OBSERVATÓRIO DA LGPD
UNIVERSIDADE DE BRASÍLIA

ANÁLISE COMPARADA
LGPD E GDPR

ORGANIZADORES

LAURA SCHERTEL MENDES

GIOVANNA MILANESE

FELIPE ROCHA DA SILVA

TAYNÁ FROTA DE ARAÚJO

ISABELA MARIA ROSAL

PAULO RICARDO SANTANA

EDUARDA COSTA

ELIS BRAYNER

ANUÁRIO DO OBSERVATÓRIO DA LGPD DA UNIVERSIDADE DE BRASÍLIA

VOLUME 1

Universidade de Brasília
Faculdade de Direito

Anuário do Observatório da LGPD da Universidade de Brasília

Análise comparada entre elementos da LGPD e do GDPR

Volume 1
Brasília-DF
2023

Anuário do Observatório da LGPD da Universidade de Brasília: Análise comparada entre elementos da LGPD e do GDPR.

Para esclarecimentos sobre esta obra, entrar em contato com observatorio.lgpd.unb@gmail.com

Volume 1

Organização
Coordenação Geral: prof.ª Laura Schertel Mendes;
Coordenação Adjunta: Giovanna Milanese;
Coordenação de Pesquisa: Felipe Rocha e Tayná Frota de Araújo;
Revisão e Organização: Eduarda Costa Almeida, Elis Bandeira A. Brayner, Isabela Maria Rosal e Paulo Ricardo da Silva Santana.

Informações

Observatório da LGPD/Unb
Faculdade de Direito
Universidade de Brasília
Campus Universitário Darcy Ribeiro, CEP: 70.910-900, Brasília-DF, Brasil

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Central da Universidade de Brasília – BCE/UNB)

A636 Anuário do Observatório da LGPD da Universidade de Brasília [recurso eletrônico] : análise comparada entre elementos da LGPD e do GDPR / organização Laura Schertel Mendes … [et al.]. – Brasília : Universidade de Brasília, Faculdade de Direito, 2024. 2 v.

Inclui bibliografia. Modo de acesso: World Wide Web.

ISBN 978-65-00-92398-8 (v. 1).

ISBN 978-65-00-92399-5 (v. 2).

1. Brasil. [Lei geral de proteção de dados pessoais (2018)]. 2. Universidade de Brasília. 3. Proteção de dados. 4. Direito comparado. I. Mendes, Laura Schertel (org.).

CDU 34

AUTORES

Ana Júlia Prezotti Duarte

Andressa Carvalho Pereira

Angélica Opata Vettorazzi

Gabriel de Araújo Oliveira

Gabriel Cabral Furtado

Eduarda Costa Almeida

Fernanda Passos Oppermann Ilzuka

Isabela de Araújo Santos

Júlia Carvalho Soub

Shana Schlottfeldt

Sofia de Medeiros Vergara

Paulo Ricardo da Silva Santana

Rafael Luís Müller Santos

Wanessa Larissa Silva de Araújo

REVISORES

A realização deste anuário contou com a significativa participação de revisores, que atuaram na avaliação e revisão dos artigos submetidos pelos pesquisadores do Observatório, fornecendo orientações e sugestões de melhoria. Oferecemos nosso mais sincero agradecimento pelas valiosas contribuições de cada um.

Ana Luísa Vogado de Oliveira

Angelo Prata de Carvalho

Davi Ory

Gabriel Fonseca

Isabela Maria Rosal Santos

Maria Cristine Lindoso

Matheus Vinicius Aguiar

Paula Baqueiro

Tainá Aguiar Junquilho

Thiago Guimarães Moraes

SUMÁRIO

APRESENTAÇÃO

É com uma profunda satisfação e sentimento de dever cumprido que introduzimos este anuário, que representa a materialização dos esforços coletivos dedicados à organização e consolidação dos estudos e discussões realizados pelo Observatório da LGPD/UnB entre os anos de 2021 e 2022. Este grupo, comprometido com a complexa temática da proteção de dados pessoais, foi guiado pela experiente Professora Laura Schertel Mendes e coordenado por Giovanna Milanese, Felipe Rocha e Tayná Frota de Araújo. Este projeto não é apenas uma compilação de ideias; é a concretização de nossa missão em aprofundar a pesquisa de alta qualidade sobre a proteção de dados pessoais no Brasil, temática de extrema relevância nos dias atuais, em um espaço público de ensino superior de excelência, a Universidade de Brasília (UnB).

A concepção deste anuário não se limitou a ser um exercício de catalogação de discussões internas; foi uma resposta proativa à necessidade de transcender as fronteiras do grupo, transformando nossos debates em uma obra que busca a sistematização dos principais temas discutidos. Com esse propósito, nos propomos a explorar e compreender as nuances e implicações da Lei Geral de Proteção de Dados Pessoais (LGPD), por meio de uma análise comparativa com o Regulamento Geral sobre a Proteção de Dados (RGPD) europeu. A estrutura deste trabalho segue a sequência dos dispositivos da LGPD, proporcionando uma análise sistemática e abrangente dos principais aspectos presentes em ambas as normativas.

O início deste trabalho remonta o ano de 2021, um período desafiador, marcado pela pandemia de COVID-19, que, apesar das adversidades, não paralisou nossas atividades. Mantivemos uma dinâmica remota com diversos encontros de discussão para a elaboração deste anuário. Perseveramos, inclusive, com encontros virtuais de capacitação em escrita acadêmica, oferecendo formação aos membros. Finalizamos a redação ainda em 2022, com esforços contínuos dos participantes, e, portanto, todos os textos possuem a mencionada limitação temporal.

Este anuário é resultado da inestimável contribuição e expertise dos graduados da UnB que compõem o Observatório da LGPD. A diversidade de conhecimento e perspectivas dos colaboradores não apenas enriqueceu, mas moldou a abordagem do anuário, oferecendo uma visão multidimensional das implicações práticas e teóricas das normas analisadas.

Com o compromisso de assegurar a mais elevada qualidade e o alto grau de rigor acadêmico, convidamos profissionais que são ou foram pós-graduandos da UnB para atuar na qualidade de revisores dos artigos. Os Revisores desempenharam papel fundamental na orientação, correção e instrução dos graduandos envolvidos no projeto, contribuindo de forma decisiva para o aprimoramento contínuo do conteúdo apresentado.

Portanto, este anuário não se propõe apenas a ser uma fonte de referência sobre a LGPD e RGPD, mas reflete, acima de tudo, nosso compromisso inabalável com a excelência acadêmica e a contribuição substancial para o entendimento e desenvolvimento do campo de proteção de dados pessoais, tanto no contexto brasileiro quanto europeu. Este é mais do que um documento; é uma expressão de nossa dedicação à disseminação de conhecimento de qualidade e ao avanço do debate sobre a proteção de dados em um cenário cada vez mais dinâmico e desafiador. Convidamos todos os interessados a mergulharem nesta obra, que não apenas documenta, mas também impulsiona o progresso e a compreensão nesse campo.

Brasília, 1º de dezembro de 2023

Laura Schertel Mendes[1]

Giovanna Milanese[2]

Felipe Rocha [3]

Tayná Frota de Araújo[4]

[1] Coordenadora Geral do Observatório da LGPD da Universidade de Brasília.
[2] Coordenadora Geral Adjunta do Observatório da LGPD da Universidade de Brasília.
[3] Coordenador de Pesquisa do Observatório da LGPD da Universidade de Brasília.
[4] Coordenadora de Pesquisa do Observatório da LGPD da Universidade de Brasília.

OS LIMITES DO EXERCÍCIO DO PRINCÍPIO DA FINALIDADE NA LGPD E NO RGPD

Gabriel de Araújo Oliveira[1]

Dispositivos da LGPD	Dispositivos do RGPD
Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: **I – finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;	**Art. 5 -** Princípios relativos ao tratamento de dados pessoais. **1.** Os dados pessoais são: **b)** Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («limitação das finalidades»

Introdução

A construção da Lei Geral de Proteção de Dados Pessoais (LGPD) remonta a um período em que o Brasil estava estagnado na seara legislativa. Não obstante os avanços na seara de proteção de dados a partir de leis esparsas,[2] os projetos e iniciativas nacionais anteriores à edição da LGPD que buscavam unificar a matéria não lograram êxito.

Enquanto países como a Alemanha, França, Espanha e Estados Unidos (DONEDA; MENDES, 2018) já ostentavam uma cultura de proteção de dados, oriunda de fluxos jurídicos a partir da década de 1970, o Brasil deu os primeiros passos rumo à criação de um marco regulatório abrangente e geral apenas no século XXI (DONEDA, 2021).

Como parte dessa construção, verificou-se a influência do Regulamento Geral sobre a Proteção de Dados (RGPD) na LGPD. A iniciativa europeia foi essencial para forçar a adequação de países como o Brasil à tendência global no sentido da proteção de dados pessoais.

[1] Bacharel e mestrando em Direito pela Universidade de Brasília (UnB). Pesquisador do Observatório da LGPD. Advogado na Bento Muniz advocacia.

[2] O Código de Defesa do Consumidor (Lei n. 8.078/1990), o Código Civil (Lei n. 10.406/2002), a Lei do Cadastro Positivo (Lei n. 12.414/2011), a Lei de Acesso à Informação Pública (Lei n. 12.527/2011) e o Marco Civil da Internet (Lei n. 12.965/2014).

Nesse contexto, o presente trabalho abordará uma parte comum entre os diplomas legais, a saber, o princípio da finalidade. Pretende-se por meio de estudo comparado entre o RGPD e a LGPD analisar o referido princípio para, em seguida, examinar casos concretos do Brasil e da Europa para compreender como se dá a sua aplicação.

1. Comentários

Entre os diversos princípios presentes nas normas de proteção de dados existentes a nível mundial, o princípio da finalidade (LGPD) ou limitação da finalidade (RGPD) distingue-se como um princípio-chave, considerado o primeiro passo na aplicação da lei de proteção de dados. Afinal de contas, o tratamento de dados objetiva a satisfação de interesses públicos ou privados que, em regra, devem ser revelados ao interessado.

O titular de dados pessoais, principal interessado e indivíduo protegido pelo ordenamento jurídico, tem resguardado o direito a um tratamento pautado pela boa-fé objetiva e transparência (BRASIL, 2018; UNIÃO EUROPEIA, 2016). Por conseguinte, é necessária a adequação da finalidade escolhida à noção de tratamento justo (*fair processing)* para obstar efeitos indesejados e/ou indevidos para o interessado.

O princípio da finalidade busca, em especial, estabelecer limites à destinação conferida aos dados pessoais coletados, para que possam ser utilizados segura e fielmente ao propósito inicial, bem como no tratamento posterior. No entanto, não significa que a simples necessidade de observância ao princípio da finalidade é capaz de enrijecer a atuação do responsável pelo tratamento de dados pessoais.

Se por um lado as legítimas expectativas do titular de dados devem ser levadas em conta para garantir a segurança jurídica e a previsibilidade do tratamento, de outro os dispositivos jurídicos ora comparados cuidaram de flexibilizar esse procedimento para possibilitar uma abordagem mais pragmática (DONEDA; MENDES, 2018). Isto é, buscou-se conciliar os interesses do titular e do responsável pelo tratamento de dados, de modo a propiciar o tratamento para outras finalidades inicialmente não determinadas, desde que compatíveis com as originais.

Sendo a Lei Geral de Proteção de Dados relativamente recente e inédita no contexto jurídico brasileiro, naturalmente passou por uma série de modificações legislativas até ser promulgada e completamente aplicável no território nacional (DONEDA, 2021). Não sendo

diferente, os estudos sobre determinados aspectos da LGPD ainda são incipientes, como é o caso dos princípios. Neste caso, a construção ocorre gradualmente por meio de debates travados na academia, do estabelecimento de diretrizes pela Autoridade Nacional de Proteção de Dados (ANPD) e, não menos importante, pela consolidação de jurisprudência por parte dos Tribunais.

Por esse motivo, para fins deste trabalho, empregou-se de forma recorrente entendimentos pacificados a respeito do tema no âmbito da União Europeia, em especial aqueles expressos no "Parecer 3/2013 Sobre Limitação da Finalidade" elaborado pelo Grupo de Trabalhos do Artigo 29º [3] da Diretiva 95/46/CE, adotado em 2 de abril de 2013.

Vale frisar, por fim, que embora desenvolvido previamente ao advento do RGPD, as lições do Parecer 3/2013 permanecem atuais e servem de fonte para países como o Brasil, que está no estágio de compreender as possíveis interpretações e aplicações dos dispositivos da LGPD, que, como dito, inspira-se sobremaneira no RGPD.

2. Primeiro Pilar: finalidades determinadas

O primeiro pilar refere-se aos requisitos intrínsecos ao princípio da finalidade, os quais são indispensáveis à proteção do titular e à verificação da conformidade e do cumprimento da função associada ao propósito da coleta de dados. Por inspiração direta no modelo desenhado pelo RGPD (BIONI; MENDES, 2019), a LGPD adotou redação similar ao dispor que as finalidades devem ser específicas, explícitas, legítimas e informadas. A diferença, conforme será visto adiante, consiste na adição do requisito "informada", que traz mais robustez e segurança ao processamento de dados.

Tanto o legislador brasileiro quanto o europeu optaram por conferir aos requisitos caráter mandamental e vinculante. Por esse motivo, a definição da finalidade pelo provedor leva em consideração todos os quatro requisitos da LGPD e os três do RGPD. A escolha não foi ao acaso, o objetivo é justamente a vinculação do tratamento de dados à finalidade que motivou a coleta (DONEDA; MENDES, 2018), impedindo o surgimento de lacunas que de alguma maneira possam vulnerabilizar e/ou lesar o titular, antes ou durante o tratamento.

[3] Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e de privacidade. As suas atribuições estavam descritas no artigo 30º da Diretiva 95/46/CE e no artigo 15º da Diretiva 2002/58/CE. Após a revogação da Diretiva 95/45/CE pelo Regulamento Geral sobre a Proteção de Dados, o Grupo de Trabalho do Artigo 29º foi substituído pelo Comitê Europeu para a Proteção de Dados, órgão da União Europeia, independente e dotado de personalidade jurídica.

A determinação ou especificação da finalidade, em primeiro lugar, representa condição prévia para identificação do fim pretendido com a coleta de dados pessoais. A partir de análise preliminar, é possível saber se a finalidade definida está em conformidade com a lei e quais as garantias necessárias devem ser aplicadas na defesa do titular (ARTICLE 29 WORKING PARTY, 2013).

Em regra, a finalidade deve ser determinada em momento anterior à coleta de dados pessoais, jamais posteriormente. Isso porque a relação entre titular e responsável pelo tratamento de dados pessoais é em si desigual, logo, a LGPD e o RGPD preveem formas de proteger o primeiro – neste caso, através do entendimento que o particular precisa ter conhecimento inequívoco desde o início do porquê da coleta. Caso contrário, a proteção pretendida teria pouca ou nenhuma efetividade.

Considerando que a determinação da finalidade assume contornos de especificidade e clareza, o nível de detalhes e o grau de precisão importam para identificar se uma finalidade de fato é determinada. Uma finalidade que é vaga ou geral como, por exemplo, nos casos em que o objetivo é "melhorar a experiência do usuário", dificilmente seria vista como específica.

No entanto, cada situação precisa ser avaliada à luz do caso concreto, porque nem sempre mais detalhes significam melhores resultados. Na realidade, a quantidade excessiva de detalhes em circunstâncias pontuais pode até ser contraproducente. A ponderação entre os meios necessários para atingir determinados fins indica quando mais ou menos detalhes são pertinentes (ARTICLE 29 WORKING PARTY, 2013).

Sob outra perspectiva, o comando que sublinha que as finalidades devem ser explícitas assinala implicitamente que todos os envolvidos no tratamento de dados e terceiros estarão em posição de equivalência. Ou seja, as finalidades devem ser expressas de tal modo que possam ser compreendidas da mesma forma por todos, incluindo o titular de dados, as autoridades de proteção de dados e os subcontratantes – independentemente das suas qualificações culturais ou linguísticas, grau de compreensão ou deficiências.

O requisito que exige que as finalidades sejam determinadas explicitamente, assim como a própria especificação da finalidade, pretende conferir transparência e previsibilidade ao procedimento a partir da imposição de limites aos responsáveis pelo tratamento na utilização dos dados coletados. Deste modo, pela limitação da atuação dos responsáveis pelo tratamento,

minimizam-se os riscos e evita-se uma possível desvirtuação do propósito inicialmente determinado.

A flexibilidade é um ponto importante quando tratamos do princípio da finalidade. Se o objetivo principal da norma é a proteção dos dados do titular, as disposições legais não podem engessar o processo de tratamentos, mas antes torná-lo seguro e prático ao interessado (particular), simplificando-o, notadamente, através de meios adequados.

As formas como as finalidades podem ser expressas são diversas. Enquanto avisos e notificações são encarados como meios comuns e, no geral, aceitáveis para explicitar as finalidades do tratamento, outros alternativos e complementares são igualmente apropriados – como se vê, por exemplo, na legislação, nas declarações públicas e no fornecimento direto de informação aos titulares (ARTICLE 29 WORKING PARTY, 2013). Tudo isso não dispensa, por óbvio, a produção de documentos escritos.

O último dos requisitos para definição da finalidade, comum à LGPD e ao RGPD, diz que os dados devem ser recolhidos para fins legítimos. Isto é, a finalidade escolhida deve estar em conformidade com a lei, em seu sentido *lato*, abrangendo aqui não apenas as normas frutos do poder legislativo federal, estadual e municipal, mas também os atos do Poder Executivo, os princípios de Direito e a jurisprudência. Em alguns casos, até elementos como o costume, códigos de conduta, códigos de ética, cláusulas contratuais, entre outros, também podem ser considerados.

A inovação por parte da lei brasileira consiste no acréscimo do requisito que enuncia que as finalidades devem ser informadas, previsão que não consta expressamente no RGPD. Nesse sentido, a finalidade deve ser suficientemente informada, inexistindo dúvida por parte do titular de dados quanto ao propósito inicial ou posterior do tratamento.

De modo similar à noção de consentimento informado presente no RGPD, o reforço dado pelo legislador brasileiro ao princípio da finalidade, que é tão importante dentro do sistema protetivo de dados e é responsável por nortear as análises de conformidade, indica a necessidade de o provedor informar que os dados estão sendo coletados e o propósito pretendido.

A compreensão por parte do titular a respeito da coleta e o do tratamento apresenta-se em conformidade com o objetivo primordial da lei de proteção de dados, tendo em vista o caráter duplo de informar que inclui a possibilidade do provedor ser demandado diretamente

pelo titular – seja para acesso, retificação, cancelamento e/ou oposição – e de obstar práticas abusivas a partir da adoção de medidas compatíveis com a legislação.

Os requisitos acima examinados constituem a primeira parte do princípio da finalidade, o qual ainda elenca como exigência a utilização compatível com o propósito inicial, conforme será visto no próximo tópico.

3. Segundo Pilar: Utilização Compatível

Conforme mencionado anteriormente, a previsibilidade e a transparência são dois elementos essenciais na definição da finalidade, porque promovem a segurança e asseguram que as legítimas expectativas do titular de dados serão atendidas, reduzindo, por conseguinte, os possíveis riscos referentes a um tratamento distinto do esperado e/ou informado.

Para tanto, faz-se necessário definir parâmetros mínimos capazes de instruir o responsável pelo tratamento, o titular de dados e terceiros interessados a responder a seguinte pergunta: o tratamento é compatível com a finalidade informada? Temos, inicialmente, que tanto a LGPD, em seu art. 6º, I, e o RGPD, no art. 5º, nº 1, alínea b), proíbem expressamente o tratamento posterior de forma incompatível com as finalidades originais.

Todavia, enquanto o RGPD delineia no art. 6º, nº 4, alíneas a) a e) aspectos a serem considerados na aferição da compatibilidade na utilização posterior, a LGPD é omissa na explicação do que, afinal, é um tratamento incompatível e como podemos identificá-lo. Ao que parece, a tarefa caberá à autoridade nacional e aos doutrinadores.

No âmbito da União Europeia, o Parecer 3/2013 Sobre Limitação da Finalidade (ARTICLE 29 WORKING PARTY, 2013) traz importantes ensinamentos sobre a compatibilidade da finalidade posterior. Ambos os legisladores, brasileiro e europeu, optaram por proibir a incompatibilidade em vez de impor um requisito de compatibilidade, com a pretensão de conferir flexibilidade à utilização posterior. Isso quer dizer que um tratamento posterior com finalidade diferente pode não ser incompatível.

Nesse sentido, a avaliação de compatibilidade se apresenta como meio de aferir a conformidade do tratamento posterior. O critério de avaliação divide-se em formal, que valoriza a comparação entre as finalidades iniciais e as posteriores para examinar a compatibilidade, e substantivo, que para além de considerar os termos iniciais e posteriores, analisa o contexto e outros fatores para entender como são ou deveriam ser as finalidades. Desta maneira, temos

critérios mais rígidos e com tendência a ser mais legalista (formal) e mais flexíveis com tendência a ser mais pragmático (substantivo).

O Grupo de Trabalho do Artigo 29º elaborou, com base nos critérios utilizados pelos Estados Membros da União Europeia, rol exemplificativo de fatores-chaves a considerar durante a avaliação de compatibilidade, a saber, (i) a relação entre as finalidades para as quais os dados foram recolhidos e as finalidades do tratamento posterior; (ii) o contexto no qual os dados foram recolhidos e as expectativas razoáveis das pessoas em causa quanto à sua utilização posterior; (iii) a natureza dos dados e o impacto do tratamento posterior sobre as pessoas em causa e (iv) as garantias aplicadas pelo responsável pelo tratamento para assegurar um tratamento leal e para impedir quaisquer impactos indevidos sobre as pessoas em causa.

Os fatores-chaves supramencionados foram incorporados ao art. 6º, número 4, do RGPD, oferecendo, assim, diretrizes a respeito do tratamento posterior. A LGPD, ao contrário, é silente sobre essa matéria.

