-07012020. Acesso em 21de setembro de 2020.

The Computer and Invasion of Privacy: Hearings Before a Subcommittee of the Committee on Government Operations, House of Representatives. U.S. Government Printing Office: Washington, 1966

UNESCO, **Keynotes to Foster Inclusive Knowledge Societies: Access to Information and Knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet, United Nations Education, Scientific and Cultural Organization**. 2015.

UNIÃO EUROPEIA. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. 1981. Capítulo II, art. 5. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.

UNIÃO EUROPEIA. Directive 95/46/EC of the european parliament and of the council – Data Protection Directive. 1995. Capítulo II, seção II, art. 7. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5.

UNIÃO EUROPEIA. Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. European Treaty Series – No 108. Strasbourg, 1981. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434

UNIÃO EUROPEIA. General data protection regulation. 2016.