O RGPD privilegiou o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, ao prever no fim do art. 5, número 1, alínea b, que esse tratamento não é considerado incompatível com as finalidades iniciais, em conformidade com ao artigo 89, n.º 1.

O aludido artigo autoriza o tratamento para fins históricos, estatísticos ou científicos, desde que o responsável pelo tratamento compense esta mudança com a aplicação de garantias adequadas e certifique que os dados não serão utilizados para aprovar medidas ou decisões relativas aos titulares. Entre as medidas de segurança, a anonimização ou pseudoanonimização dos dados são as mais comuns para evitar que, sempre que possível, os titulares não possam ser (re)identificados.

O legislador brasileiro preferiu classificar esse tipo de finalidade posterior enquanto uma base legal (art. 7º, IV), enquadrando-a como "estudos por órgão de pesquisa" consoante definição atribuída pelo art. 5º, XVIII da LGPD[4]. Tal qual o regulamento europeu, a LGPD prevê a adoção de medidas de segurança – especificamente a anonimização – como garantia do tratamento de dados. Portanto, as abordagens distinguem-se à medida que no RGPD o

[4] Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

tratamento para fins históricos, estatísticos ou científicos é considerado uma autorização para o tratamento posterior, ao passo que o equivalente na LGPD compreende uma das bases legais.

Por fim, insta salientar que ambos os dispositivos preveem exceções que limitam a aplicação das regras e princípios, bem como o exercício de direitos e obrigações. São casos, por exemplo, de tratamento de para fins de segurança pública (art. 4º, III, alínea a) da LGPD; art. 23, nº 1, alínea c) do RGPD), defesa nacional (art. 4º, III, alínea b) da LGPD; art. 23, nº 1, alínea b) do RGPD), segurança do Estado (art. 4º, III, alínea c) da LGPD; art. 23, nº 1, alínea a) do RGPD) e atividades de investigação e repressão de infrações penais (art. 4º, III, alínea d) da LGPD; art. 23, nº 1, alínea d) do RGPD).

As normas protetivas vão além ao incluir outras hipóteses que afastam parcial ou completamente a incidência da lei ou do regulamento no tratamento de dados pessoais. Nesse sentido, quando o tratamento é realizado por pessoa natural para fins exclusivamente particulares e não econômicos, bem como para fins exclusivamente jornalísticos, artísticos ou acadêmicos, a LGPD não se aplica.

Por sua vez, o RGPD elenca rol mais extenso que abrange a limitação nos casos de defesa da independência judiciária e dos processos judiciais; da prevenção, investigação, detecção e repressão de violações da deontologia de profissões regulamentadas; da defesa do titular dos dados ou dos direitos e liberdades de outrem; da execução de ações cíveis, etc.

Na prática, a observância dos requisitos da finalidade e da utilização posterior compatível entrelaçam-se dentro da análise de conformidade realizada caso a caso. As noções sobre o princípio da finalidade ganham forma a partir do impulsionamento da máquina judiciária, poder responsável por garantir a correta aplicação das normas protetivas.

Deste modo, a fim de ilustrar o quanto exposto, a seguir serão realizados breves estudos de casos tendo como parâmetro decisões judiciais que discutem, ainda que tangencialmente, o princípio da finalidade.

4. Estudos de Caso

Dados mostram que um ano após a entrada em vigor da Lei Geral de Proteção de Dados, a Lei nº. 13.709/18, a justiça brasileira já proferiu mais de 600 decisões tendo como base este

dispositivo legal.[5] O número de demandas judiciais comprova o anseio da população e a necessidade da lei de proteção de dados no contexto de elevada circulação de informações dentro da economia movida a dados.

As normas da lei de proteção de dados carecem de lapidação e, sendo assim, o Poder Judiciário exerce função essencial consistente na interpretação e aplicação dos dispositivos. Em razão da novidade normativa, o cenário ainda é incipiente, porém, a tendência é que à medida que situações variadas forem apresentadas ao Poder Judiciário, mais posicionamentos consolidados teremos.

4.1. Caso Ministério Público do Distrito Federal e Territórios vs. Serasa Experian – Comercialização ilegal de dados pessoais

No ano de 2020, o Ministério Público do Distrito Federal e Territórios (MPDFT) ajuizou Ação Civil Pública[6] em desfavor da Serasa S/A (Serasa Experian), aduzindo, em síntese, que a empresa comercializava de forma ilegal/irregular dados pessoais de aproximadamente 150 milhões de brasileiros.

Na peça exordial, o *Parquet* narra que através dos serviços "Lista Online" e "Prospecção de Clientes", a Serasa Experian vendia dados de pessoais naturais, tais como CPF, nome, endereço, telefones e sexo, a um custo de R$ 0,98 (noventa e oito centavos). Ademais, alega que o serviço oferecia a possibilidade de segmentar grupos específicos por meio do uso de filtros, tais como sexo, idade, poder aquisitivo, classe social, localização, modelos de afinidade e triagem de risco. O ente ministerial alerta para os riscos de dano atrelado à prática de comercialização, que no caso não contava com o consentimento expresso dos titulares de dados.

A Serasa Experian, em sede de contestação, refutou as alegações apresentadas pelo MPDFT, argumentando que os serviços oferecidos não eram novos, inclusive já haviam sido objeto de ações judiciais[7] e contavam com convalidação do Poder Judiciário. Além disso, afirmou que os serviços estariam em conformidade com a LGPD, logo, não geravam risco de dano para os consumidores.

---

[5] SOPRANA, Paula. Justiça já tem 600 decisões envolvendo lei de proteção de dados. Folha. Disponível em: <https://www1.folha.uol.com.br/mercado/2021/07/justica-ja-tem-600-decisoes-envolvendo-lei-de-protecao-de-dados.shtml>. Acesso em 14 de set. 2021.

[6] Processo n. 0736634-81.2020.8.07.0001, em curso na 5ª Vara Cível de Brasília do Tribunal de Justiça do Distrito Federal e Territórios (TJDFT).

[7] Ações nº 0220078-81.2014.8.21.0001 e 028331674-2014.8.21.000, ambas no Estado do Rio Grande do Sul.

Em sede de cognição sumária, o Juízo de origem indeferiu o pedido de tutela antecipada formulado pelo MPDFT, sob a justificativa que a base legal do legítimo interesse autorizaria a hipótese de tratamento de dados exposta. Nas palavras do magistrado:

> [...] esses elementos interessam ao desenvolvimento econômico, à livre iniciativa, à livre concorrência e, portanto, à própria defesa do consumidor (art. 2º, incisos V e VI, da Lei 13.709/18), na medida em que são indispensáveis à proteção ao crédito e, também, à catalisação e formalização de relações comerciais aptas a atingir o seu almejado adimplemento, mediante informações prévias, claras, objetivas e transparentes acerca das características pessoais dos contratantes.[8]

O julgador prossegue pontuando que em razão dos dados não compreenderem elementos sigilosos ou confidenciais (consiste exclusivamente em informações públicas ou de natureza cadastral) e por não se tratar de dados sensíveis, afasta-se a necessidade de consentimento expresso do titular para compartilhamento com terceiros, sendo possível o tratamento com base no art. 7º, incisos IX e X, da Lei nº. 13.709/18.

No entanto, o entendimento da origem não foi ratificado pela instância recursal. O MPDFT interpôs agravo de instrumento[9] em face da decisão denegatória, devolvendo para o Tribunal o enfrentamento da questão objeto da decisão agravada.

O relator do agravo de instrumento compreendeu que a prática de comercialização de dados pessoais sem o consentimento, ainda que não se trate de dados sensíveis, fere a LGPD, com potencial para ensejar violação à privacidade, intimidade e imagem das pessoas.

Os dados pessoais de natureza cadastral dificilmente poderiam ser enquadrados como manifestamente públicos, consoante o art. 7º, § 4º, da LGPD, uma vez que são fornecidos exclusivamente à Serasa Experian. Portanto, a comercialização desses dados com terceiros sem a devida autorização macula o processo de tratamento de dados, bem como desvia dos fins inicialmente especificados sem que haja as adaptações exigidas, senão vejamos:

[8] Processo n. 0736634-81.2020.8.07.0001, em curso na 5ª Vara Cível de Brasília do Tribunal de Justiça do Distrito Federal e Territórios (TJDFT).
[9] Processo n. 0749765-29.2020.8.07.0000, em curso no Tribunal de Justiça do Distrito Federal e Territórios (TJDFT).

> Não é influente a alegação da agravada (Serasa Experian), de que obteve diretamente os dados do próprio titular (salvo a hipótese de fornecimento do consentimento deste) ou se obteve as informações de outro controlador, uma vez que, evidentemente, ao fornecer os dados o titular o fez para fins específicos, não se podendo presumir haver aquiescência a que esses dados sejam compartilhados como tem sido feito, porquanto, como já dito, não se pode extrair que tenham sido tornados públicos de forma ampla e irrestrita a ponto de poderem ser comercializados.

Destaca-se, ainda, parte do julgado em que são sopesados as finalidades e o legítimo interesse da Serasa Experian de um lado, e de outro, as legítimas expectativas, os interesses e a proteção aos milhões de brasileiros que constam na base de dados da empresa. A partir dessa análise, o relator concluiu, com fundamento no art. 7º da LGPD, que o consentimento é a regra maior a ser observada para o tratamento de dados pessoais.

Ao adotar os fundamentos fáticos e jurídicos do Relator do agravo de instrumento, o Juízo de 1ª instância salientou a importância de se observar os princípios gerais da LGPD, sobretudo o da finalidade. Embora o tratamento posterior em si não seja vedado pela legislação, exige-se que seja compatível com a finalidade inicial e que esteja amparado em uma das bases legais do art. 7º da LGPD.

Observa-se no caso narrado que a empresa utilizou os dados coletados para atividade posterior incompatível com a finalidade original, a saber, comercialização/transferência de dados cadastrais, o que na hipótese requer outra base legal. A interpretação do Tribunal de Justiça do Distrito Federal e Territórios foi no sentido de rechaçar o legítimo interesse como base legal, tendo em vista o risco às legítimas expectativas e aos interesses dos titulares. Portanto, a base legal que melhor se adequa à situação é o consentimento, conforme o art. 7º, § 5º da LGPD.

4.2. Caso Orange România S/A v. Autoridade Nacional de Supervisão do Tratamento de Dados Pessoais (Romênia) – Armazenamento ilegal de dados pessoais

Lado outro, no âmbito da União Europeia, foi levado à apreciação do Tribunal de Justiça da União Europeia (TJUE) pedido de decisão prejudicial[10] apresentado pelo *Tribunalul*

[10] Previsto nos artigos 19º, n.º 3, alínea b), do Tratado da União Europeia e no artigo 267º do Tratado sobre o Funcionamento da União Europeia, o reenvio prejudicial é um mecanismo fundamental do direito comunitário europeu. O mecanismo visa garantir a interpretação e a aplicação uniformes deste direito na União, oferecendo aos órgãos jurisdicionais dos Estados-Membros um instrumento que lhes permite submeter ao Tribunal de Justiça da

Bucureşti (Tribunal Regional de Bucareste, Romênia) a respeito da coleta e do armazenamento de dados no contexto de negociações contratuais.

Na origem, a Orange România S/A, empresa prestadora de serviços de telecomunicações, insurgiu-se contra a aplicação de multa pela *Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal* (Autoridade Nacional de Supervisão do Tratamento de Dados Pessoais, Romênia), por alegação de violação ao artigo 32º[11] cumulado com o artigo 8º[12] da Lei nº. 677/2001,[13] em razão do armazenamento indevido de cópias de documentos de identificação dos seus clientes sem o consentimento expresso destes.

Como prática de negócio, a Orange România celebrava na sua sede contratos escritos objetivando a prestação de serviços de telecomunicações móveis, de modo que aos contratados eram anexados documentos de identificação. O conteúdo desses contratos incluía notadamente uma declaração de fato assinalando que o cliente tinha sido informado e consentido com a coleta e o armazenamento de cópias dos seus documentos de identificação. Impende destacar que o consentimento era dado através da aposição de cruzes em caixas que figuravam nas cláusulas contratuais.

De acordo com a autoridade nacional, a Orange România não comprovou que os clientes tivessem feito uma escolha informada relativamente à coleta e armazenamento das cópias dos documentos de identificação. Portanto, a empresa não cumpriu com um dos requisitos para a adoção do consentimento como base legal para esse tratamento, isto é, o consentimento supostamente não estaria sendo informado.

União Europeia, a título prejudicial, questões relativas à interpretação do direito da União ou à validade dos atos adotados pelas instituições, órgãos ou organismos da União. Recomendações à atenção dos órgãos jurisdicionais nacionais, relativas à apresentação de processos prejudiciais.
Tribunal de Justiça da União Europeia. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016H1125(01)&from=PT >. Acesso em: 2 de outubro de 2021.

[11] Em tradução livre: "O tratamento de dados pessoais por operador ou por pessoa por ele habilitado, em violação do disposto no art. 4-10 ou desconsiderando os direitos previstos no art. 12-15 ou no art. 17, constitui contravenção, se não for cometida em condições que constituam crime, e for sancionada com multa de 10.000.000 lei a 250.000.000 lei".

[12] Em tradução livre: "1. O tratamento de código numérico pessoal ou outros dados pessoais com função de identificação de aplicabilidade geral só pode ser realizado se: a) o titular dos dados deu expressamente o seu consentimento; ou b) o tratamento esteja expressamente previsto em dispositivo legal. 2. A autoridade de supervisão pode estabelecer outros casos em que o tratamento dos dados fornecidos no par. (1), apenas na condição de serem criadas salvaguardas adequadas para respeitar os direitos das pessoas em causa".

[13] Relativa à Proteção das Pessoas no que concerne ao Tratamento de Dados Pessoais e à Livre Circulação desses Dados, destinou-se a transpor as disposições da Diretiva 95/46 para o direito nacional. Disponível em: <http://legislatie.just.ro/Public/DetaliiDocument/32733> . Acesso em: 2 de outubro de 2021.

Conquanto a discussão gire em torno do consentimento do titular de dados, não se olvida que o princípio da finalidade está intrinsicamente conectado a esta base legal, uma vez que o titular consente com o tratamento dos seus dados para uma ou mais finalidades específicas, consoante preconiza o artigo 6.º, n.º 1, alínea a), do RGPD.

Em uma análise sistemática, o tratamento de dados em desconformidade com os requisitos da base legal consentimento pode também implicar na incompatibilidade com o princípio da finalidade. Isso porque o consentimento é concedido para finalidade(s) específica(s), a(s) qual(is) deve(m) ser de conhecimento inequívoco do titular e observada pelo provedor.

No caso ora apresentado, a empresa Orange România deixou de informar devidamente aos seus clientes sobre o armazenamento dos documentos de identificação, o que ao entender do TJUE violou o Regulamento Europeu porque "cabe ao responsável pelo tratamento dos dados demonstrar que a pessoa em causa manifestou, através de um comportamento ativo, o seu consentimento para o tratamento dos seus dados pessoais e obteve previamente uma informação a respeito de todas as circunstâncias relacionadas com esse tratamento".

Considerações Finais

Como exposto, o princípio da finalidade (LGPD) ou limitação da finalidade (RGPD) representa importante princípio dentro do sistema protetivo de dados do Brasil e da Europa, ao estabelecer limites ao modo como os provedores podem usar os dados dos titulares de dados (interessados), à medida que oferece certo grau de flexibilidade no tratamento.

Não obstante a diferença de cenários, é notável que o Brasil se esforça para seguir o caminho de adequação ao RGPD, considerando o contexto de amplo desenvolvimento dos países europeus no tocante à matéria de princípios de proteção de dados. Como exemplos maiores, temos os documentos elaborados pelo Comitê Europeu e a vasta jurisprudência dos Tribunais Nacionais e do Tribunal de Justiça da União Europeia.

Observam-se inúmeras semelhanças entre os diplomas legais ora estudados, entre as quais estão os requisitos (as finalidades devem ser específicas, explícitas e legítimas), a necessidade de utilização compatível, seja em relação à finalidade inicial ou posterior, bem como hipóteses para limitação da aplicação das regras e princípios.

No entanto, as diferenças decorrem da própria pretensão dos textos legais, sendo o RGPD uma extensa e detalhada fonte do direito comunitário europeu, a qual atualiza e sucede a Diretiva 95/46/CE, sendo aplicável a mais de 20 países. Em contrapartida, a LGPD apresenta-se como uma norma mais concisa, porém robusta, com pretensão inédita de unificação da matéria no cenário nacional e inspiração direta no RGPD.

Frisam-se como diferenças a adição do requisito "informada" à LGPD, que traz mais robustez e segurança ao processamento de dados, um rol maior de hipóteses para limitação aplicação das regras e princípios do RGPD e a classificação do tratamento para fins históricos, estatísticos ou científicos como utilização posterior no RGPD e como uma base legal na LGPD.

Deste modo, partindo do pressuposto da existência de disparidade entre o cenário europeu e o brasileiro, compreende-se que o princípio da finalidade teve até o momento mais oportunidade de desenvolvimento na Europa, em decorrência dos fluxos comunitários e internacionais dos anos 80 e 90 – em prol da harmonização de entendimentos e convergência de normas – que o consolidaram um princípio basilar no que diz respeito ao processamento de dados pessoais. Isso significa dizer que os desafios advindos do cenário brasileiro moldarão a percepção e a aplicação do princípio da finalidade no futuro, fazendo com que as discussões suscitadas se transformem em fonte de entendimento deste princípio basilar.

Referências bibliográficas

ARTICLE 29 WORKING PARTY. Opinion 03/2013 on purpose limitation. Bruxelas: [s. n.], 2013. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em: 21 out. 2021.

BIONI, Bruno; MENDES, Laura Schertel. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados brasileira: mapeando convergências na direção de um nível de equivalência. Revista de Direito do Consumidor, São Paulo, v. 28, n. 124, p. 157-180, jul./ago. 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República; 2018 [Acesso em 12.jun.2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a

Diretiva 95/46/CE . Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 18 ago. 2021.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021, p. 3-20.

DONEDA, Danilo; MENDES, Laura Schertel. Reflexões iniciais sobre a nova lei geral de proteção de dados. Revista dos Tribunais: Revista de Direito do Consumidor, vol. 120/2018, p. 469 – 483, Nov - Dez/2018.

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscila (Coords.). Lei Geral de Proteção de Dados – Caderno Especial. São Paulo: Revista dos Tribunais, 2019. p. 35-56

O PRINCÍPIO DA NECESSIDADE NO ÂMBITO DA LGPD E DOA RGPD: TEORIA E PRÁTICA

Gabriel Cabral Furtado[1]

Dispositivos da LGPD	Dispositivos do RGPD
Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: **III** – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;	**Art. 5** - Princípios relativos ao tratamento de dados pessoais **1.** Os dados pessoais são: **c)** Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (‘minimização dos dados’).

Introdução

É inegável a relevância dos princípios jurídicos para a interpretação e para a aplicação do direito. São os princípios, nas importantes palavras de Humberto Ávila (2019), espécie de normas jurídicas de caráter finalístico que prescrevem conteúdos relacionados à conduta humana. Desse modo, atuam fundamentalmente no estabelecimento das principais balizas para a aplicação das demais normas, cuja interpretação é concretizada a cada caso.

No âmbito da Lei Geral de Proteção de Dados (Lei n° 13.709/2018), que foi elaborada tendo por base o imprescindível equilíbrio entre a crescente necessidade de proteção dos titulares de dados pessoais e o desenvolvimento econômico-inovador, os princípios estão descritos em seu artigo 6° e possuem incidência horizontal a todos os seus dispositivos. Por seu turno, na esfera do Regulamento Geral sobre a Proteção de Dados (RGPD), que objetiva sobretudo reforçar e unificar a proteção de dados pessoais na União Europeia, os princípios norteadores constam no artigo 5°.

Nesse contexto, o presente artigo se propõe a analisar, sob os vértices teórico e prático, o princípio da necessidade ou minimização (*data minimisation*), expressamente previsto no inciso III do art. 6° da normativa brasileira e na alínea “c” do item 1 do art. 5° da normativa

[1] Bacharel em Direito na Universidade de Brasília (UnB). Integrante do grupo de pesquisa Observatório da LGPD.

europeia. Buscar-se-á, nesse caminho, (i) tecer comentários doutrinários acerca do princípio supramencionado, abrangendo-se a jurisdição nacional e a europeia; e, posteriormente, (ii) examinar um caso nacional – a Ação Direta de Inconstitucionalidade n° 6.387 – e outro estrangeiro – "*TK" vs. Associação dos condóminos do edifício M5A –*, a fim de compreender como o princípio da necessidade vem sendo aplicado na prática jurídica em âmbito territorial e internacional.

1. Comentários

Os princípios da LGPD constituem verdadeira condição de legitimidade para o tratamento de dados, de modo a refletir a essência do diploma e propriamente justificar a coleta, o compartilhamento e o processamento de dados. Servem, nesse caminho, como barreira legal de modulação à conduta do agente de tratamento de dados, inserido em um modelo *ex ante* de proteção.

De modo mais atido ao escopo deste artigo, o princípio da necessidade, alçado no parágrafo III do artigo 6° da LGPD, consiste em uma limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos. Portanto, o intento é de justamente tratar o mínimo possível de dados, em uma concepção que objetiva, sobretudo, controlar e eventualmente bloquear o uso incondicional de dados pessoais.

Nessa esteira, é notório que o princípio da necessidade manifestamente se conecta a outros princípios. Primeiramente, cumpre pontuar que ele limita o princípio da eficiência[2], vez que coletar mais dados que o estritamente necessário é um obstáculo à obtenção de resultados rápidos e precisos buscados pela Administração Pública, de sorte a gerar prejuízo ao titular dos dados e aos demais afetados. Além disso, está ligado ao princípio da finalidade[3], haja vista que a sua coleta só pode ocorrer tendo em conta, rigorosamente, a finalidade por ela pretendida, rejeitando a captação excessiva.

[2] Alçado no art. 37 da Constituição Federal de 1988, cuida-se de um dos princípios constitucionais regentes do Direito Administrativo, segundo o qual a administração pública deve, na atuação de suas atividades, racionalizar os meios para atingir os fins. *In verbis*: Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e **eficiência** e, também, ao seguinte (...). (grifos nossos).

[3] Previsto no art. 6°, I da LGPD. Veja: Art. 6º. (...): I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Ademais de expressamente previsto no artigo 6°, III da LGPD, releva pontuar que o princípio da necessidade está também contemplado no artigo 18, IV do mesmo diploma, que evidencia o direito do titular em requisitar a "anonimização, bloqueio ou eliminação de **dados desnecessários, excessivos ou tratados em desconformidade***".* Sob outro vértice, o mesmo princípio baliza uma das formas de tratamento de dados sensíveis que dispensa o consentimento do titular, qual seja o compartilhamento de dados necessários à execução de políticas públicas, consoante previsto na alínea b do inciso II do art. 11, *in verbis*:

> **Art. 11**. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> **II** – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> **a)** tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

No assunto, a doutrina propõe relevante divisão na compreensão do princípio da necessidade. Nesse rumo, diz-se que a minimização se divide em sentido estrito – o qual diz respeito ao tratamento da menor quantidade de dados possível para uma finalidade específica – , e sentido *lato* – que se relaciona à articulação de medidas de salvaguardas[4] que ambicionam mitigar os riscos para os direitos fundamentais dos titulares. Nesse sentido, há um dever de cuidado duplo, que provoca dois juízos diferentes: um em torno da menor intrusividade do tratamento de dados, outro acerca da menor lesividade (BIONI; RIELLI; KITYAMA, 2021).

A vertente da menor intrusividade, em palavras gerais, envolve a verificação de outros tipos de dados menos intrusivos, disponíveis ao controlador, os quais poderiam ser eventualmente utilizados para atingir as mesmas finalidades pretendidas. Sobre o assunto, o *Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation* (2017) acuradamente ressalta que o adjetivo "necessário" não é sinônimo de "indispensável", mas também não se traduz na ideia de "útil", "razoável" ou "desejável".

[4] No âmbito da legislação europeia de tratamento de dados, releva mencionar o disposto no Artigo 89, n°1 do RGPD, segundo o qual os controladores e processadores devem implementar medidas técnicas – a saber, garantir a proteção do acesso mediante senha; e da transferência de dados, mediante criptografia – e organizacionais – como o registro de atividades, o treinamento do pessoal, etc. – apropriadas para proteger os direitos e a liberdade dos titulares de dados cujos dados pessoais são coletados e processados para fins de arquivo de interesse público, de investigação científica ou histórica, ou, ainda, estatísticos.

Assim, de forma relacionada à aplicação do legítimo interesse, o modo mais simples de se identificar a necessidade é questionar se existe outra forma de atingir o interesse pretendido, com menor ofensividade sobre os dados pessoais. Se não há ou se há outra forma que, todavia, exija um esforço desproporcional, então pode-se dizer que o processo é necessário. Doutro lado, se houver várias maneiras de atingir o objetivo, é recomendável a realização de um Relatório de Impacto à Proteção de Dados (RIPD)[5] com o propósito de identificar a conduta menos invasiva.

A vertente do possível impacto do tratamento de dados sobre os direitos e liberdades fundamentais dos titulares, sob outro vértice, presta-se a analisar o potencial lesivo do tratamento, para o qual devem ser ajuntadas medidas mitigatórias de riscos, a saber a anonimização e a pseudonimização.[6] Nesse caminho, Bioni, Rielli e Kityama (2021) lecionam que:

> Essa faceta da minimização é extraída do próprio art. 10, inciso II, na medida em que ele condiciona a fundamentação do tratamento no legítimo interesse à, dentre outros elementos, "proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas [...] os direitos e liberdades fundamentais, nos termos desta Lei". Medidas de promoção e proteção dos direitos e liberdades dos titulares, que se enquadram nessa categoria são, por exemplo, a anonimização ou pseudonimização, já que são aptas a mitigar os potenciais impactos negativos de um tratamento de dados pessoais.

De forma semelhante, na normativa europeia (RGPD), o princípio da necessidade equivale ao "princípio da minimização dos dados" e "limitação da conservação", de modo que os dados pessoais deverão ser adequados (suficientes para cumprir adequadamente o seu propósito declarado), pertinentes (racionalmente ligados ao propósito) e limitados ao necessário para os propósitos do tratamento. Segundo esse princípio, os dados pessoais apenas devem ser

[5] Previsto no art. 5º, XVII, da LGPD, cuida-se de uma documentação do agente de tratamento a quem competem as decisões referentes ao tratamento de dados pessoais. *In verbis*: Art. 5º Para os fins desta Lei, considera-se: **XVII - relatório de impacto à proteção de dados pessoais**: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; (grifos nossos)

[6] A LGPD define, no inciso XI do artigo 5°, que a anonimização é a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo". A definição para os dados pseudonimizados, por seu turno, está no artigo 13, §4º do diploma, sendo o "tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro".

tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios.

Assim, caso se verifique que foram solicitados dados em excesso, o tratamento passará a ser ilícito. Cuida-se, nessa hipótese, de contraordenação muito grave, a qual está prevista e sancionada nos termos da alínea "a" do n.º 5 do artigo 83.º do RGPD, senão veja:

> **Art. 83.º (...) 5.** A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.º 2, a coimas até 20000000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado:
> **b)** Os princípios básicos do tratamento, incluindo as condições de consentimento, nos termos dos artigos 5, 6º, 7º e 9º;(...)

É precisamente por isso que o controlador precisa assegurar que o prazo de armazenamento do dado pessoal também seja limitado ao mínimo necessário. Isto é, os dados pessoais precisam ser descartados assim que terminado o tratamento, considerada a oferta do produto ou do serviço[7]. Isso se afirma, pois não é possível, à luz do princípio da necessidade, a coleta massiva de dados pessoais para só depois se pensar nos possíveis usos e destinos dos dados. Nesses casos, ainda, há de se reconhecer a evidente relação proporcional entre a quantidade de dados tratada e a responsabilidade, notadamente em casos de vazamentos e incidentes de segurança.

Nesse contexto, as empresas controladoras e operadoras de dados pessoais efetivamente precisam adotar medidas para se adequarem ao princípio da necessidade – a saber, providenciando o levantamento de todos os dados coletados e tratados (e a varredura dos dados pessoais armazenados e suas respectivas naturezas); a revisão das políticas das referidas coletas; e até o treinamento dos contratados para evitar a coleta desnecessária – e, portanto, ilegal – de dados pessoais. Os responsáveis pelo tratamento, ainda, devem divulgar as categorias de dados pessoais envolvidos no tratamento, de sorte a vinculá-las adequadamente à específica finalidade

[7] Relaciona-se a esse ponto o artigo 17 do RGPD, que explicitamente dispõe acerca do direito ao esquecimento, uma salvaguarda de suma importância para a aplicação dos princípios de proteção de dados, destacadamente o princípio de minimização de dados. *In verbis*: "**Artigo 17° - 1**. O titular dos dados tem o direito de obter do responsável pelo tratamento o apagamento dos dados pessoais que lhe digam respeito sem demora injustificada e o responsável pelo tratamento tem a obrigação de apagar os dados pessoais sem demora injustificada quando se aplique um dos seguintes motivos: **(a)** os dados pessoais não são mais necessários em relação aos fins para os quais foram coletados ou processados de outra forma (...)".

pretendida, nos termos do art. 15º, nº 1, alínea 'b' do RGPD, sob pena de violação aos princípios da minimização de dados e da transparência.

No que concerne à utilização de dados pela Administração Pública, no mesmo caminho, é preferível a adoção de um meio que seja, concomitantemente, menos gravoso para o indivíduo e para o interesse público, ante a evidente inserção na temática de intervenção na privacidade e liberdade individuais. Sobre o tema, dispõe o seguinte trecho do Conseiderando 156 do RGPD:

> As condições e garantias em causa podem implicar procedimentos específicos para o exercício desses direitos por parte do titular de dados, se tal for adequado à luz dos fins visados pelo tratamento específico a par de medidas técnicas e organizativas destinadas a reduzir o tratamento de dados pessoais de acordo com os princípios da proporcionalidade e da necessidade.

Por outro lado, é notório que uma conduta conforme leva, em muitos casos, a uma redução de despesas com segurança de dados. Afinal, apesar de não expressamente prevista nos princípios elencados no art. 6º da LGPD, a proporcionalidade da segurança, como antecipado, também é uma diretriz norteadora do regulamento. Logo, a revisão da estrutura de armazenamento e da segurança de informação – para que sejam adequadas ao tamanho da operação – contribuem duplamente (i) à adequação principiológica; e (ii) à redução de despesas.

2. Estudos de Caso

2.1. Medida Cautelar na Ação Direta de Inconstitucionalidade n° 6.387/ DISTRITO FEDERAL

Em âmbito nacional, a temática principiológica da LGPD foi tratada pela Corte Suprema em sede do julgamento da medida cautelar pleiteada na Ação Direta de Inconstitucionalidade n° 6387/DF[8]. Cuida-se, mais especificamente, de ação ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) contra o inteiro teor da Medida Provisória nº 954, de 17 de abril de 2020, que dispunha sobre "o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística". O compartilhamento tinha por finalidade suportar a produção estatística oficial durante a situação crítica de saúde

[8] As ações diretas de inconstitucionalidade nº 6388, 6389, 6390 e 6393, por igualmente impugnarem a validade constitucional da Medida Provisória nº 954/2020, tramitaram em conjunto com o feito em comento.

pública de importância internacional decorrente do coronavírus, de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.

O requerente materialmente alegou, em síntese, que a Medida Provisória supramencionada violou dados sigilosos, inclusive o telefônico, dos brasileiros; detinha finalidade genérica e imprecisa, qual seja, a produção de estatística oficial mediante a realização de entrevistas não presenciais no âmbito de pesquisas domiciliares; não definiu procedimentos de controle pelo Judiciário, pelo Ministério Público ou por órgãos da sociedade civil para a guarda dos dados disponibilizados no âmbito da Fundação IBGE; não apresentou precisamente a modalidade, a frequência e o objetivo das pesquisas a serem realizadas, nem as razões que justifiquem a necessidade do compartilhamento dos dados para a pesquisa estatística; dentre outros argumentos.

Nesse caminho, o Conselho Federal da Ordem dos Advogados do Brasil/CFOAB argumentou que a Medida Provisória questionada impõe restrições à proteção de direitos fundamentais, haja vista que não atende ao critério da proporcionalidade, notadamente no que tange às dimensões da adequação, da necessidade e da proporcionalidade em sentido estrito. O IBGE, doutro lado, sustentou que o compartilhamento de dados estabelecido na Medida Provisória não se confundia com o rastreamento de clientes, de modo que não haveria acesso ao conteúdo das comunicações telefônicas. Sumariamente, os pontos de vista em combate eram, portanto:

Síntese argumentos CFOAB	**Síntese argumentos IBGE**
A violação irrestrita ao direito à privacidade em nome do combate à pandemia do coronavírus, agravada pelos objetivos abstratos contidos na MP.	A necessidade de continuidade do recolhimento de dados para a produção de pesquisas oficiais durante a pandemia, em conformidade à confidencialidade estatística.

Quanto ao caso, importa ressaltar que somente um dispositivo da MP nº 954/2020 dispôs sobre a finalidade e o modo de utilização dos dados. Nesse sentido, o §1º do art. 2º limitava-se a enunciar que:

> §1º Os dados de que trata o caput serão utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.

É de se ver, como bem observou a Ministra Rosa Weber,[9] que a norma não delimitou: (i) o objeto da estatística a ser produzida; (ii) sua finalidade específica; (iii) sua amplitude; (iv) a necessidade de disponibilização dos dados; (v) como os dados serão efetivamente utilizados. Outrossim, é imperativo consignar que, mesmo em cenários de crise, o compartilhamento de dados deve estar em conformidade aos mandamentos constitucionais e legais, notadamente no que tange à estrita relação entre adequação e necessidade.

Não por outro motivo, em decisão monocrática que deferiu a medida liminar pleiteada, a Ministra apontou, dentre outros aspectos, que:

> *Consideradas **a necessidade**, a adequação e a proporcionalidade da medida, **não emerge da Medida Provisória nº 954/2020**, nos moldes em que editada, **interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia.***
>
> *Ao não definir apropriadamente como e para que serão utilizados os dados coletados, **a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade**, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades.* (grifos nossos)

Como esclarecido em tópico anterior, o que se busca com a diretriz principiológica inaugurada pela LGPD é uma transição do paradigma do máximo possível de dados para o mínimo necessário de dados. À vista disso, o que há de ser definido no caso concreto, visando à resolução da controvérsia, é: (i) a quantidade e a variedade de dados pessoais efetivamente necessárias; (ii) a finalidade específica ou concreta, geralmente inserida dentro de uma finalidade geral; (iii) o ponto ótimo entre a minimização da coleta de dados pessoais e a efetividade do processo, aplicando-se as normativas cabíveis.

In casu, concluiu-se que a MP 954/2020 não estabeleceu interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. Nesse caminho, ao deixar de definir apropriadamente a forma e a finalidade de coleta dos dados, o dispositivo não ofereceu condições para aferição de sua adequação e necessidade, bem como falha do ponto de vista da transparência necessária para uma adequada conciliação entre a demanda de produção estatística e os direitos fundamentais à proteção de dados e à autodeterminação informativa.

[9] Ministra relatora da ação direta em análise.

Em 07/05/2020, o Plenário da Corte, referendando a decisão de deferimento da medida cautelar da Ministra relatora, suspendeu a eficácia da questionada MP, com comando para que o IBGE deixasse de solicitar às empresas concessionárias a disponibilização dos dados. Sob o vértice constitucional, assentou o Informativo 976/STF:

> O art. 2º da MP 954/2020 impõe às empresas prestadoras do STFC e do SMP o compartilhamento, com o IBGE, da relação de nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas. Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). Sua manipulação e seu tratamento, desse modo, devem observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional.

Posteriormente, a ação direta foi julgada prejudicada, por perda superveniente do seu objeto, vez que a Medida Provisória nº 954/2020 não logrou ser convertida em lei no prazo constitucional previsto e teve sua vigência encerrada em 14/8/2020.

2.2. "TK" vs. Associação dos condóminos do edifício M5A ('*A Asociaţia de Proprietari bloc M5A-ScaraA'*

No âmbito europeu, relevante controvérsia foi analisada pelo Tribunal de Justiça da União Europeia (TJUE)[10] envolvendo a aplicação concreta do princípio da minimização. No caso, a Terceira Secção do referido Tribunal proferiu acórdão em controvérsia que envolvia a instalação de sistemas de videovigilância nas partes comuns de um edifício para habitação. Foi analisada questão prejudicial[11] em relação à interpretação do artigo 6°, n° 1, alínea 'c', e do artigo 7°, alínea 'f', da Diretiva 95/46/CE[12] do Parlamento Europeu e do Conselho, de 24 de

[10] O TJUE é o supremo tribunal da União Europeia (UE).
[11] Com objetivo de garantir uma aplicação efetiva e isonômica das normas e evitar interpretações divergentes, os juízes nacionais dos estados-membros da UE têm o poder-dever de, no contexto da União Europeia, consultarem o Tribunal de Justiça europeu a fim de que sejam esclarecidos pontos de interpretação do direito da União. Assim, visa-se a verificar a conformidade da respectiva legislação nacional com esse direito. Ademais, o pedido de decisão prejudicial pode ainda ter por finalidade a fiscalização da legalidade de um ato de direito da União Europeia.
[12] A Diretiva 95/46/EC foi substituída pelo RGPD, que se tornou aplicável em 25 de maio de 2018.

outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *In verbis*:

> **Artigo 6°. 1.** Os Estados-Membros devem estabelecer que os dados pessoais serão: (...) **c)** Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente;
> **Artigo 7°.** Os Estados-Membros estabelecerão que o tratamento de dados pessoais só poderá ser efetuado se: (...) ou **f)** O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do n° 1 do artigo 1°.

A legislação romena concernente ao tema, por sua vez, dispunha que qualquer tratamento de dados pessoais, exceto se referente a dados pertencentes a determinadas categorias[13], só pode ser efetuado se a pessoa em causa tiver dado expressa e inequivocamente o seu consentimento para esse tratamento. No bojo do processo originário, a decisão da Autoridade Nacional de Supervisão do Tratamento de Dados Pessoais romena (ANSPDCP)[14], relativa ao tratamento de dados pessoais obtidos por videovigilância, na versão aplicável ao processo principal, previa, nos seus artigos 1°; 4°; 5°, n°´s 1 a 3; e 6° que:

> **Art. 1°.** A recolha, gravação, armazenamento, utilização, transmissão, divulgação ou qualquer outra operação de tratamento de imagens por videovigilância, que permita,

[13] Lei n° 677/2001, Art. 5°. 2. "O consentimento do titular dos dados não é exigido nos seguintes casos:
a) quando o tratamento for necessário para a execução de um contrato ou em negociações pré-contratuais em que seja parte o titular dos dados ou para a adoção de medidas, a seu pedido, antes da celebração de um contrato ou durante as negociações pré-contratuais;
b) quando o tratamento for necessário para a proteção da vida, da integridade física ou da saúde do titular dos dados ou de outra pessoa exposta a ameaça;
c) quando o tratamento for necessário para o cumprimento de uma obrigação legal do responsável pelo tratamento;
d) quando o tratamento for necessário para a execução de atribuições de interesse público ou destinadas ao exercício de prerrogativas de poder público de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;
e) quando o tratamento for necessário para a realização de um interesse legítimo do responsável pelo tratamento ou do terceiro a quem os dados são comunicados, desde que esse interesse não afete os interesses ou os direitos e liberdades fundamentais do titular dos dados;
f) quando o tratamento disser respeito a dados provenientes de documentos acessíveis ao público, nos termos da lei;
g) quando o tratamento for efetuado exclusivamente para fins estatísticos, de investigação histórica ou científica, e os dados permanecerem anónimos durante todo o tratamento."
[14] Órgão responsável por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento da legislação de tratamento de dados na Romênia.

> direta ou indiretamente, identificar pessoas singulares, constituem operações de tratamento de dados pessoais abrangidas pelo âmbito de aplicação da [Lei n° 677/2001].
>
> **Art 4°.** A videovigilância pode ser realizada principalmente para os seguintes fins: **a)** prevenção e combate à criminalidade; **b)** monitorização do tráfego rodoviário e das infrações ao direito estradal; **c)** segurança e proteção de pessoas, bens e valores, edifícios e instalações de utilidade pública e respectivos recintos; **d)** execução de medidas de interesse público ou exercício de prerrogativas de poder público; **e)** realização de interesses legítimos, desde que não sejam violados os direitos e liberdades fundamentais das pessoas em causa.
>
> **Art 5°. 1.**A videovigilância pode ser efetuada em locais e espaços abertos ou destinados ao público, incluindo vias públicas de acesso situadas no domínio público ou privado, nas condições previstas na lei. **2.** As câmaras de videovigilância são instaladas de forma visível. **3**.É proibida a utilização de câmaras de videovigilância dissimuladas, exceto nos casos previstos na lei.
>
> **Art 6°.** O tratamento de dados pessoais através de sistemas de videovigilância é efetuado com o consentimento expresso e inequívoco da pessoa em causa ou nos casos previstos no artigo 5°, n° 2, da Lei n° 677/2001 […]

Como antecipado, o pedido prejudicial foi exprimido no âmbito de litígio oposto por um indivíduo – "TK" – em face de uma associação de condôminos, no qual o morador formula requerimento no sentido de que a associação desative o sistema de videovigilância do edifício, além de que remova as câmeras instaladas nas partes comuns dele (fachada, elevador e corredor do piso térreo), por constituir violação do direito à reserva da vida privada. Alegou, ainda, que a associação "tinha assumido a função de responsável pelo tratamento dos dados pessoais sem ter seguido o procedimento de registro previsto na lei para o efeito".

A associação, em resposta, mencionou que a decisão de instalação de câmeras no prédio foi aprovada em assembleia geral dos condôminos e tinha sido tomada para controlar as movimentações no edifício da forma mais eficaz possível, em razão do fato de o elevador ter sido várias vezes vandalizado, além de apartamentos e partes comuns terem sido objeto de assaltos e furtos.

O Tribunal de Primeira Instância de Bucareste ressaltou a previsão de que o tratamento de dados pessoais necessário para proteger a vida, a integridade física ou a saúde do titular dos dados ou de outra pessoa exposta a ameaça excepciona a necessidade de consentimento

expresso (artigo 5°, n° 2 da Lei romena n° 677/2001). Em adição, sustentou que o sistema de videovigilância *in casu* "não parece ter sido utilizado de forma ou com uma finalidade que não correspondesse ao objetivo declarado pela associação dos condôminos do edifício", havendo proporcionalidade entre o propósito prosseguido pela ingerência nos direitos e liberdades dos cidadãos e os meios utilizados. Nessas circunstâncias, o órgão jurisdicional local suspendeu o julgamento da lide e submeteu ao Tribunal de Justiça a questão prejudicial.

Nesse contexto, recorreu-se ao TJUE para o fornecimento de orientações sobre como avaliar se um determinado tratamento (no caso, um sistema de videovigilância) poderia ser considerado 'necessário' para efeitos dos interesses legítimos prosseguidos pelo responsável pelo tratamento.

O TJUE considerou a necessidade de uma operação de tratamento ser examinada em conjunto com o princípio da minimização de dados, o qual restringe as opções do responsável pelo tratamento àquelas adequadas, relevantes e não excessivas em relação às finalidades para as quais são recolhidos.

Ademais, salientou ser necessária uma ponderação[15] dos direitos e interesses opostos no caso concreto – sendo vedada a mera exclusão da possibilidade de tratamento de determinadas categorias de dados pessoais – para apreciar qual deveria prevalecer: o direito à proteção de dados ou o interesse legítimo prosseguido pelo responsável pelo tratamento.

Sustentou, ainda, não ser exigido o consentimento da pessoa em causa enquanto requisito para o tratamento de dados pessoais na hipótese do artigo 7°, alínea "f" da Diretiva 95/46/CE. Com efeito, ressaltou ser um dos requisitos a legitimidade do interesse visado pelo responsável pelo tratamento – *in casu* a proteção de bens, da saúde e da vida dos condôminos. Frisou o TJUE que tal condição impõe ao órgão jurisdicional nacional que verifique se o interesse legítimo no caso não pode ser razoavelmente alcançado de modo igualmente eficaz por meio de outras formas menos atentatórias aos direitos à reserva da vida privada e à proteção

[15] Nessa ponderação, deve-se considerar diversos elementos, tais como: (i) o caráter variável, a depender da acessibilidade da fonte ao público, da gravidade da violação dos direitos fundamentais da pessoa em causa pelo referido tratamento; (ii) a natureza dos dados pessoais em questão, destacando-se aqueles potencialmente sensíveis, assim como outras características do tratamento, sobretudo o número de pessoas que têm acesso a esses dados e as formas de acesso a eles; (iii) as expectativas razoáveis dos indivíduos de que os seus dados pessoais não serão tratados posteriormente; (iv) a importância, para todos os condôminos do edifício em causa, do interesse legítimo prosseguido no caso vertente pelo sistema de videovigilância, na medida em que visa essencialmente a garantir a proteção de bens, da saúde e da vida.

dos dados pessoais (relacionando-se à vertente da menor intrusividade do princípio da necessidade)**.**

Decidiu, também, que o requisito relativo à proporcionalidade do tratamento dos dados no processo parece ter sido contemplado, eis que (i) foi adotada medida alternativa previamente – sistema de segurança, instalado na entrada do edifício, composto por um intercomunicador e um cartão magnético –, que se revelou insuficiente; e (ii) o sistema de videovigilância está limitado às partes comuns do condomínio e às suas vias de acesso.

Em conclusão, o Tribunal europeu esclareceu que a proporcionalidade deve ser examinada, também, tendo em vista o modo concreto de instalação e funcionamento do dispositivo, que devem limitar o seu impacto sobre os direitos individuais e garantir concomitantemente a eficácia do sistema de videovigilância. Portanto, o controlador deve aferir, entre outros aspectos, "se é suficiente que a videovigilância funcione apenas à noite ou fora do horário normal de trabalho, além de bloquear as imagens captadas em áreas onde a vigilância é desnecessária".

O dispositivo da questão prejudicial, por último, destacou que, desde que o tratamento dos dados pessoais cumpra os requisitos previstos no artigo 7°, alínea "f", não haveria vedação jurídico-legal à instalação do sistema de videovigilância.

3. Considerações finais

Do exposto, resta perceptível que o princípio da necessidade – denominado, na legislação europeia, de princípio da minimização – possui vital importância na compreensão e na aplicação da LGPD e do RGPD. Com efeito, para além de conferir maior efetividade à coleta e ao tratamento de dados, tal princípio evita exposições desnecessárias dos tutelados pelos diplomas supramencionados, na medida em que baliza a realização do tratamento ao que se mostrar imprescindível à consecução da finalidade previamente delimitada.

Como visto, existem diferentes dimensões que resultam da obrigação de minimização dos dados, eis que essa deve ser aplicada à quantidade de dados recolhidos, à extensão do processamento, ao período de armazenamento e à própria acessibilidade aos dados. Nesse caminho, releva destacar que o entendimento e a aplicação do princípio em análise se conectam a outros princípios, notadamente o da eficiência, da proporcionalidade, da finalidade e da adequação, como vêm decidindo os tribunais.

Por último, insta repisar o imperioso objetivo do princípio em comento, qual seja promover a difícil transição da lógica do máximo possível de dados para o mínimo necessário de dados, com menores intrusividade e lesividade aos indivíduos, e de modo a barrar, ainda, o uso incondicional de dados.

Referências bibliográficas

ÁVILA, HUMBERTO. Teoria dos princípios: da definição à aplicação dos princípios jurídicos. 19. ed. rev e atual. - São Paulo: Malheiros, 2019.

BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. O Legítimo Interesse na LGPD: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa. 2021 BRASIL. Constituição da República Federativa do Brasil de 1988.

BRASIL. *Lei nº 13.709, de 14 ago. 2018, Lei Geral de Proteção de Dados Pessoais (LGPD)*, Brasília, DF. BRASIL, Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n° 6387. Relatora: Min. Rosa Weber, julgado em 7/5/2020, DJe 12/11/2020. 2020.

DATA PROTECTION NETWORK. Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation. Reino Unido, 2017. Disponível em: https://www.dpnetwork.org.uk/wp-content/uploads/2018/11/DPN-Guidance-A4-Publication-17111.pdf. Acesso: 22 mar. 2022.

DOHMANN, Indra. A Proteção de Dados Pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. RDP, Brasília, Volume 17, n. 93, 9-32, maio/jun. 2020.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. -- São Paulo: Thomson Reuters Brasil. 2020.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo, *et al.* Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

FALK, Matheus. Os "princípios jurídicos" da LGPD e do RGPD: uma leitura a partir da Teoria dos Princípios de Humberto Ávila. In: WACHOWICZ, Marcos. Proteção de dados pessoais em perspectiva: LGPD e RGPD na ótica do direito comparado. Curitiba: Gedai, UFPR 2020.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. Disponível em: Minha Biblioteca UnB.

PINHEIRO, Patrícia Peck. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018. São Paulo: Saraiva Educação, 2018.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão de 11.12.2019, processo C-708/18. 2019. Disponível em: <https://curia.europa.eu/juris/document/document.jsf;jsessionid=4A9F71BCDFB6F507CC5D0302FA1AE329?text=&docid=221465&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=35786932>. Acesso: 6 abr. 2021.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamentos Europeu e do Conselho*, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz

respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE . 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso: 5 abr. 2022

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 1965. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso: 5 abr. 2021.

UNIÃO EUROPEIA. Carta dos direitos fundamentais da União Europeia (2016/C 202/02). 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR. Acesso: 5 abr. 2021.

WIMMER, Miriam. *O regime jurídico do tratamento de dados pessoais pelo Poder Público.* In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021,p.271-288. Disponível em: Minha Biblioteca UnB.

ANONIMIZAÇÃO DE DADOS PESSOAIS: UM ESTUDO À LUZ DA LGPD E DO RGPD

Ana Júlia Prezotti Duarte[1]

Dispositivos da LGPD	Dispositivos do RGPD
Art. 5º Para os fins desta Lei, considera-se: **III** - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; **XI** - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; **Art. 12**. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. **§ 1º** A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. **§ 2º** Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. **§ 3º** A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.	**Considerando 26.** Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação.

[1] Graduanda em Direito na Universidade de Brasília. Integrante do Observatório da LGPD (UnB) e do Grupo de Estudos Constituição, Empresa e Mercado (GECEM/UnB).

Introdução

Este artigo parte de uma investigação bibliográfica acerca do processo de anonimização, em que se busca evidenciar suas implicações quanto à proteção de dados, bem como seus aspectos legais e teóricos. Nesse sentido, por meio de uma análise comparativa entre o artigo 12, da Lei Geral de Proteção de Dados (LGPD), e o Considerando 26, do Regulamento Geral sobre a Proteção de Dados europeu (RGPD), procurar-se-á promover um diálogo entre os dois marcos normativos, destacando os pontos em que convergem ou se distanciam.

Perpassando pelo conceito de dado anonimizado, com o critério da razoabilidade insculpido em lei, tem-se o objetivo de delinear os problemas quanto aos métodos de anonimização, além de investigar tal instituto como processo. Adiante, passa-se a analisar a zona cinzenta entre os conceitos de dados pessoais e dados anonimizados – destacando as soluções encontradas pelo legislador no que se refere ao risco permanente de re-identificação do titular.

Posteriormente, com o fito de gerar maior concretude para o presente estudo e de explorar a visão europeia x visão brasileira acerca do tema em comento, serão analisadas duas decisões jurisprudenciais sobre a problemática, o caso *Breyer*, julgado sob a égide do RGPD, que tratou da definição do dado pessoal, e a Apelação Cível n° 1000631-31.2020.8.26.0452, sob aplicação da LGPD, acerca do tratamento de dados anonimizados no âmbito de um Sistema de Monitoramento Inteligente.

Ao final, verifica-se que a qualificação dos dados depende de uma análise contextual e dinâmica, de acordo com as inovações tecnológicas, não se restringindo à compreensão dicotômica e estática entre dados pessoais e dados anonimizados. Tal assertiva repercute diretamente na atividade de tratamento de dados, demandando do controlador a realização de um teste que leve em consideração todos os meios suscetíveis de serem razoavelmente utilizados. Somente assim, torna-se possível assegurar a conformidade com o regulamento e, ao mesmo tempo, o usufruto das informações, sem que se resulte na violação dos direitos individuais dos titulares.

1. Comentários

1.1. O enigma do dado: a anonimização entre a LGPD e o RGPD

Em ambos os estatutos, o que se extrai dos dispositivos em relevo é que os dados anonimizados, em virtude de não se referirem a uma pessoa natural identificada ou identificável, desde a origem ou após tratamento, não serão considerados dados pessoais – estando fora do seu escopo de aplicação – salvo se for possível descobrir a respectiva autoria (FINKELSTEIN; FINKELSTEIN, 2020). Simplificadamente, se assim caracterizados, os dados podem ser utilizados livremente, não estando sujeitos às restrições impostas pela proteção de dados (BONATTI; KIRRANE, 2019; MACHADO; DONEDA, 2018). Entretanto, essa definição não é trivial; mesmo que identificadores diretos sejam removidos de um banco de dados, ainda será factível reidentificar indivíduos singulares combinando este agregado com outras informações (GRUSCHKA et al., 2018).

A anonimização se trata de um caso "forte" de de-identificação, por meio do qual se busca tornar impraticável, ou até impossível (empregando todos os meios considerados razoáveis) a re-identificação (inclusive pelo próprio controlador) (PINHO, 2017). Salienta-se que a problemática relativa à anonimização envolve os denominados quasi-identificadores, variáveis que podem não identificar sujeitos diretamente, mas que, ocasionalmente, estabelecem uma correlação substancial com elementos identificadores únicos e que podem ser usados para re-identificação indireta (JÚNIOR; MARTINS, 2021).

Os métodos comuns de anonimização existentes são: a supressão, em que os valores de um atributo são completamente removidos ou substituídos por um valor fictício, como um *, sendo aplicável, geralmente, aos identificadores explícitos; a generalização, consistente na modificação da escala ou ordem de magnitude, no caso dos quasi-identificadores, como a data de nascimento (substituindo o formato mês/dia/ano por apenas ano); a permutação, que procura dividir os dados em grupos e embaralhar os valores sensíveis; e, por fim, a perturbação, que diz respeito à substituição de valores removendo o *link* ao dado original, mas de forma a manter suas propriedades estatísticas (BIONI, 2020; GRUSCHKA et al, 2018).

A definição de dado anonimizado prevista no Considerando 26, do RGPD, bem como no artigo 5°, III, e refletida no art. 12, da LGPD, aponta para a existência de três critérios para que o dado seja considerado anônimo: (1) a impossibilidade de se inferir o valor de um atributo de um indivíduo; (2) a inexistência de uma forma conhecida e sistemática de (re)indeitificar os

dados (conhecida como *single-out*); e (3) a incapacidade de conectar dois ou mais registros de uma mesma pessoa (PINHO, 2017; FINCK; PALLAS, 2020; COUVOKIAN; CASTRO, 2014).

Da leitura do artigo 5º, I, da LGPD, evidencia-se que o regulamento brasileiro, assim como o europeu, adotou a estratégia expansionista, consolidando-se como uma legislação de escopo alargado. Nada obstante, diversamente do RGPD, a LGPD não estabeleceu um rol exemplificativo do que pode ser definido como dado pessoal (BIONI; MONTEIRO, 2021).

De um lado, a abordagem reducionista retrai a possibilidade de classificação de um dado como pessoal. Sob esse prisma, somente informações diretamente atreladas a uma pessoa natural *identificada* serão consideradas dados pessoais, a exemplo do RG, do CPF e da biometria. Por outro, conforme se verifica dos contornos da LGPD e do RGPD, com a abordagem expansionista, o vínculo do titular do dado com a informação pode ser mediato, indireto ou inexato e, portanto, se referir a uma pessoa *identificável*, tal como ocorre com profissão, interesses pessoais, endereço de IP e de e-mail corporativo (BIONI; MONTEIRO, 2021).

Outrossim, diferentemente do RGPD, a LGPD dispõe que o dado pode ser considerado pessoal quando empregado para formular perfis comportamentais ("*profiling*") de uma pessoa natural específica e esse tratamento possa culminar na identificação do titular dos dados (KATEIFIDES; MACHADO, 2019; MORIBE et al., 2019). Esse dispositivo da LGDP demonstra um amadurecimento da legislação brasileira no que tange ao regulamento europeu, levando-se em conta o cuidado em regular expressamente as situações oriundas do processamento do *big data* por algoritmos, o que ocorre, comumente, no direcionamento de anúncios publicitários, em matéria de crédito e justiça criminal.

No que concerne ao dado anonimizado, a fim de determinar se esforços razoáveis foram realmente empreendidos, novamente os estatutos se aproximam, como se verá adiante.

Cabe destacar mais uma semelhança entre a legislação brasileira e o regulamento da União Europeia, uma vez que há, no inciso II, do artigo 16 da LGPD, previsão de conservação dos dados, para fins de estudo por órgão de pesquisa, utilizando-se da anonimização, embora esta não seja especificamente recomendada pelo RGPD. Também detém o titular a prerrogativa de requerer a *anonimização*, bloqueio, ou eliminação de dados que sejam desnecessários à finalidade do processamento, ou que estejam sendo submetidos a tratamento em desarmonia com a lei (GRADIM, 2020).

Outra situação possível ocorre quando o *link* entre identificadores explícitos – como o endereço eletrônico ou o número de CPF – e informações sensíveis, a exemplo da orientação sexual e situação financeira de um indivíduo, é o objetivo da análise. Nesta hipótese, a anonimização não é factível e o regulamento deve ser observado. Assim, diante da inviabilidade em tornar o dado anônimo e, simultaneamente, manter a utilidade da informação para fins científicos, estatísticos ou históricos, a pseudoanonimização afigura-se como a técnica mais adequada (GRUSCHKA et al, 2018).

A LGPD brasileira, diversamente do RGPD, não sistematizou adequadamente a figura da pseudoanonimização, muito menos estipulou normativamente incentivos expressos para a sua adoção por parte dos agentes de tratamento de dados. Ao passo que o regulamento europeu estabeleceu até mesmo o afrouxamento de algumas obrigações legais, a LGPD apenas mencionou a pseudoanonimização sem desenvolver propriamente o seu instituto (BIONI, 2020).

De acordo com a definição do artigo 4(9) do RGPD, a pseudonimização consiste no processamento de dados pessoais de modo que não possam mais ser atribuídos a um sujeito específico sem o uso de informação adicional. Nessa perspectiva, é importante consignar que os dados pseudoanonimizados continuam sendo dados pessoais, diferindo-se da anonimização justamente por se referirem a uma pessoa natural identificável. Percebe-se, então, que o Considerando 26 e o seu requerimento de meios razoáveis suscetíveis de serem utilizados permanecem relevantes para a realização desse escrutínio (MOURBY et. al., 2018).

Os autores sugerem que as seguintes perguntas devem ser feitas: a) as pessoas naturais são identificáveis com base na disposição do Considerando 26, tendo em vista todos os meios razoáveis possíveis de serem utilizados? b) se a resposta para a questão acima for afirmativa, a pseudoanonimização foi aplicada com base na disposição do artigo 4(5) do RGPD?

A pseudoanonimização se refere a um processo que reduz o risco de identificação direta, mas que não produz dados anônimos. Dessa forma, dados pseudoanonimizados recaem sob a tutela do regulamento de proteção de dados pessoais. Mas se for preciso reverter este processo, isso pode ser feito pelo controlador, que detém os pseudônimos de mapeamento para os parâmetros identificáveis (GRUSCHKA et al., 2018); como se fosse uma chave capaz de tornar o dado, novamente, pessoalizado.

No entanto, ainda assim é possível chegar à conclusão de que há sim incentivos, mesmo que tácitos, a serem extraídos da LGPD. Na medida em que a pseudoanonimização é o "meio do caminho", a zona de transição entre um dado pessoal e um dado anonimizado, seria possível relacioná-la às diversas referências que a LGPD faz para que os agentes de tratamento "sempre que possível" anonimizem os dados.

Isto pois, a lógica normativa é enxergar o processo de retirada dos identificadores de uma base de dados como uma importante medida de segurança alinhada com o princípio do *privacy by design* proposto na nova legislação. E esse é exatamente o cerne das técnicas de pseudoanonimização, mesmo que a combinação dos dados pseudonimizados com outros conjuntos de dados ainda permita a re-identificação total ou parcial dos indivíduos (BIONI, 2020).

1.2. A faceta escura entre o dado anonimizado e o dado pessoal

No contexto atual, a dificuldade está em avaliar se os métodos disponíveis de anonimização produzem, de fato, dados que são legalmente anônimos. Nessa ótica, é preciso se atentar à questão de que as garantias de tais técnicas e os requerimentos estabelecidos pelas duas leis possuem naturezas distintas. Isso porque, não há como verificar se o conceito legal de anonimização é obedecido em relação a alguns valores padronizados das variáveis *k, l, t e* ε, porquanto o nível de proteção assegurado pela escolha do parâmetro depende das fontes de dados adicionais a que o atacante tenha acesso e essa quantidade de informação é difícil de ser estimada. Por conseguinte, ainda que a discrepância entre as definições técnicas e legais fosse solucionada, o desafio de se mensurar a quantidade de informação disponível seria refletida na escolha imprecisa dos parâmetros aceitáveis (BONATTI; KIRRANE, 2019).

De acordo com Bruno Bioni (2020), o dado anônimo seria a antítese do dado pessoal, ao impedir a identificação da pessoa natural. Elucida-se que a definição de um dado como anônimo tendo por base uma análise contextual que se volta para a suposta irreversibilidade do processo de anonimização traz à tona o problema de seu viés elusivo ou de sua inviabilidade teórica.

Nesta senda, qualquer dado pessoal anonimizado possui o risco inerente de se tornar um dado pessoal, haja vista que sua identificabilidade é remota (identificável) e não imediata (identificada). Por esse motivo, as leis que adotam o conceito expansionista de dados pessoais (que tendem a se *expandir* à medida que a tecnologia o permita) e, concomitantemente, o

estabelecem em franca contraposição aos dados anônimos, teriam grande chance de incidirem em uma redundância normativa.

A fim de manter a coerência, a solução encontrada foi a criação de um filtro que fosse capaz de incorporar a elasticidade desse conceito expansionista, para que fosse possível uma delimitação mais clara da fronteira entre dados pessoais e dados anônimos, sob pena de esta ser sempre transponível (BIONI, 2020).

Dessa maneira, tanto o RGPD quanto a LGPD optaram pelo critério da razoabilidade para definir o espectro do conceito expansionista de dados pessoais. Em outras palavras, o perímetro de elasticidade do conceito de dado pessoal como aquele vinculado a uma pessoa identificável diz respeito ao esforço razoável desprendido no processo de identificação do titular do dado (BIONI, 2020). Esse filtro depende de uma "régua" que enseja a imputação da responsabilidade civil em hipótese de reversão (JUNIOR; MARTINS, 2021).

Consoante Junior e Martins (2021), o conceito de entropia dos dados consegue definir com precisão o espírito da "razoabilidade" insculpido em lei, na medida em que exige elementos mínimos para a confiabilidade da anonimização e para a aferição de seus riscos e falibilidades. Nesse descortino, a entropia atua de modo a indicar o que é preciso para, num corredor repleto de portas fechadas e trancadas com chaves diferentes, cada qual representando as inferências que podem ser feitas, impedir que alguém circule por mais de uma porta, fazendo o cruzamento de diversas informações.

Hodiernamente, verifica-se que não existe mais a pretensão de uma anonimização robusta, tendo se reconhecido amplamente que sempre haverá fatores de risco de identificação e re-identificação de pessoas com o tratamento de dados anonimizados, diante do volume maciço de informações disponibilizadas *online* e do desenvolvimento da capacidade de processamento e análise de algoritmos e de aprendizado de máquina (MACHADO; DONEDA, 2018).

Dessa maneira, torna-se muito mais prudente entender a anonimização e o conceito de dados anonimizados como um processo, mutável e por meio do qual se torna possível manter a utilidade de um banco de dados, e não como um artifício para escapar do regulamento de proteção de dados e de se esvaziar as obrigações que este impõe.

Observa-se que o aspecto mais importante quando se trata da anonimização é a velocidade com que potenciais tecnologias estão se desenvolvendo diuturnamente

(BOLOGNINI; BISTOLFI, 2017), criando um cenário de insegurança tanto para as empresas, que não conseguem assegurar com absoluta certeza a proteção do dado, quanto para os titulares, cujo exercício do direito à privacidade é prejudicado pela cláusula do *take it or leave it* ("pegar ou largar") – pelos altos custos sociais e monetários atrelados a tal liberdade de escolha.

Desse modo, os legisladores brasileiro e europeu tiveram que encontrar uma saída no tocante ao risco de estagnação do conceito legal, considerando-se o desenvolvimento científico e tecnológico. Ao invés de restringi-lo a uma tecnologia que poderia se tornar ultrapassada com o tempo, valeu-se da razoabilidade, conceito este que pode ser constantemente atualizado e ressignificado (BIONI, 2020).

Caberá, então, ao intérprete-aplicador aferir, à luz dos fatos concretos, se é provável que, da conjugação de outros elementos, a identidade do titular dos dados anonimizados possa ser revelada (CORDEIRO, 2018). Para tanto, estabeleceram-se dois eixos de análise.

O primeiro é o objetivo, composto pelos elementos fatoriais: estado da arte da tecnologia, custo e tempo. Cuida-se de uma avaliação dinâmica e circunstancial, que procura evidenciar qual é o grau de investimento financeiro e temporal que deve ser efetuado para se reverter o processo de anonimização. O RGPD também utiliza esses três fatores objetivos para a delimitação da razoabilidade (BIONI, 2020).

O segundo eixo de análise, que está presente apenas na legislação brasileira, é o subjetivo e se centra não nos padrões sociais acerca da reversibilidade de um dado pessoal, mas na capacidade individual de engenharia reversa do agente de tratamento de dados. Além disso, é relevante observar a capacidade subjetiva de terceiros que ingressam no fluxo informacional de uma organização, sobretudo, quando se está diante de atividades em que há enriquecimento de dados que envolvam agentes externos para ensejar uma atividade de tratamento de dados (BIONI, 2020).

No que se refere à criptografia, por exemplo, parcela da doutrina que sustenta ser esta um modo de anonimização parte da premissa de que o dado pessoal criptografado permanece com o mesmo *status* de possibilidade de identificação do titular para o agente que possui a chave criptográfica. Por conseguinte, elegeu-se o eixo de análise subjetivo, centrado na habilidade de engenharia reversa do controlador, e não nos esforços possíveis e razoáveis de qualquer pessoa em obter a informação.

Entretanto, constata-se que, se o sistema não oferecer segurança aos dados cifrados, seja por falha intencional ou eventual, os dados em questão podem ser considerados pessoais. Logo, afigura-se mais consentâneo com a realidade pensar esta espécie de dado como informação pessoal *prima facie*, pseudoanonimizado, sendo aplicável o estatuto de proteção de dados pessoais, mesmo que de forma modulada (MACHADO; DONEDA, 2018).

Enquanto o Considerando 26 do RGPD incorpora um teste baseado no respectivo risco de identificação, o Grupo de Trabalho do Artigo 29o desenvolveu um teste paralelo segundo o qual não pode haver nenhum risco remanescente de identificação para que um dado seja qualificado como anônimo.

Sobre este aspecto, há duas teorias distintas: (i) a teoria relativa, que limita a análise da razoabilidade aos meios e conhecimentos detidos pelo encarregado dos dados; e (ii) a teoria objetiva, inclinada a uma análise abstrata que considera os meios e os conhecimentos detidos não só pelo responsável, mas também por terceiros (CORDEIRO, 2018).

Cordeiro (2018) aponta os principais argumentos que indicam a fragilidade da teoria objetiva: no seu estado mais puro, todos os dados seriam considerados pessoais; a atribuição de importância aos meios e conhecimentos detidos por terceiros impediria que o encarregado dos dados tivesse ciência se está ou não a violar a legislação aplicável, visto que não tem controle sobre a sua anonimidade.

O Considerando 26 do RGPD sugere, inequivocamente, a relevância dos conhecimentos e meios detidos por terceiros. Todavia, não é claro a que terceiros ele alude: todos os sujeitos de direito ou somente uma categoria bem específica, a exemplo de quem trabalha com o responsável dos dados?

Em caso de dúvida, sob a perspectiva da interpretação da lei, a funcionalização exige que se assuma o sentido que mais resguarda os interesses dos titulares de dados pessoais. Da leitura do seguinte trecho fornecido pelo Considerado 26 (“Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, quer pelo responsável pelo tratamento quer por outra pessoa”), deverão ser considerados os meios detidos por terceiros, mas apenas aqueles *suscetíveis de ser razoavelmente utilizados* (CORDEIRO, 2018).

Por último, faz-se relevante elucidar que podem existir dados os quais, embora totalmente anonimizados, podem, ainda assim, ser considerados dados pessoais. É o que

colaciona a abordagem consequencialista, segundo a qual pouco importa se um tratamento emprega uma informação isolada ou combinada que não se associe direta ou indiretamente a uma pessoa identificada ou identificável. O enfoque está muito mais no impacto que o tratamento pode ter no livre desenvolvimento da personalidade de um grupo ou indivíduo, em que se observa uma zona cinzenta, faceta escura entre os conceitos de dados pessoais e de dados anonimizados (BIONI; MONTEIRO, 2021).

Ganha espaço, então, uma escolha normativa de cunho consequencialista, que levará em conta não só a lógica excludente entre dados pessoais e dados anonimizados, mas também a relação de causa e efeito que uma simples atividade de tratamento de dados pode exercer na vida de seus titulares.

2. Estudos de Caso

2.1. O caso do Sistema de monitoramento de Inteligência: o tratamento de dados anonimizados

O presente caso trata-se do repasse de dados anonimizados ao governo estadual de São Paulo, mediante um acordo de cooperação técnica com empresas de telecomunicações, a fim de mapear os pontos de aglomeração social e, com isso, informar aos cidadãos acerca da incidência da COVID-19. Esta decisão é relevante para o estudo sobre o instituto da anonimização, uma vez que discute o conceito de dado anonimizado, bem como traz uma análise contextual do tratamento dos dados de geolocalização, para, assim, aferir se houve violação do direito à privacidade da Autora. Observe a ementa:

> APELAÇÃO – AÇÃO CONDENATÓRIA – SERVIÇOS DE TELEFONIA MÓVEL – INDEFERIMENTO DA INICIAL – REFORMA – EXISTÊNCIA DE INTERESSE DE AGIR E LEGITIMIDADE PASSIVA – CAUSA MADURA – POSSIBILIDADE DE ADENTRAR NO MÉRITO – REPASSE DE DADOS ANONIMIZADOS AO GOVERNO ESTADUAL – ACORDO DE COOPERAÇÃO TÉCNICA ENTRE EMPRESAS DE TELECOMUNICAÇÃO E GOVERNO ESTADUAL – SISTEMA DE MONITORAMENTO INTELIGENTE (SIMI-SP) – AUSÊNCIA DE VIOLAÇÃO AO DIREITO À PRIVACIDADE – RESPALDO LEGAL, JURISPRUDENCIAL E ADMINISTRATIVO – ENVIO DE MENSAGENS DO GOVERNO À AUTORA INFORMANDO SOBRE AUMENTO DE CASOS DE CORONAVÍRUS (COVID-19) – AUSÊNCIA DE PRÁTICA ABUSIVA – DEFINIÇÃO DE SERVIÇO PARA FINS CONSUMERISTAS – INEXISTÊNCIA DE DANO MORAL

> 1 – Legitimidade passiva da ré para responder por danos advindos de envio de mensagens SMS à autora sem sua autorização. Pertinência subjetiva. 2 – Interesse de agir que não está condicionado à existência de prévio pedido administrativo junto à ré para cancelar o envio de mensagens SMS (inafastabilidade da jurisdição). 3 – Possibilidade de, anulando a r. Sentença por indeferir a inicial incorretamente, julgar o mérito da ação, considerando a teoria da causa madura positivada no atual Código de Processo Civil (CPC, art. 1.013, § 3º, I). Precedentes. 4 – Constitui mero exercício regular do direito o envio de dados anonimizados (informações insuscetíveis de identificação pessoal), tais como dados de geolocalização, às autoridades governamentais, por meio de acordo de cooperação técnica e do Sistema de Monitoramento Inteligente (SIMI-SP). Respaldo legal (Decreto Estadual n. 64.963/20, art. 1º, § único, II; LGPD, art. 5º, III), jurisprudencial (Precedentes recentes do C. STJ e do Órgão Especial deste E. TJSP a respeito disso), e administrativo (Acordo de Cooperação, Pareceres técnicos da AGU e do Ministério da Ciência, e notícias de adoção da mesma medida pela Comunidade Europeia). 5 – Envio pelo Governo do Estado de São Paulo de mensagens SMS informando sobre o aumento de número de casos na região não se qualifica como serviço, à luz do conceito doutrinário e legal (CDC, art. 3º, § 2º), mas pode ser cessado, condenando-se a ré prestadora de serviços à obrigação de não fazer. 6 – Inexistência de violação ao direito à privacidade que evidencia a falta de responsabilidade civil e, portanto, o descabimento de indenização por danos morais. RECURSO PARCIALMENTE PROVIDO (TJSP; Apelação Cível 1000631-31.2020.8.26.0452; Relator (a): Maria Lúcia Pizzotti; Órgão Julgador: 30ª Câmara de Direito Privado; Foro de Piraju - 1ª Vara; Data do Julgamento: 21/09/2020; Data de Registro: 21/09/2020).

Conforme se depreende do acórdão, a parte autora construiu um cenário fantasioso de vigilância social, semelhante àqueles desenvolvidos nas famosas distopias de George Orwell e Aldous Huxley – 1984 e Admirável Mundo Novo, respectivamente. Alegou que a ré estaria repassando informações ao governo estadual, através do chip de seu celular, de modo a violar seu direito fundamental à privacidade, à intimidade e seu direito de ir e vir.

O estado de São Paulo, em meados de abril de 2020, anunciou uma parceria com as operadoras de telefonia com o intuito de executar um Sistema de Monitoramento de Inteligência, destinado à utilização de dados digitais para medir a adesão à quarentena em todo o Estado e também enviar mensagens de alerta para regiões com maior incidência da COVID-19.

Essa parceria deveria observar, em especial, o seguinte comando, previsto no decreto criador do SIMI-SP:

> Art. 1º - Fica instituído o Sistema de Informações e Monitoramento Inteligente – SIMI, consistente em ferramenta de consolidação de dados e informações coligidos por órgãos e entidades da Administração Pública estadual.
> Parágrafo único - O SIMI:
> 1. destina-se a apoiar a formulação e avaliação das ações do Estado de São Paulo para enfrentamento da pandemia da COVID-19;
> 2. **não conterá dados pessoais, assim considerados aqueles relacionados a pessoa natural, identificada ou identificável, limitando-se a dados anonimizados** (grifo nosso).

Nesse sentido, foi destacado na decisão que, desde o início, o governo estadual se preocupou com a captação de dados anonimizados, definidos estes, na LGPD, em seu art. 5º, III: *"*dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento*".* Além disso, fez-se menção à conceituação insculpida no Considerando n° 26, do RGPD, sob a alcunha de *anonymized data*, chamando atenção para a semelhança com a importada pelo ordenamento jurídico brasileiro.

O que se constata de mais relevante na decisão é a análise contextual do tratamento de dados em relevo e a conceituação dos dados anonimizados. Nessa ocasião, o julgador ressaltou a ideia que subjaz o conceito, qual seja, a impessoalidade dos dados enviados, uma vez que irrelevantes para os fins perseguidos pelo acordo, tendo apenas sido concedido ao Estado mecanismos de mapear os pontos de aglomeração social, informação esta imprescindível para o manejo da pandemia do COVID-19. Esclareceu que a remessa é de mera geolocalização impessoal, sem identificação do número de celular, bem como que os dados são agregados, viabilizando a elaboração de gráficos e mapas com os índices de isolamento que serão apresentados na plataforma *Big Data*.

Outro ponto importante diz respeito ao modo de acesso à Plataforma pelo Governo de São Paulo, realizado por meio de login e senha, de maneira que não há compartilhamento de dados pessoais, mas acesso somente a "mapas de calor" e "mapas de identificação de zonas". Vale ressaltar que as informações prestadas pelas operadoras de telefonia não são processadas em tempo real, mas um dia após a conexão, obstando o monitoramento e o reconhecimento da

base de dados da prestadora de telefonia da qual se originaram os dados – a evidenciar que não se instaurou um regime totalitário de violação à privacidade.

A Comunidade Europeia, assim que a crise sanitária eclodiu, veio a público se manifestar precisamente sobre a utilização de dados de geolocalização pelos seus Estados-membros, chegando à mesma conclusão que embasou o governo estadual: a viabilidade de utilização dos dados anonimizados.

No caso brasileiro, em síntese, o Tribunal consignou que nenhum dado pessoal e identificável da autora foi enviado pela ré ao governo estadual, sendo que o repasse de dados anônimos, impessoais e insuscetíveis de pessoalização e identificação não configura violação ao direito à privacidade.

Contudo, vale frisar que o julgador não se desfez da concepção dicotômica e estanque entre dados anonimizados e dados pessoais, pois se valeu da suposição de irreversibilidade do processo de anonimização, o que não encontra respaldo na realidade concreta. Há sempre um risco inerente de re-identificação do titular, diante das ferramentas tecnológicas existentes, bem como da presença de milhares de bancos de dados que guardam informações relevantes sobre os seus titulares. Ainda assim, é possível verificar que houve a observância do parâmetro da razoabilidade previsto no artigo 12, da LGPD, que exige a ponderação dos recursos, do custo e conhecimento necessários para realizar uma re-identificação, com base no contexto tecnológico do momento.

2.2. O caso Breyer: na busca de um parâmetro

No caso Breyer v. Bundesrepublik Deutschland[2], a corte julgou se um endereço IP nas mãos de um controlador deveria ser considerado dado pessoal, quando este não poderia ser usado para identificar um usuário por si só, mas somente quando combinado com dados adicionais coletados do provedor de internet. Neste caso, a corte reputou ser o dado pessoal, pois o controlador tinha meios legais de identificar o usuário, embora esses meios estivessem disponíveis apenas no evento improvável de um ataque cibernético. Ainda que o TJUE não tenha considerado que o dado era anonimizado, a corte sugeriu que as restrições legais ao acesso à chave para re-identificar os dados codificados podem tornar os dados anônimos, ao invés de pseudonimizados, sob certas circunstâncias (PELOQUIN, et al, 2020).

[2]TJUE 19-out.-2016, proc. C-582/14 (Breyer v Bundesrepublik Deutschland).

Conquanto o Parecer 5/2014 do Grupo de Trabalho do Artigo 29o faça referência a "*means likely reasonably to be used"* (meios suscetíveis de serem razoavelmente utilizados, em tradução livre), estabelece-se que todo processo de anonimização deve ser completamente irreversível, alertando contra novas tecnologias que poderiam tornar conjuntos de dados anteriormente presumidos anônimos em dados pessoais (GROOS; VEEN, 2020). Na contramão, no julgamento do caso Breyer, o TJUE adotou uma visão mais flexível, porquanto, mesmo sabendo que um endereço IP dinâmico pode permitir a reidentificação, em algum momento, esta informação não foi suficiente para determinar seu juízo.

Em primeiro lugar, foi observado que não são todos os meios que devem ser levados em conta, mas tão somente aqueles razoáveis e legítimos. Nesse viés, a Corte está mais inclinada a uma abordagem contextual relacionada ao risco, posto que analisa se, concretamente, é possível a reidentificação pelo controlador com o auxílio legítimo de uma terceira parte. De um lado, o Parecer 5/2014 se refere a técnicas abstratas de anonimização que, apenas se forem seguidas à risca, o dado pode ser reputado anonimizado. Por outro, o caso Breyer demanda um teste concreto para o dado em questão e, por conseguinte, para o resultado e o contexto no qual o dado está sendo processado. Desta feita, consoante a decisão, há dois testes distintos (GROOS; VEEN, 2020):

> 1. Quanto ao controlador que não é proibido por lei para realizar a identificação, o dado será anônimo caso este processo exija um esforço desproporcional em termos de tempo, custo e mão-de-obra, de modo que o risco de identificação parece ser, na verdade, insignificante.
> 2. No que se refere ao controlador que não se amolda ao primeiro teste, sendo o risco de identificação significativo, o dado permanecerá anônimo se este processo, seja pelo controlador ou pela ajuda de uma terceira parte, for proibido por lei.

Conforme Groos e Veen (2020), o primeiro teste é contundente sob o ponto de vista legal, mas precisa ser operacionalizado na prática, pois um atacante pode conseguir acesso ao dado, o que constitui uma prática ilegítima em quase todas as jurisdições.

Percebe-se que a decisão do TJUE está em consonância com o teste previsto no Considerando 26, do RGPD, bem como do art. 12, da LGPD, vez que incorpora, essencialmente, uma abordagem baseada no risco para qualificar a informação. Quando há um risco razoável de identificação, o dado deve ser tratado como pessoal, no que concerne a todos os efeitos do regime de proteção de dados. Diversamente, quando o risco for inexpressivo, o

dado pode ser considerado anonimizado, ainda que a identificação não possa ser excluída com absoluta certeza (FINCK; PALLAS, 2020).

De fato, o Parecer 5/2014 traz em seu bojo a ideia de que nenhum risco pode ser tolerado, adotando uma visão muito mais rígida do que aquela extraída do texto legal. Ou seja, ao passo que os dispositivos legais reconhecem que a anonimização nunca pode ser absoluta, haja vista que as tecnologias mudam com o tempo, a postura irrestrita do Grupo de trabalho indica que a anonimização deve ser permanente (FINCK; PALLAS, 2020).

O caso *Breyer* suscita, ainda, outra questão relevante. A ênfase do tribunal na legalidade (apenas em relação ao governo) de obrigar ISPs (provedores de serviço de internet) a revelar os dados necessários para redesenhar um conjunto de dados despersonalizado foi a chave para a sua conclusão. O que nos faz questionar, por um lado, se a ilegalidade de um ato que enseja a identificação justifica que ele seja sempre considerado como razoavelmente improvável. Por outro lado, a adoção de uma abordagem absoluta pode efetivamente descartar a existência de dados anônimos, pois, em última análise, sempre haverá partes capazes de combinar um conjunto de dados com informações adicionais que podem identificá-lo novamente (FINCK; PALLAS, 2020).

Entre as diversas críticas à posição da Corte no caso Breyer, Cordeiro (2018) destaca: a disponibilidade tecnológica, técnica e humana que as empresas possuem; os dados coletados por uma entidade europeia poderem ser repassados a entidades sediadas fora do espaço europeu; as discrepâncias legislativas entre os vários países – o que é lícito sob a ótica do Direito europeu pode ser considerado ilícito em outro ordenamento jurídico; ou a ocorrência recorrente de ataques cibernéticos. O que se defende, portanto, é que, à luz do critério último da razoabilidade, deve-se levar em conta as condutas ilícitas, desde que se possa razoavelmente se dispor delas.

Tal conclusão é reforçada por alguns elementos interpretativos: (i) elemento literal – o termo razoabilidade não exclui ilicitudes; (ii) elemento teleológico – o propósito da lei geral de proteção de dados é resguardar, preventivamente, a devassa dos dados pessoais de sujeitos específicos; e (iii) elemento sistemático – o regime de proteção de dados foi concebido precisamente porque se reconhece que os dados pessoais de cada indivíduo podem ser obtidos ilegalmente (CORDEIRO, 2018).

O autor, ainda, concretiza tal modelo interpretativo à luz de três situações concretas:

1. Qualquer pessoa tem os meios necessários para acessar a informação, em razão de esta ser pública; assim sendo, esses dados não são anônimos, mas pessoais, pois qualquer sujeito possui os meios necessários à sua disposição para desvendar a identidade dos titulares dos dados.

2. O responsável pelo tratamento de dados detém os meios necessários para acessar a informação – situação discutida no acórdão Breyer;

3. Um terceiro tem os meios necessários para acessar a informação.

Aos dois últimos casos é dada solução idêntica – os dados serão anonimizados sempre que o responsável (segunda situação) ou o terceiro (terceira situação) disponham dos meios necessários para identificar os titulares dos dados. Entretanto, nem todos os meios têm relevância jurídica, mas somente os que sejam expectáveis de serem empregados. Diferentemente da posição do TJUE, no acórdão *Breyer*, portanto, o critério legal seria o da razoabilidade e não da razoabilidade mais licitude (CORDEIRO, 2018).

Logo, coadunando com a posição do autor (2018), um meio-termo entre a teoria relativa e a objetiva parece ser a solução mais viável, o que ele denomina de concepção gradual da teoria objetiva, consoante a qual o responsável pelo tratamento dos dados ou as entidades de supervisão devem se ater aos meios detidos por todos os terceiros, porém, limitando a sua análise às informações que, razoavelmente, esses terceiros tenham a seu dispor.

Desta feita, o encarregado do tratamento de dados apenas poderá ser responsabilizado, à luz da boa-fé objetiva, caso esteja dentro do esperado que um terceiro tenha à sua disposição os meios necessários para identificar os titulares dos dados anonimizados e aquele não tenha tomado as precauções devidas pelo regulamento de proteção de dados.

Considerações Finais

Diante da análise comparativa realizada entre o tratamento dado pela LGPD e o RGPD quanto ao instituto da anonimização, percebe-se que, em contraste com a perspectiva legal binária, a realidade opera em um espectro muito mais complexo, tendo em vista o limite móvel que existe entre dados pessoais e dados anônimos, com uma tendência expansiva desses primeiros conforme o avançar da tecnologia.

Nessa linha, nota-se que a qualificação do dado depende do contexto, de forma que a pessoalidade não deve ser vista como propriedade do dado, mas do ambiente no qual este está

inserido. Em síntese, a mesma informação pode ser qualificada como pessoal ou anônima e, consequentemente, sujeitar-se ou não ao regime de proteção de dados.

Ademais, percebe-se que a utilização da razoabilidade como parâmetro extraído dos dispositivos da LGPD e do RGPD (art. 12 e Considerando 26) vai ser avaliada diferentemente se a entidade for uma pessoa com personalidade jurídica privada, uma agência do governo ou uma grande plataforma *online*. Por se tratar de um conceito aberto, torna-se necessário avaliar periodicamente a estratégia de anonimização, considerando o cenário em que o controlador deve assegurar a efetividade de tal processo.

Esse exame é feito de forma *ex ante*, definindo-se o contexto no qual quer se operar e a finalidade do uso do dado anonimizado, com o intuito de compreender quais são os riscos de re-identificação. Ao mesmo tempo, consoante a evolução tecnológica e científica, a técnica pode ser aprimorada *ex post* com meios alternativos de anonimização.

A situação ideal implicaria potencializar concomitantemente a privacidade e a utilidade dos dados, o que, entretanto, é impossível de se alcançar na prática: o desafio advém não apenas das limitações das técnicas existentes, bem como da interconexão entre milhares de bancos de dados contendo informações relevantes. Por isso, afigura-se tão essencial avaliar, concretamente, o fim perseguido com o processamento, para, assim, decidir qual é a técnica mais adequada; afinal, em certas situações, o objetivo do controlador será manter o caráter pessoal dos dados e, em outras, priorizar-se-á a proteção da identidade do sujeito.

Por fim, cumpre adotar uma concepção gradual da teoria objetiva, mais consentânea com a realidade concreta e sem incorrer em absolutismos. Distanciando-se do critério da razoabilidade mais licitude do caso *Breyer* e considerando a dinamicidade existente dentro da qualificação do dado como anonimizado ou pessoal, devem ser levados em conta todos aqueles meios suscetíveis de serem razoavelmente utilizados, para, então, pensar nas possíveis implicações do regime de proteção de dados e nas estratégias que podem ser utilizadas a fim de melhor balancear a privacidade dos titulares e a utilidade das informações.

Referências bibliográficas

BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 191-201, 2020.

BIONI, Bruno; MONTEIRO, Ricardo. Data Privacy Brasil. LGPD: O Essencial, 2021. Disponível em: <https://cursos.dataprivacy.com.br/cursos/

exibir/123/combo-ead-muito-alem-da-lgpd> Acesso em: 15 de janeiro de 2021.

BOLOGNINI, Luca; BISTOLFI, Camilla. Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. Computer Law & Security Review, v. 33, n. 2, p. 171-181, 2017.

BONATTI, Piero A.; KIRRANE, Sabrina. Big Data and Analytics in the age of GDPR. IEEE International Congress on Big Data, 2019.

CAVOUKIAN, Ann; CASTRO, Daniel. Big Data and innovation, setting the record straight: de-identification does work. The Information Technology & Innovation Foundation, Ontario, p. 1-18, jun. 2014.

CORDEIRO, A. Barreto Menezes. Dados pessoais: conceito, extensão e limites. Revista de Direito Civil, Coimbra, v. 3 n. 2, pp. 297-321, 2018.

FINCK, Michèle; PALLAS, Frank. They who must not be identified—distinguishing personal from non-personal data under the GDPR. International Data Privacy Law, 2020.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e lei geral de proteção de dados pessoais. Revista de Direito Brasileira, v. 23, n. 9, p. 284-301, 2020.

GRADIM, Luca Cisneiros. *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*. Mestrado em Direito/Relações Internacionais pela FAJS do UniCEUB, 2020.

GROOS, Daniel; VEEN, Evert- Ben van. Anonymized Data and the Rule of Law. European Data Protection Law Review, vol. 6, 2020, p. 498-508.

GRUSCHKA, *et al*. Privacy Issues and Data Protecion on Big Data: A Case Study Analysis under GDPR. IEEE International Congress on Big Data, 2018.

JÚNIOR, José Luiz de Moura Faleiros; MARTINS, Guilherme Magalhães. PROTEÇÃO DE DADOS E ANONIMIZAÇÃO: PERSPECTIVAS À LUZ DA LEI Nº 13.709/2018. REI-REVISTA ESTUDOS INSTITUCIONAIS, v. 7, n. 1, p. 376-397, 2021.

KATEIFIDES, Alexis *et al;* MONTEIRO, Renato *et al*. Comparing privacy laws: GDPR v. LGPD. *One Trust Data Guidance; Baptista Luz Advogados*, 2019.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. Rev. Trib, v. 998, p. 99-125, 2019.

MOURBY, Miranda *et al*. Are. pseudonymised data always personal data? Implifcations os the GDPR for administrative data research in UK. Computer Law & Security Review, 34, 2018, p. 222-233.

PELOQUIN, David et al. Disruptive and avoidable: GDPR challenges to secondary research uses of data. European Journal of Human Genetics, v. 28, n. 6, p. 697-705, 2020.

PINHO, Frederico. Anonimização de bases de dados empresariais de acordo com a nova Regulamentação Europeia de Proteção de Dados. Universidade do Porto, 2017.

ANÁLISE COMPARATIVA ENTRE O ESCOPO MATERIAL DA LGPD E DO RGPD

Eduarda Costa Almeida[1]

Dispositivos da LGPD	Dispositivos do RGPD
Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. **Art. 4º** Esta Lei não se aplica ao tratamento de dados pessoais: **I** - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; **II** - realizado para fins exclusivamente: **a)** jornalístico e artísticos; ou **b)** acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; **III** - realizado para fins exclusivos de: **a)** segurança pública; **b)** defesa nacional; **c)** segurança do Estado; ou **d)** atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional 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 o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. **§ 1º** O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. **§ 2º** É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa	**Artigo 2º.** Âmbito de aplicação material **1**. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados. **2.** O presente regulamento não se aplica ao tratamento de dados pessoais: **a)** Efetuado no exercício de atividades não sujeitas à aplicação do direito da União; **b)** Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE; **c)** Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; **d)** Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. **3**. O Regulamento (CE) n.º 45/2001 aplica-se ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n.º 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, são adaptados aos princípios e regras do presente regulamento nos termos previstos no artigo 98.º **4.** O presente regulamento não prejudica a aplicação da Diretiva 2000/31/CE, nomeadamente as normas em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus artigos 12.º a 15.º.

[1] Bacharel em Direito na Universidade de Brasília. Coordenadora de pesquisa do grupo de pesquisa Observatório da LGPD.

de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo. **§ 3º** A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. **§ 4º** Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.	

Introdução

Com o desenvolvimento tecnológico, as pessoas passaram a utilizar aparelhos tecnológicos, como *smartphones* e computadores, para acessarem conteúdos disponíveis do mundo *online*. Com isso, é notória a intensificação do fluxo de dados pessoais entre pessoas e entidades privadas ou públicas em uma sociedade da informação.[2] No entanto, esta nova lógica do mundo digital tem desafiado a proteção de alguns direitos e liberdades, principalmente quanto à privacidade e à autodeterminação informativa.

Como resposta a esse cenário, a disciplina jurídica dos dados pessoais e a proteção dos titulares desses dados durante o tratamento de informações pessoais ganharam força no debate político, tanto no plano nacional quanto internacional. Quanto à segunda seara e em vista da globalização e da disseminação de produtos e serviços pela internet, essa discussão passou a ser relevante internacionalmente para que fosse possível um adequado fluxo transfronteiriço de dados pessoais. Com isso, diferentes países ao redor do mundo optaram por elaborar legislações específicas sobre o tratamento de dados, como é o caso da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados ou LGPD), no Brasil, e o Regulamento 2016/679 (Regulamento Geral sobre Proteção de Dados ou RGPD), na União Europeia. (DLA Piper, 2021)

[2] O termo sociedade da informação "refere-se às transformações técnicas, organizacionais e administrativas que têm como "fator-chave" não mais os insumos baratos de energia – como na sociedade industrial – mas os insumos baratos de informação propiciados pelos avanços tecnológicos na microeletrônica e telecomunicações" (WERTHEIN, 2000, p. 71).

No Brasil, já existiam legislações esparsas que tratavam do tema de dados pessoais em contextos específicos, a exemplo das previsões no Código de Defesa do Consumidor e do Marco Civil da Internet. No entanto, essas legislações disciplinavam o fluxo de dados pessoais apenas de modo pontual no contexto consumerista e da internet, respectivamente, por isso os legisladores entenderam pela necessidade de uma lei que regulamentasse o tema de forma genérica aplicável a maior parte das relações jurídicas. Assim, a LGPD inaugura a regulação de proteção de dados pessoais no Brasil com um modelo próximo ao desenvolvido pela União Europeia (UE).

Uma das características do modelo de regulação brasileiro, assim como o europeu, é a centralidade do princípio da proibição, que determina a necessidade de uma justificativa para todo tratamento de dados pessoais. Esse princípio é traduzido por meio da especificação de bases legais autorizadoras do uso de dados previstas na LGPD e no RGPD. Assim, esse princípio "deve ser sempre entendido no sentido de que o tratamento lícito para determinadas finalidades e de determinada maneira não significa necessariamente que qualquer outro tratamento segundo a vontade do agente de tratamento dos dados fosse admissível" (DOHMANN, 2020, p. 20).

Diferente da LGPD, o RGPD não inaugura as formas de regulação da proteção de dados na União Europeia, mas revoga a Diretiva 95/46/EC que já versava sobre o tema. É relevante notar que o ato jurídico que regula a matéria na Europa foi modificado. Antes do RGPD, a proteção de dados pessoais era disciplinada por uma diretiva, ou seja, um ato legislativo da UE que deve ser incorporado, transposto, por meio de uma lei nacional editada por cada país membro (UNIÃO EUROPEIA-d, 2016). Como consequência, as diretivas não possuem efeito imediato, sendo necessária lei de transposição, e isso permite maior abertura para que os países regulem a matéria de maneiras diferentes entre si, já que devem observar apenas os parâmetros mínimos dispostos na diretiva.

Com a vigência do Regulamento 2016/679, a matéria de proteção de dados passa a ser regida de modo uniforme e diretoem todos os países da UE. Como regulamento, o RGPD é obrigatório e diretamente aplicável em todos os países da União, por isso ele é imediatamente aplicável pelos tribunais nacionais (EUR-LEX, 2015). A mudança da forma do ato jurídico é um indicativo da centralidade adquirida pelas discussões acerca da proteção de dados no contexto europeu. Essa alteração é resultado principalmente de duas comunicações ao

parlamento europeu,[3] além da desatualização da Diretiva 95/46 frente aos avanços nas técnicas de tratamento de dados pessoais e o aumento da capacidade computacional, bem como ante a necessidade de se enquadrar o impacto das novas tecnologias em um mundo globalizado.

Além disso, o art. 8º da Carta dos Direito Fundamentais da UE reconheceu a proteção de dados pessoais como um direito fundamental, e, para sua concretização, a Carta determinou que esse direito seria matéria de uma norma própria para que se pudesse garantir tratamento leal dos dados pessoais e para fins específicos (UNIÃO EUROPEIA-e, 2016). Assim, a UE elaborou o RGPD e passou a ter um diploma com objetivo de garantir maior certeza jurídica ao tratamento de dados pessoais, impondo novos deveres aos agentes que processam essas informações e garantindo novos direitos aos titulares de dados pessoais (CUNHA, 2020, p. 11).

O RGPD é aplicado a um escopo material específico, e a primeira delimitação do âmbito material de incidência do regulamento é a própria definição de dados pessoais, de forma que, quando a informação não for reconhecida como um dado pessoal, a norma não será aplicada às relações jurídicas advindas desse dado não pessoal. Da mesma maneira, o Regulamento estabelece situações específicas nas quais não se aplica. A estrutura da LGPD é similar, tendo em vista que, inicialmente, o conceito de dado pessoal foi delimitado, e, a partir daí, os casos excepcionais em que a lei não será aplicada foram explicitados.

Diante desse contexto, o presente artigo pretende analisar, de maneira comparada, os dispositivos sobre o escopo material da LGPD e do RGPD, de forma a compreender o campo de aplicação em comum das normas de proteção de dados pessoais no Brasil e na União Europeia, além dos cenários em que elas não são aplicadas em vista de divergências no conceito de dados pessoal ou de previsão expressa de não aplicação das normativas. Com isso, este artigo não busca estudar o escopo territorial de incidência das duas normas.[4]

Este estudo sobre o escopo material da lei e do regulamento foi realizado a partir de revisão bibliográfica das legislações, jurisprudências e doutrinas brasileira e europeia. Com a pesquisa, buscou-se delinear qual a diferença da aplicação material das duas normas específicas

[3] A primeira é "Uma abordagem global de proteção de dados pessoais na União Europeia", de 1 de novembro de 2010, está disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:033E:0101:0110:PT:PDF . A segunda é "Proteção da privacidade num mundo interligado. Um quadro europeu de proteção de dados para o século XXI", de 25 de janeiro de 2012, ela está disponível em: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2012)9

[4] Esta matéria está especificamente regulamentada nos artigos 3º e 4º, inciso IV, da LGPD e no Artigo 3.º do RGPD, bem como em outros dispositivos esparsos.

de proteção de dados e as consequências dessa diferença. Para tanto, este estudo está dividido em três partes, a primeira versou sobre aspectos introdutórios do tema de incidência e fundamentos das normas em exame. Já a segunda parte analisou aspectos do texto da lei e da doutrina sobre o assunto e a terceira destacou casos práticos de aplicação do âmbito material da LGPD e do RGPD. Dessa forma foi possível traçar um quadro comparativo entre as formas de aplicação das duas normas e algumas considerações sobre essas regulações, suas semelhanças e diferenças, além dos efeitos dessas divergências.

1. Comentários à legislação

Diante de uma sociedade da informação e do processamento de dados de modo ubíquo e constante, a proteção de informações pessoais busca garantir o devido processamento desses dados, já que são "projeções da personalidade e como tais devem ser considerados e tutelados" pelo ordenamento jurídico (MENEZES; COLAÇO, 2020, p. RB-6.4). Com isso, essa proteção recai sempre que há o tratamento de dados pessoais, esta expressão foi objeto do tópico a seguir. Em seguida, analisou-se as hipóteses previstas nos diplomas objeto deste artigo que excetuam essa regra.

1.1. Quando as normas de proteção de dados se aplicam?

As normas de proteção de dados pessoais ora em análise são aplicáveis quando há tratamento de dados pessoais, isto é, qualquer operação, automatizada ou não, que é efetuada sobre as informações pessoais, como a coleta, a classificação, a utilização, o acesso, a transmissão, entre outros. Nota-se que este conceito, descrito no art. 5º, X, da LGPD e no art. 4º, nº 2, do RGPD, abrange as diversas formas de utilização dados pessoais, seja durante simples coleta ou armazenamento, seja em casos de processamento automatizado de informações referente a pessoas. Com isso, o ato de tratar dados pessoais é vasto e pode ser configurado a partir de qualquer forma de manipulação de uma informação, seja por atores públicos ou privados.

Somado a isso, o objeto regulado por essas normas é o dado pessoal, que é definido pelo art. 6º, I, da LGPD, e pelo art. 4º, nº 1, do RGPD, como toda informação relativa a uma pessoa identificada ou identificável. Nota-se que dado pessoal é entendido a partir de um conceito amplo de dado, isto porque se o dado pessoal tivesse um significado fixo e estanque, ele,

facilmente, seria tornado obsoleto com o desenvolvimento tecnológico. Assim, é importante que o conceito de dados pessoais seja abrangente para englobar possíveis aplicações da tecnologia que permitam a identificação de uma pessoa para além dos elementos conhecidos e utilizados atualmente.

Em vista deste conceito alargado de dados pessoais, o RGPD evidencia de forma exemplificativa uma série de elementos identificadores que podem tornar uma pessoa identificada direta ou indiretamente, como é o caso de dados de localização, identificadores por via eletrônica e números de identificação. Nesse sentido, o Considerando 26 do RGPD acrescenta informações sobre o conceito de dado pessoal indireto, que pode ocorrer a partir da combinação de dados que podem torná-los informações pessoais. Já a LGPD apenas descreve o que é um dado pessoal de forma objetiva e não determina exemplos de dados pessoais.Essa diferença pode ser consequência da própria técnica legislativa adotada pelas duas jurisdições, mas possui impactos significativos.

Na LGPD, há uma maior abertura para questionamento se, em um caso concreto, aquela informação seria ou não um dado pessoal em situações limítrofes, como é o caso dos dados de localização de uma pessoa, ou mesmo seus dados mentais. Como o RGPD apresenta exemplos do que seriam dados pessoais, há maior segurança sobre os aspectos que são considerados para configuração de dados pessoais e, consequentemente, para aplicação do regulamento. Com isso, a jurisprudência brasileira terá de avançar a respeito da delimitação do significado de um dado pessoal, a partir da definição posta pela LGPD.

Diante da definição de dados pessoais, é importante destacar que a nacionalidade do titular de dados é irrelevante para aplicação das normas, de forma que as informações pessoais estão protegidas mesmo que sejam relativas a cidadãos estrangeiros. Ainda, as duas regulações não incidem sobre informações de pessoas jurídicas, salvo na medida em que os dados de pessoas não naturais permitam identificar uma pessoa singular.

Além disso, dados pseudonimizados são informações não atribuídas a uma pessoa "sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados não possam ser atribuídos a uma pessoa singular identificada ou identificável" (UNIÃO EUROPEIA-b, 2016). Por isso, essas informações estão no escopo da LGPD e do RGPD. Em acordo com o Considerando 28 do RGPD, a adoção de medidas de pseudonimização é adequada e incentivada pelo regulamento por poder permitir a redução dos riscos do tratamento indevido

para os titulares de dados, além de ser uma técnica de proteção dos dados desde a concepção, já que o ato de relacionar aquela informação a uma pessoa natural é dificultado.

Por outro lado, os dados anonimizados não estão no escopo dos diplomas de proteção de dados, já que eles não permitem a identificabilidade de uma pessoa, ou seja, são informações que não estão relacionadas a pessoa alguma (DOHMANN, 2020, p. 118). Esse aspecto não invalida o caráter amplo das normas de proteção de dados, de forma que, especificamente, "a LGPD, como norma geral, deve proporcionar respostas regulatórias isonômicas para todas as atividades e setores em que vier a ser aplicada" (DONEDA, 2020, p. 36).

1.2. Quando as normas de proteção aos dados pessoais não se aplicam?

Apesar do escopo material amplo das normas de proteção de dados, os diplomas brasileiro e europeu descrevem algumas hipóteses taxativas em que essas regulações não se aplicam. Dessa forma, este artigo apresenta um quadro comparativo entre as exceções de incidência dos diplomas expressamente previstas, a fim de se perceber as semelhanças e as diferenças entre a LGPD e o RGPD quanto ao estabelecimento de hipóteses em que a observância das normas de dados não é obrigatória.

1.2.1. Uso doméstico de dados

A primeira exceção em comum de aplicação da LGPD e do RGPD diz respeito aos casos em que há tratamento de dados pessoais realizado por pessoas naturais para finalidade exclusivamente particular e não econômica. Essa previsão é justificada em vista da falta de relevante assimetria de poder e de informações entre os atores envolvidos. As normativas buscam regular "o âmbito da sociedade de redes, na qual o poder informacional é dominado pelos agentes econômicos e/ou pelo próprio Estado" (MENEZES; COLAÇO, 2020, p. RB-6.4).

Essa exceção, prevista tanto no art. 4º, I, da LGPD, quanto no art. 2.º, nº 1, (c), do RGPD, é relevante para a viabilidade das relações interpessoais privadas, visto que as pessoas utilizam informações pessoais em suas comunicações rotineiras. Dessa forma, as normativas de proteção de dados não se aplicam no caso de armazenamento de números de telefone ou fotografias em um celular pessoal, envio de cartas com conteúdo pessoal, ou elaboração de lista de convidados para uma festa. Este dispositivo foi analisado pelo Tribunal de Justiça da União Europeia, como se verá na terceira seção deste artigo.

1.2.2. Uso jornalístico e artístico

O tratamento de dados pessoais para fins exclusivamente jornalísticos e artísticos também é uma exceção prevista no art. 4º, II, "a", da LGPD. Sob o fundamento da liberdade de expressão e de imprensa, a atividade jornalística deve ser imune ao regulamentado na LGPD, já que "uma interdição prévia do Estado na atuação jornalística importaria sua própria aniquilação" (MENEZES; COLAÇO, 2019, RB-6.5).

Nesse sentido, a legislação brasileira não se aplica à hipótese de processamento de informações pessoais para fins artísticos e jornalísticos. Porém outras atividades relacionadas, mas que não se confundem com o jornalismo, realizadas por uma empresa com função de jornal, como o *marketing*, por exemplo, estão sob o escopo material da LGPD, já que o uso de dados não é para fins jornalísticos ou artísticos.

Por sua vez, o art. 85º e o Considerando 153 do RGPD dispõem sobre a relação entre o tratamento de dados e a liberdade de expressão e de informação. O Regulamento indica a possibilidade de os Estado-Membros estabelecerem isenções e derrogações de algumas das previsões do RGPD, de forma a facilitar o tratamento de dados nesse âmbito. As derrogações versam sobre os princípios de proteção de dados, os direitos do titular, o responsável pelo tratamento e subcontratante, a transferência de dados para países terceiros, as autoridades de controle independentes, a cooperação e coerência, e as situações específicas de tratamento de dados explícitas no regulamento. Assim, as legislações editadas pelos países membros devem conciliar a liberdade de expressão e de informação e o direito à proteção de dados previstos no regulamento. Ainda, os Estados-Membros devem notificar a Comissão Europeia sobre as disposições existentes no direito interno de cada país (UNIÃO EUROPEIA, 2016).

1.2.3. Uso acadêmico e de pesquisa

O artigo 4º, II, "b", da LGPD, prevê que a lei não se aplica ao tratamento de dados pessoais realizado para finalidade acadêmica, mas as hipóteses previstas nos artigos 7º e 11 devem ser observadas. Em vista da lógica do princípio da proibição, esses dispositivos explicitam as bases legais autorizativas para o tratamento de dados na realização de estudos e pesquisas, incentivando o uso de técnicas de anonimização no uso de dados para pesquisa.

Segundo a LGPD, apenas os órgãos de pesquisa[5] podem se valer dessas bases legais, de forma a restringir as possibilidades de incidência desses fundamentos.

Nesse sentido, a regulação própria de tratamento de dados em pesquisas serve para "equilibrar os direitos individuais e a busca pelo interesse público a partir da aplicação de medidas técnicas e organizacionais suficientes e adequadas para garantir a proteção dos dados e o mínimo possível de processamento" (MENEZES; COLAÇO, 2019, RB-6.6). Além disso, para que a atividade de pesquisa seja lícita, ela deve observar outros parâmetros éticos e de direcionamento descritos na legislação brasileira (MENEZES; COLAÇO, 2019, p. RB-6.6). Um exemplo é a Lei 8.080, de 19 de setembro de 1990, que institui o Sistema Único de Saúde e apresenta diretrizes sobre os limites éticos nas pesquisas científicas para a área de saúde. Logo, a não incidência da lei de proteção de dados não significa a falta de outras formas de regulação das atividades de pesquisa.

Por outro lado, o RGPD apresenta salvaguardas mais específicas sobre o tratamento de dados para finalidades de pesquisa científica ou histórica, de estatística e de arquivamento de informações de interesse público. O art. 89º do RGPD determina que o regulamento é aplicável a estas hipóteses e ele incentiva a adoção de medidas técnicas e organizacionais para assegurar os princípios de proteção de dados, principalmente o da minimização dos dados. Ao mesmo tempo, a UE ou os Estados-Membros podem estabelecer legislações específicas sobre a possibilidade de derrogação dos direitos dos titulares previstos no regulamento quando a concretização desses prejudique a realização dos objetivos perseguidos nas pesquisas e estudos estatísticos (UNIÃO EUROPEIA, 2016).

O RGPD não contém uma definição formal do que constitui pesquisa científica, mas especifica algumas salvaguardas relevantes para essa hipótese de tratamento, como a minimização de dados, a adoção de práticas de *Privacy by Design* e *by Default*, além da pseudonimização (MONDSCHEIN; MONDA, 2018). Em acordo com o Considerando 159, aplica-se uma definição ampla à noção de pesquisa, afirmando que o processamento de dados pessoais para fins de pesquisa científica deve ser interpretado de uma maneira abrangente, incluindo, por exemplo, desenvolvimento tecnológico, pesquisa fundamental, pesquisa aplicada e pesquisa com financiamento privado.

[5] Segundo o art. 5º, XVIII, da LGPD, são órgãos de pesquisa aqueles "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico" (BRASIL, 2018).

1.2.4. Tratamento de dados pessoais para investigação penal e segurança pública

A LGPD e o RGPD não são aplicáveis ao processamento de dados para atividades de investigação penal e segurança pública, esta previsão é semelhante entre as normativas. Especificamente, o Considerando 19 do RGPD descreve que o regulamento europeu não se aplica ao processamento de informações pessoais "efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública" (UNIÃO EUROPEIA, 2016).

Por isso, percebe-se que o legislador brasileiro e o europeu destacam as atividades de polícia criminal para fora do escopo de proteção das normativas gerais já positivadas sobre proteção de dados. No entanto, as consequências da não aplicação dessas normas são diferentes nas duas regiões.

No Brasil, apesar da Lei Geral de Proteção de Dados não se aplicar diretamente aos casos de tratamento de dados pessoais para persecução penal e segurança pública, como previsto no art. 4º, III, "a" e "d" da lei, a LGPD determina que uma legislação específica será elaborada para dispor sobre o uso de dados nesse cenário. Ainda, esta lei futura deverá garantir os princípios de proteção de dados pessoais, os direitos dos titulares e o devido processo legal, além de prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, segundo o art. 4º, §1º, da LGPD.

Sendo assim, por mais que o uso de dados pessoais para fins de segurança e a "tecnologia avancem, é necessária regulação específica sobre o uso de inovações aplicadas ao contexto de segurança pública a fim de evitar o grande potencial de uso abusivo" (ALMEIDA, 2020, p.268).

Não obstante essa previsão legal, não há projetos de lei em tramitação sobre o devido tratamento de dados para segurança pública e persecução penal no Congresso Federal, nas formas previstas na LGPD. Entretanto, em novembro de 2019, a presidência da Câmara dos Deputados criou uma comissão de juristas especialistas com finalidade de elaboração de um anteprojeto de lei nos moldes da LGPD (JÚNIOR, 2019). Este anteprojeto foi encaminhado à Câmara dos Deputados em novembro de 2020 (STJ, 2020), no entanto é necessário que algum parlamentar apresente o projeto para que ele tramite na casa legislativa, e isso ainda não ocorreu.

Por conseguinte, a matéria de tratamento de dados na segurança pública em sentido amplo está em um vácuo legislativo no Brasil, o que acarreta insegurança jurídica nos deveres a serem cumpridos pelas autoridades públicas e nos direitos dos cidadãos titulares de dados.

Por outro lado, apesar do RGPD não se aplicar a esse cenário, a UE aprovou, concomitantemente ao regulamento, a Diretiva 2016/680, chamada Diretiva sobre a Proteção de Dados na Polícia e no Judiciário. Como diretiva, ela é resultado de um ato legislativo da União Europeia, mas deve ser transposta pelos países membros por meio da promulgação de uma lei específica que observe os parâmetros mínimos indicados na Diretiva. O Capítulo II dessa normativa evidencia os princípios que regem a matéria de proteção de dados na esfera criminal, tais como o princípio da finalidade, da exatidão e da segurança, além dos prazos de conservação das informações pessoais e as condições específicas do tratamento. Além disso, a Diretiva dispõe sobre os direitos dos titulares de dados, as responsabilidades e as obrigações dos agentes de tratamento, além dos casos de cooperações e transferências de dados para outros agentes (UNIÃO EUROPEIA-a, 2016).

Diante dessa perspectiva, essa matéria de proteção de dados é tratada de forma diferente no contexto brasileiro e europeu, em vista das proteções já conhecidas e positivadas pelo ordenamento europeu e a falta de lei específica no Brasil. Este vácuo legislativo evidencia o silêncio e a omissão do Estado brasileiro em garantir o devido tratamento de dados pessoais em um contexto tão caro à concretização de direitos humanos e direitos fundamentais, tais como a privacidade e a inviolabilidade da vida privada (BRASIL, 1988).

1.2.5. Tratamento de dados pessoais para segurança nacional e outros similares

A utilização de informações pessoais para ações de segurança nacional e hipóteses similares também é excepcionada nas normativas sobre proteção de dados em ambas as regiões. A LGPD apresenta essa exceção no art. 4º, III, “b” e “c”, para os casos de uso de dados de defesa nacional e segurança do Estado. Assim como as hipóteses de tratamento de dados para segurança pública, investigação e repressão de infrações penais, a lei prevê a necessidade de uma legislação específica sobre o assunto que observe os princípios da proteção de dados pessoais, os direitos do titular e o devido processo legal. No entanto, atualmente, ainda não há projeto de lei ou mesmo anteprojeto nesse sentido.

O RGPD segue lógica parecida. O art. 2, nº 2, (a) determina sua não aplicação nas hipóteses de tratamento de dados efetuados no exercício de atividades não sujeitas à aplicação do direito da União, como é o caso do tema atinente à segurança nacional (UNIÃO EUROPEIA, 2016).

Já o art. 2º, nº 2, (b) exclui da aplicação do RGPD o uso de informações pessoais efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito do título V, capítulo 2, do Tratado da UE, ou seja, questões relacionadas à política externa e de segurança comum (UNIÃO EUROPEIA-B, 2016).

Segundo o considerando 16 do RGPD, o regulamento não se aplica a questões de proteção dos direitos e liberdades fundamentais ou à livre circulação de dados pessoais relacionados às atividades não abrangidas pelo âmbito de aplicação do direito da UE, como as atividades relativas à segurança nacional.

Ainda, o RGPD não se aplica ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relacionadas à política externa e de segurança comum da União. Nesse diapasão, o art. 23 do Tratado da União Europeia dispõe especificamente sobre essas atividades na UE para delimitação de uma política comum de defesa que poderá conduzir a uma defesa comunitária entre os países membros (UNIÃO EUROPEIA-B, 2016).

2. Estudos de Caso

O escopo material das leis de proteção de dados foi objeto de uma decisão do Tribunal de Justiça da União Europeia (TJUE) ainda durante a vigência da Diretiva 95/46. O TJUE analisou o processo C-101/01, no qual uma senhora sueca chamada Lindqvist foi acusada de violar a legislação sueca de proteção de dados pessoais ao publicar, em seu blog pessoal na internet, dados pessoais, como nome e número de telefone, de determinado número de pessoas que trabalhavam com ela numa igreja (TJUE, 2003).

A publicação dessas informações no blog pessoal da acusada ocorreu sem que os seus companheiros de trabalho, os titulares de dados disponíveis no blog, fossem informados sobre a publicação de seus dados. No entanto, assim que ela soube que seus colegas não apreciaram o conteúdo publicado, ela apagou os dados. No tribunal sueco, Lindqvist foi condenada a pagar multa, porém submeteu a questão ao Tribunal de Justiça, em vista da interpretação sobre o

direito comunitário previsto na Diretiva 95/46, que também não era aplicada nos casos de tratamento de dados para fins domésticos (UNIÃO EUROPEIA-C, 1995).

Diante deste imbróglio, o TJUE entendeu que a senhora Lindqvist realizou tratamento de dados pessoais das pessoas que trabalhavam com ela na igreja e que a exceção de aplicação da diretiva de proteção de dados nos casos de uso doméstico deve ter como objeto apenas "as actividades que se inserem no âmbito da vida privada ou familiar dos particulares, o que não é o caso do tratamento de dados de carácter pessoal que consiste na sua publicação na Internet de maneira que esses dados são disponibilizados a um número indefinido de pessoas".

Logo, o TJUE afirmou que o tratamento de dados no caso em análise não ensejaria a aplicação da exceção prevista. A decisão é relevante em vista da disseminação de páginas na internet e de redes sociais que são alimentadas com informações de pessoas para fins domésticos, mas também profissionais.

Ainda sobre o escopo material das normativas, o TJUE analisou o caso C-345/17 sobre a incidência ou não da Diretiva 95/46 no caso em que um cidadão, chamado Buivids, gravou e publicou determinado vídeo em uma delegacia da polícia nacional da Letônia enquanto fazia uma declaração no âmbito de um processo administrativo que lhe foi interposto. A autoridade de proteção de dados da Letônia concluiu que Buivids infringiu a Lei de Proteção de Dados Pessoais porque não informou aos policiais a finalidade pretendida do tratamento dos dados pessoais que lhes dizem respeito. O senhor Buivids afirmou que desejava, com a publicação do vídeo em questão, chamar a atenção da sociedade sobre algo que ele considerou constituir conduta ilícita por parte da polícia.

Com isso, o TJUE foi chamado a se manifestar sobre os limites da aplicação da Diretiva de dados. O tribunal entendeu que os Estados devem proteger os direitos fundamentais e liberdades das pessoas singulares e, em particular, o seu direito à privacidade, no que diz respeito ao tratamento de dados pessoais. Esse objetivo não pode, no entanto, ser perseguido sem a necessária conciliação entre esses direitos fundamentais e o direito fundamental à liberdade de expressão, de igual relevância. Mesmo que o senhor Buivids não seja jornalista, o Tribunal afirmou que seria preciso reconhecer, no caso concreto, o fato de que o tratamento de dados pessoais foi realizado exclusivamente para fins jornalísticos, na medida em que o vídeo busca a divulgação de informações, opiniões ou ideias para o público (TJUE, 2019).

Considerações finais

O modelo regulatório adotado pela LGPD é similar ao RGPD, de modo que o próprio escopo de aplicação material da lei brasileira também muito se assemelha ao europeu. Apesar disso, existem diferenças e omissões relevantes quanto à incidência da matéria tutelada pelas normativas de proteção de dados nas duas regiões. Estes aspectos devem ser apreciados, tendo em vista o desenvolvimento de uma sociedade da informação e da globalização e o fluxo intenso de dados, inclusive para fora do país de origem do tratamento. Essa transferência de dados entre países tem como efeito a imposição de desafios sobre formas de garantia e proteção à autodeterminação informativa e o devido tratamento de dados pessoais.

Ainda, diante da semelhança entre os modelos, os dispositivos europeus e as interpretações sobre eles influenciam o desenvolvimento doutrinário e jurisprudencial sobre conceitos e ferramentas de proteção de dados já discutidas e implementadas na União Europeia. Este aspecto é ainda mais relevante em vista do conceito de dado pessoal e das lacunas existentes, de forma que as especificações previstas no RGPD podem auxiliar possíveis interpretações sobre o escopo e o limite de um dado pessoal segundo a LGPD.

Nesse sentido, as duas normativas analisadas conferem um significado amplo ao conceito de tratamento de dados pessoais, de forma que a manipulação de uma informação relacionada a uma pessoa singular enseja a incidência da Lei. A fim de preservar-se o caráter geral da LGPD e do RGPD, entretanto, os legisladores destacaram hipóteses excepcionais e taxativas sobre a não aplicação das normativas de proteção de dados, quais sejam, o tratamento de dados para uso doméstico, jornalístico e artístico, acadêmico e em pesquisa, em segurança pública e investigação penal, e para segurança nacional e similares.

Em geral, as três primeiras exceções de aplicação das normas possuem fundamentos semelhantes entre si, de forma que a não incidência da LGPD e do RGPD para uso de dados no âmbito doméstico é justificada pela natureza essencialmente privada dessas relações. Já no caso do tratamento de dados para fins jornalísticos e artísticos, a exceção da lei é prevista diante da necessidade de proteção da liberdade de expressão e de imprensa. Porém, neste último caso, o RGPD difere da LGPD e específica alguns elementos do regulamento de proteção de dados que devem ser definidos pelos países membros, como a aplicação dos princípios do regulamento e dos direitos dos titulares previstos nele. Já o uso de informações pessoais para fins acadêmicos e de pesquisa também não está no escopo material amplo das normativas por motivações

similares quanto ao desenvolvimento científico, mas é regulado de forma peculiar pelo regulamento europeu, frente aos dispositivos da LGPD.

Já a exceção de aplicação das normativas para os casos de tratamento de dados pessoais para fins criminais, seja diante da segurança pública e investigação, seja diante da segurança nacional e questões correlatas à defesa do Estado, é tratada de forma diferente entre as relações em análise. A LGPD não é aplicada a essas hipóteses, mas determina a necessidade de edição de lei própria que observe, principalmente, os princípios de proteção de dados e os direitos dos titulares. No entanto, ainda não existe nenhuma regulação neste sentido.[6] Já a UE possui um arcabouço normativo complexo a fim de equilibrar a proteção de dados e outros direitos fundamentais, por meio da Diretiva UE 680/2016.

Portanto, o escopo material das normas de proteção de dados é abrangente, e é nesse sentido que elas alcançam a pretensão de serem gerais e aplicáveis às mais diversas formas de tratamento de informações pessoais realizadas pelos diferentes setores da sociedade, nos âmbitos público e privado. Assim, a fim de balancear o âmbito de incidência dessas normas em um contexto de intensificação dos fluxos de dados, as normas destacam hipóteses específicas que, diante de uma justificativa adequada, são exceções à aplicação da LGPD e do RGPD. Com o passar do tempo, todavia, será possível a consolidação de uma jurisprudência robusta sobre a incidência da LGPD em vista de seu escopo material e suas exceções de aplicação.

[6] Para preencher essa lacuna, nota-se que foi apresentado ao Presidente da Câmara dos Deputados um anteprojeto de Lei para o tratamento de dados pessoais na segurança pública e persecução penal chamada LGPD Penal. O anteprojeto foi construído por uma comissão de juristas sob a relatoria da Professora Laura Schertel.

Referências bibliográficas

ALMEIDA, Eduarda Costa. Reconhecimento facial e segurança pública: como garantir a proteção de dados pessoais e evitar os riscos da tecnologia. *In:* ARAS, Vladimir Barros, *et al.* **Proteção de dados pessoais e investigação criminal**. Brasília: ANPR, 2020.

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

CUNHA, Daniel Alves da, e outros. **Guia do processo de adequação ao regulamento geral de proteção de dados: implementação e auditoria**. Coimbra: Edições Almedina, S.A., 2020. p. 11

DOHMANN, Indra. A Proteção de Dados Pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. **RDP**, Brasília, Volume 17, n. 93, 9-32, maio/jun. 2020, p. 20

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo, *et al.* **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

DLA PIPER. **Data Protection Laws of the World**. 2021. Disponível em: https://www.dlapiperdataprotection.com/ Acesso: 15 jul. 2021.

EUR-LEX. **Regulamentos da União Europeia**. 2015. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:l14522. Acesso: 15 jul. 2021.

MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a Lei Geral de Proteção de Dados não se aplica? .*In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.) **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters. Brasil, 2019.

MONDSCHEIN, Christopher. F; MONDA, Cosimo. The EU's General Data Protection Regulation (GDPR) in a Research Context. In: Kubben P., Dumontier M., Dekker A. (eds) **Fundamentals of Clinical Data Science**. Springer, Cham.2018. Disponível em: https://doi.org/10.1007/978-3-319-99713-1_5. Acesso: 15 jul. 2021.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão de 6.11.2003, processo C-101/01**. 2003. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62001CJ0101&from=en. Acesso: 15 jul. 2021.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão de 14.02.2019, processo C-345/17. 2019**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62017CJ0345. Acesso: 15 jul. 2021.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamentos Europeu e do Conselho de 27 de abril de 2016** relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. 2016. Disponível em:https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso: 15 jul. 2021.

UNIÃO EUROPEIA-A. **Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680#d1e1324-89-1. Acesso: 15 jul. 2021.

UNIÃO EUROPEIA-B. **Tratado da União Europeia (versão consolidada)**. 2016. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF. Acesso: 15 jul. 2021.

UNIÃO EUROPEIA-C. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995**, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 1965. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso: 15 jul. 2021.

UNIÃO EUROPEIA-D. **Tratado sobre o Funcionamento da União Europeia**. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14527. Acesso: 15 jul. 2021.

UNIÃO EUROPEIA-E. **Carta dos direitos fundamentais da União Europeia** (2016/C 202/02). 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR. Acesso: 15 jul. 2021.

WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ci. Inf.,** Brasília, v. 29, n. 2, p. 71-77, maio/ago. 2000. Disponível em: https://www.scielo.br/j/ci/a/rmmLFLLbYsjPrkNrbkrK7VF/?lang=pt&format=pdf. Acesso em: 22 de jul. 2021.

O CONSENTIMENTO VÁLIDO NA INTERPRETAÇÃO DO RGPD E DA LGPD: UMA ANÁLISE ENTRE AS SIMILITUDES E DISPARIDADES ENTRE AMBAS AS LEGISLAÇÕES

Isabela de Araújo Santos[1]

Dispositivos da LGPD	Dispositivos do RGPD
Art. 5º Para os fins desta Lei, considera-se: (...) **XII** - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; (...)	**Artigo 4º** - Definições Para os fins deste Regulamento, entende-se por: (...) (11) "consentimento" do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento; (...)

Introdução

Em um Estado Democrático de Direito, a regulação jurídica do tratamento de dados pessoais está amparada na ideia de que o indivíduo deve usufruir de autodeterminação informacional, ou seja, "deve ter o poder para controlar livremente a revelação e a utilização dos seus dados pessoais na sociedade, preservando, assim, a sua capacidade de livre desenvolvimento de sua personalidade" (MENDES, 2014, p. 60).

Logo, para que o indivíduo consiga exercer seu poder de autodeterminação informativa, torna-se necessário um instituto jurídico pelo qual possa expressar sua vontade de autorizar ou não o processamento e tratamento de seus dados pessoais: o consentimento (MENDES, 2014).

Veremos, no presente artigo, que diversas são as situações envolvendo o consentimento dos titulares de dados no contexto europeu e no brasileiro. O primeiro caso que será analisado é o "Processo C-61/19", que consiste em um acórdão do Tribunal de Justiça da União Europeia (TJUE) cujas justificativas do julgamento elucidam muito bem a definição de consentimento válido sob a luz da legislação europeia. O segundo caso a ser apresentado será o acórdão de um Agravo de Instrumento julgado pelo Tribunal de Justiça do Distrito Federal (TJDFT), do qual

[1] Bacharela em Direito pela Universidade de Brasília e atuante na área de proteção de dados pessoais e análise regulatória de novas tecnologias na Bioni Consultoria.

poderemos extrair a importância dada pela Lei Geral de Proteção de Dados (LGPD) brasileira ao consentimento dos titulares de dados.

Ademais, insta salientar que o Guia (*Guidelines*) de nº 5 do *European Data Protection Board* (EDPB) trata, minuciosamente, da importância do consentimento como alicerce de garantia ao direito à proteção de dados, além de determinar critérios para sua utilização como base legal adequada para o tratamento de dados pessoais. A Lei Geral de Proteção de Dados, por sua vez, também apresenta requisitos específicos para utilização do consentimento dos titulares, de modo que se coaduna a diversos dispositivos do *General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados - RGPD), divergindo, todavia, sutilmente em certos pontos, como veremos adiante.

1. Estudos de Caso

Passemos, desta feita, à análise dos casos europeu e brasileiro, a fim de esmiuçar os aspectos relevantes para a definição de consentimento válido em cada uma das respectivas legislações.

1.1. Case C-61/19 - TJUE

O primeiro caso a ser avaliado no presente artigo é o processo C-69/19, julgado pelo TJUE em 11 de novembro de 2020. Trata-se de um pedido de decisão prejudicial apresentado pela empresa Orange România S.A. - que presta serviços de telecomunicações móveis no mercado romeno - contra a Autoridade Nacional de Supervisão de Tratamento de Dados Pessoais da Romênia (ANSPDCP), que havia aplicado multa à empresa por ter recolhido e conservado cópias de títulos de identidade dos seus clientes, sem o consentimento válido destes, tendo a autoridade lhe ordenado que destruísse essas cópias (UNIÃO EUROPEIA, 2020b).

A condenação à pena pecuniária foi aplicada com fundamento na Diretiva 95/46 da União Europeia, que estabelece, em seu artigo 2º, alínea ‘h’, que o consentimento somente será considerado válido se for uma manifestação de vontade livre, específica e informada, por meio da qual o titular aceita que seus dados pessoais sejam objeto de tratamento. Ademais, a Diretiva ainda preconiza, em seu artigo 10, que os Estados-Membros da União Europeia devem estabelecer que os responsáveis pelo tratamento dos dados forneçam aos titulares pelo menos as seguintes informações:

> i) identidade do responsável pelo tratamento e, eventualmente, do seu representante;
> ii) finalidades do tratamento a que os dados se destinam;
> iii) outras informações, tais como: os destinatários ou categorias de destinatários dos dados, oua existência do direito de acesso aos dados que lhe digam respeito e do direito de os retificar, desde que sejam necessários, tendo em conta as circunstâncias específicas da obtenção dos dados, para garantir aos titulares um tratamento adequado de suas informações.

Ademais, a ANSPDCP justificou a aplicação da multa à Orange România com base nos artigos 32 e 42 do Regulamento 2016/679 - cuja vigência revogou a Diretiva 95/46 -, que enunciam, dentre outras hipóteses, os requisitos para a verificação do consentimento válido dos titulares de dados. Tal consentimento válido, segundo os dispositivos citados do Regulamento 2016/679, deve ser obtido mediante um **ato positivo claro** que indique uma manifestação de **vontade livre, específica, informada e inequívoca** de que o titular de dados consente ao tratamento dos dados que lhe digam respeito, como, por exemplo, mediante uma declaração escrita, inclusive em formato eletrônico, ou uma declaração oral.

Logo, sob a égide da legislação europeia, sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento autorizado e do seu alcance.

Após verificar que os preceitos e pré-requisitos de tratamento de dados pela base legal do consentimento coadunavam-se explicitamente com a legislação europeia, o TJUE concluiu, no presente caso, que **os clientes não validaram seu consentimento livremente**, uma vez que a Orange România havia recolhido cópias das carteiras de identidades de clientes que não teriam autorizado validamente o tratamento de tais informações, bem como obteve o consentimento dos clientes estritamente por meio de cláusula contratual relativa à conservação de cópias dos atos que continham dados pessoais para fins de identificação.

Isso porque **o simples fato de a cláusula contratual ter sido validada não demonstraria uma manifestação positiva do consentimento** desses clientes para que fosse recolhida e conservada uma cópia do seu documento de identidade. Afinal, não há como demonstrar que essa cláusula foi efetivamente lida e, muito menos, entendida por esses titulares em seu conteúdo e alcance.

Ademais, torna-se importante destacar que caberia ao próprio responsável pelo tratamento dos dados - no caso, a Orange Romênia - provar que os titulares dos dados manifestaram seu consentimento por ação livre e inequívoca. Igualmente, também caberia à empresa demonstrar previamente que foram disponibilizadas informações a respeito de todas as circunstâncias relacionadas com esse tratamento, de modo inteligível e de fácil acesso e numa linguagem clara e simples - o que não ocorreu na situação narrada.

Por essas razões, o pedido da Orange Romênia foi negado pelo TJUE, tendo sido mantida a decisão de primeiro grau, bem como a multa aplicada pela ANSPDCP.

1.2. Agravo de Instrumento nº 0749765-29.2020.8.07.0000 - TJDFT

O TJDFT julgou, em 01 de junho de 2021, uma situação similar ao Processo C-61/19, no que tange à definição do consentimento válido e em que momento esse consentimento deve ser requerido, de acordo com as respectivas legislações.

No caso, o Ministério Público do Distrito Federal e Territórios (MPDFT) interpôs agravo de instrumento contra decisão de primeiro grau que havia indeferido concessão de tutela de urgência a fim de suspender a comercialização, por parte da SERASA S.A., de dados pessoais de titulares por intermédio de produtos inscritos em serviços de "Lista Online" e "Prospecção de Clientes".

O MPDFT afirmou que a empresa estaria comercializando os dados de milhões de brasileiros - tais como sexo, idade, poder aquisitivo, classe social, localização, modelos de afinidade e triagem de risco - por meio desses serviços. O custo do serviço girava em torno de R$ 0,98 por indivíduo e exigiria um universo de 150.000.000,00 de CPFs, demonstrando claramente que a situação se configuraria como um grande incidente de segurança monetizável ou mesmo um vazamento de dados.

Desta feita, o TJDFT entendeu que a atitude por parte da SERASA S.A. iria de encontro com a LGPD, uma vez que esse diploma normativo impõe a necessidade de manifestação específica para cada uma das finalidades para as quais os dados estão sendo tratados. Por essa razão, o compartilhamento dos dados, na forma como realizado pela empresa, seria ilegal e desrespeitaria o direito à privacidade dos cidadãos brasileiros - como disposto no artigo 5º, inciso X, da Constituição Federal brasileira -, assim como feriria seus direitos à intimidade,

privacidade e honra dos titulares dos dados - como estabelecido no artigo 2º, incisos I e IV da LGPD.

O Tribunal ainda acrescentou que, em relação aos dados pessoais sensíveis - que também estiveram envolvidos no caso em questão -, de acordo com o artigo 11 da LGPD, em seu inciso I, o tratamento somente é cabível com o consentimento do titular ou responsável, manifestado de forma específica e destacada, ressalvadas hipóteses excepcionais, descritas no inciso II, em que é dispensado o consentimento do titular.

Ademais, **diferentemente do que alegava a empresa, o fato de a LGPD dar tratamento específico aos dados sensíveis não exclui a proteção aos demais dados pessoais, conforme se extrai da interpretação do artigo 7º da LGPD.** Não haveria como considerar, portanto, a situação fática apresentada como uma hipótese de dispensa do consentimento, pois **não seria um caso de legítimo interesse da empresa** - preconizado no inciso IX do referido artigo -, **muito menos de compartilhamento de dados com finalidade de proteção ao crédito** - como explicita o inciso X do artigo 7º.

Segundo o TJDFT, a interpretação que se extrai do art. 7º, da LGPD, portanto, é a de que **o consentimento pelo titular é a regra principal a ser observada para o tratamento de dados pessoais**, "tanto é que o § 4º, daquele dispositivo, prescreve textualmente - de forma a evitar dúvidas interpretativas - a dispensa do consentimento apenas para os dados tornados manifestamente públicos pelo titular" (DISTRITO FEDERAL E TERRITÓRIOS, 2021).

Portanto, para os dados não sensíveis, o controlador que, nos termos da lei, tenha interesse e legitimidade, deveria, de igual forma, obter o consentimento dos titulares, ressalvada a hipótese de dados tornados manifestamente públicos pelo titular - o que não se verifica na situação em análise, por não se tratar de hipótese meramente cadastral, mas, sim, comercial.

O Tribunal, destarte, considerou ilícito o compartilhamento de dados realizados pela SERASA S.A., determinando a suspensão da comercialização de dados pessoais pela empresa por meio de produtos por "Lista Online" e "Prospecção de Clientes", além de ter aplicado uma multa no valor de R$ 5.000,00 por venda efetuada.

2. Legislação europeia e brasileira: o consentimento dos titulares de dados pessoais

Tendo em vista os julgamentos relatados, é possível relacioná-los com outras questões importantes relativas aos direitos de titulares de dados em ambos os ordenamentos jurídicos mencionados.

No primeiro momento, será examinado o RGPD e suas nuances a respeito da base legal do consentimento, bem como será mencionado o Guia de nº 5 do *European Data Protection Board*, que originaram o entendimento no que tange ao consentimento contido no regulamento, para, em seguida, realizarmos uma análise da legislação brasileira. Com isso, a partir de uma perspectiva comparada, será possível identificarmos as diferenças e semelhanças da posição adotada por cada legislação quanto à base legal do consentimen**o** dos titulares de dados pessoais.

2.1. O Regulamento Geral sobre a Proteção de Dados europeu

Assim como a Diretiva 95/46 e o Regulamento 2016/679, o Guia de nº 5 do *European Data Protection Board*, de 4 de maio de 2020, estabelece uma análise da noção do consentimento no Regulamento Geral sobre a Proteção de Dados da União Europeia, focando nas mudanças dessa concepção desde a publicação no "Opinion 15/2011" publicado pelo extinto Article 29 Working Party.

Segundo o referido Guia*s*, passou a ser obrigação dos controladores de dados a descoberta de novas soluções de operação com observância de parâmetros legais a respeito da proteção de dados pessoais e do interesse dos seus fornecedores.

De acordo com o artigo 6(1) do RGPD, o consentimento é uma das seis bases legais para o tratamento de dados pessoais:

> Artigo 6. Licitude do tratamento
> 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
> **(a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas**;
> (b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
> (c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

> (d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
> (e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
> (f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. (UNIÃO EUROPEIA, 2016a) - (grifos nossos)

Ademais, o artigo 4(11) do RGPD define o consentimento como "uma manifestação livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento" (UNIÃO EUROPEIA, 2016b).

Desta feita, para que se entenda plenamente como o consentimento deve ser aplicado sob a ótica do RGPD, devemos analisar cada elemento que caracteriza sua validade: a necessidade de ele ser dado livremente, de ser específico, de ser informado e de ser fornecido explicitamente por ato positivo claro e inequívoco.

2.1.1. O consentimento livre

O elemento da liberdade, no contexto da proteção de dados, implica a real possibilidade de escolha e de controle do titular sobre seus dados. Logo, se houver qualquer tipo de pressão ou coação para a concessão desse consentimento, sob pena de consequências negativas exageradas, o consentimento não será tido como lícito.

Além disso, a relação entre o controlador e o titular de dados é considerada desequilibrada, principalmente quando esse controlador é uma autoridade pública ou em contexto laboral entre empregado e empregador. Nesses casos, pode-se discutir a inadequação do consentimento como base legal a ser utilizada para fundamentar o tratamento de dados pessoais, tendo em conta essa assimetria de poder relacional.

Desse modo, para que o consentimento seja efetivamente livre, não pode estar vinculado a nenhum tipo de empacotamento (*bundling)* com aceitação de termos ou condições, nem a nenhuma amarração (*tying)* com previsões contratuais ou serviços que não sejam necessários para a plena eficácia contratual. Ou seja, as bases legais do consentimento e do contrato não

podem, de maneira alguma, serem confundidas, pois isso limitaria a liberdade de escolha dos titulares de dados.

Logo, é necessária uma vinculação objetiva entre o processamento de dados e o propósito de execução do contrato. Um exemplo em que não há respeito a essa conexão de finalidade contratual seria a situação hipotética de um aplicativo de edição de foto requer, ao seu usuário ou à sua usuária, o acesso a sua geolocalização, sem dar a opção a esses usuários de não consentir com esse fornecimento de informação para usufruir de seu serviço. Considerando que a geolocalização não é um dado necessário para a edição de fotos – finalidade a que o aplicativo se propõe –, torna-se ilícito o consentimento dado pelos usuários, a partir do momento em que se constata que o consentimento não foi fornecido livremente (UNIÃO EUROPEIA, 2020a).

Outrossim, insta salientar que, quando um serviço envolve múltiplos processamentos de dados para mais de um fim, há a necessidade de que o titular e eventual fornecedor dos dados possa escolher quais dados ele permite serem processados, em vez de terem de consentir por todo um pacote de dados para diversos propósitos. O consentimento deve ser dado para cada um deles, devendo haver, portanto, **granularidade**.

Um caso que exemplifica claramente uma situação não granular de consentimento é a situação em que uma loja pede o consentimento dos seus clientes cadastrados para fornecer dados a fim de enviar-lhes, por e-mail, as ofertas do mês e , concomitantemente, para divulgar esses mesmos dados com outras lojas do mesmo grupo empresarial para finalidades de *marketing*. Considerando que, nessa situação, não houve separação de autorizações para cada finalidade, não houve granularidade no requerimento do consentimento.

Ademais, cabe destacar que, para que o consentimento seja livre, há a necessidade de o controlador de dados demonstrar que o titular pode recusar ou retirar o consentimento sem detrimento algum, ou seja, sem nenhum custo ou desvantagem. Algumas situações que podem configurar detrimento são: intimidação, coerção ou qualquer outro tipo de consequência negativa para o titular e eventual fornecedor dos dados.

2.1.2. O consentimento específico

Além de livre, o consentimento válido deve ser específico e, para que isso ocorra, a noção de granularidade tem suma relevância novamente: o controlador deve separar informações a fim de determinar especificamente os propósitos para os quais pretende tratar aqueles dados.

Essa exigência de especificidade do uso dos dados coletados tem como objetivo evitar a ocorrência do fenômeno denominado de *function creep*, isto é, quando nossos dados são usados para um fim diferente daquele originalmente justificado. Isso faz com que os controladores que desejem obter consentimento de coleta de dados para vários diferentes propósitos devam proporcionar aos titulares opções *opt-in* separadas para cada um desses fins aos quais serão destinados esses dados.

Por fim, já que os controladores devem fornecer informações específicas sobre a finalidade do tratamento dos dados, isso já indica também para a necessidade de que o consentimento seja informado, como outro pressuposto de sua validade.

2.1.3. O consentimento informado

Para que se configure o consentimento informado, o RGPD elenca, em seu artigo 20 o conjunto mínimo de informações necessárias a serem passadas ao fornecedor de dados, sendo elas (UNIÃO EUROPEIA, 2016a):

> i) a identidade do controlador;
> ii) o propósito de cada operação de processamento;
> iii) que tipo de dados serão coletados e usados;
> iv) a existência do direito de retirada do consentimento;
> v) informações relativas a decisões automatizadas; e
> vi) possíveis riscos concernentes à transferência de dados.

Portanto, pode-se constatar que o RGPD não prescreve a forma pela qual as informações mínimas devem ser veiculadas, de modo que a informação sobre o consentimento pode ser alcançada de diversas maneiras, como, por exemplo, por declarações escritas ou orais, por mensagens de vídeos ou por áudios.

Todavia, independentemente da forma veiculada, essa informação deve apresentar uma linguagem clara e compreensível para todas as pessoas. E, se por um acaso, esse controlador

visa a obter consentimento de titulares que são responsáveis por crianças, pessoas analfabetas, ou portadoras de deficiências auditivas e/ou visuais, por exemplo, ele deve adequar a linguagem da informação veiculada para que seja compreensível para o respectivo público.

2.1.4. O consentimento explícito por ato positivo claro e inequívoco

O consentimento ainda requer um ato positivo claro e inequívoco que não demonstre, de maneira alguma, ambiguidade. Isso significa que o fornecedor deve ter consentido por meio de uma ação afirmativa, que pode ter sido obtida por diversos meios - escritos, orais, inclusive eletrônicos.

Logo, o silêncio ou a mera falta de manifestação do titular de dados não podem ser considerados formas de obtenção do consentimento. Contudo, os controladores ainda têm a liberdade de obter o consentimento por meios alternativos, a exemplo de movimentos físicos dos titulares, desde que estes sejam qualificados como atos afirmativos.

Um possível exemplo de manifestação de consentimento por movimento físico é ilustrado na situação em que, em um aplicativo de *delivery*, como iFood e Uber Eats, para permitir o acesso à geolocalização, o usuário ou a usuária tenha de clicar o dedo sobre a tela do aparelho móvel para fornecer esse consentimento de maneira explícita.

Contudo, de maneira a obter o consentimento explícito propriamente dito, é necessária a configuração de situações em que há claro risco de falha na proteção de dados dos titulares. O Guia de nº 5 do EDPB elencam duas hipóteses mais usuais: na transferência internacional de dados e na automatização de decisões, incluindo casos de *profiling* (perfilização).

Logo, o termo “explícito” refere-se ao modo como o titular expressou seu consentimento: ele deve explicitá-lo normalmente por meio de uma declaração escrita para que seja evitada potencial dúvida futura quanto à validade daquele consentimento. Porém, é fato que hoje temos outros meios de obtê-lo, a exemplo de preenchimento de formulário online, envio de e-mail, escaneamento de documento assinado ou assinando-o eletronicamente.

2.1.5. Condições adicionais para a obtenção de consentimento válido segundo o RGPD

Cumpre ainda frisar que há uma obrigação do controlador de dados de demonstrar o consentimento dado pelo titular. O RGPD não diz exatamente como essa demonstração deve ser feita, contudo, é fato que há esse ônus da prova do controlador evidenciado nas Diretrizes de nº 5 (UNIÃO EUROPEIA, 2020a).

Ademais, o RGPD não estabelece uma regra de tempo de duração do consentimento, pois isso dependeria do contexto e da finalidade aos quais a coleta de dados se propôs a cumprir. Quando essa finalidade acaba, os dados devem ser, a princípio, deletados.

Em relação à revogação do consentimento, vale apontar ainda que o RGPD não faz menção se a obtenção e a retirada devem ser feitas pela mesma ação. Todavia, se o consentimento foi obtido, por exemplo, por meio eletrônico, como deslizando a tela do celular, a retirada dele deve ser realizada por um meio e por uma ação de igual facilidade e acessibilidade.

O EDPB ainda menciona, nessa diretiva, a situação atribuída às crianças: os menores de dezesseis anos só poderão dar seu consentimento sob autorização de seus responsáveis, exceto se o controlador de dados for autoridade pública, o que autorizaria o menor a partir dos 13 anos a fornecer esses dados livremente, sem prévia autorização.

Por fim, as Diretrizes de nº 5 esclarecem que, quando os dados são coletados para fins de pesquisa, a especificidade e a granularidade podem ser flexibilizadas. Porém, isso não significa que não deve haver transparência por parte do controlador e do operador dos dados. Logo, como forma de proteção dos titulares, os controladores são incentivados a se utilizar de ferramentas, como a anonimização e a minimização, para que os direitos desses fornecedores de dados sejam resguardados ao máximo.

2.2. Entendimentos atuais da LGPD no que concerne o consentimento dos titulares

O consentimento na Lei Geral de Proteção de Dados Brasileira é interpretado de maneira semelhante ao do Regulamento Geral sobre a Proteção de Dados Europeu, embora possua suas particularidades, a serem elucidadas nesta seção.

Em seu artigo 5º, inciso XII, a LGPD define o consentimento como uma "**manifestação livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados

pessoais para uma finalidade determinada" - grifos nossos (BRASIL, 2018). Assim, o consentimento pode ser considerado, em certa medida, um processo de tomada de decisão do titular de dados. Em adição, em seu artigo 7º, o consentimento é elencado como uma das dez bases legais para o tratamento de dados (BRASIL, 2018):

> CAPÍTULO II
> DO TRATAMENTO DE DADOS PESSOAIS
> Seção I
> Dos Requisitos para o Tratamento de Dados Pessoais
> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - Mediante o fornecimento de consentimento pelo titular; (...)

Ademais, a LGPD, em seu artigo 8º, estabelece que o consentimento deverá ser fornecido por escrito ou por qualquer outro meio que demonstre a manifestação de vontade do titular; e, caso seja fornecido por escrito, deverá constar de cláusula destacada das demais cláusulas contratuais.

A legislação brasileira, assim como a europeia, estabelece que cabe ao controlador de dados o ônus da prova de que o consentimento foi obtido dentro dos limites legais. Outra semelhança com o RGPD seria a de que o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.

Outrossim, a LGPD declara vedado o tratamento de dados pessoais mediante vício de consentimento, além de considerar que o consentimento deve referir-se a finalidades determinadas, sendo tidas como nulas as autorizações genéricas para o tratamento de dados.

O artigo 9º da LGPD, ademais, enuncia o direito que o titular de dados tem ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva para atendimento do princípio do livre acesso.

Dentre as informações sobre o tratamento dos dados, estão inclusas (BRASIL, 2018):

> i) finalidade específica do tratamento;
> ii) forma e duração do tratamento, observados os segredos comercial e industrial;
> iii) identificação do controlador;
> iv) informações de contato do controlador;

> v) informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> vi) responsabilidades dos agentes que realizarão o tratamento; e
> vii) direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD.

Insta salientar ainda que, no §1º do art. 9º, da LGPD é estabelecido que, caso as informações fornecidas ao titular, quando o consentimento for requerido, tenham conteúdo abusivo ou enganoso ou não tenham sido previamente apresentadas com transparência, de forma clara e inequívoca, o consentimento será considerado nulo.

Contudo, na prática, esses pré-requisitos de validade do consentimento na LGPD, assim como no RGPD, podem se deparar com alguns contratempos quando observa-se a realidade dos titulares de dados, afinal muitos usuários de aplicativos, sites e plataformas digitais nem ao menos leem os termos de política de privacidade e de uso dos respectivos controladores e, quando o fazem, acabam por não entender a linguagem técnica desses termos. "Mais do que isso, caso o usuário não concorde com os termos apresentados, é comum que sua única opção seja não desfrutar de importantes produtos e serviços online. Entretanto, assim fazendo, acaba enfrentando elevados custos sociais (...)" (MENDES; FONSECA, 2020, p. 352).

"Por isso, a disciplina do consentimento não deve ser tratada sob viés negocial, mas sim a partir do poder de autodeterminação e a consideração dos direitos fundamentais em questão." (TEPEDINO; FRAZÃO; OLIVA, p. 48). Logo, pode-se inferir que nada adianta uma base legal prevista em lei se não há de fato um livre fluxo informacional e uma real autonomia dos titulares de dados pessoais. Até porque, como bem elucida Bruno Bioni:

> O ser humano não é uma ilha, ele se conforma e se desenvolve quando se relaciona com os demais "no seio da sociedade que o abriga". Nesse sentido, os dados pessoais não só se caracterizam como um prolongamento da pessoa (subjetividade), mas, também, influenciam essa perspectiva relacional da pessoa (intersubjetividade). A proteção dos dados pessoais é instrumental para que a pessoa possa livremente desenvolver a sua personalidade (BIONI, 2019, p. 83).

Ainda sobre o tema Bioni enfatiza que:

> Trata-se, portanto, de se afastar de uma estratégia regulatória puramente liberal, que é incoerente com a posição de vulnerabilidade do sujeito em causa. Necessário se faz uma maior intervenção, seja do ponto de vista do desenho normativo ou da formulação

> de políticas públicas em *lato sensu* para que se **empodere o sujeito vulnerável e, por outro lado, que não se foque apenas na instrumentalização do controle dos dados pessoais** a ponto de se pensar em uma normatização substantiva da privacidade informacional. (BIONI, 2019, p. 166) - (grifos nossos)

No caso brasileiro, desta feita, cabe à Autoridade Nacional de Proteção de Dados (ANPD) garantir a observância da autodeterminação informativa dos cidadãos, de modo a promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais. Além disso, a ANPD torna-se responsável por estimular a adoção de uma padronização de conduta por parte dos fornecedores de serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados e, consequentemente, faça haver a observância de um consentimento livre, informado, inequívoco e expresso - como bem preceitua a LGPD.

Considerações Finais

A partir da análise dos casos e dos dispositivos legais apresentados neste artigo, observa-se que a legislação europeia somente considera como livre o consentimento em que há a possibilidade de escolha por parte do titular de dados ou se o titular puder revogá-lo, sem prejuízo para si de ordem contratual e consumerista.

Em contrapartida, na LGPD, o consentimento será considerado válido se as informações apresentadas pelo controlador de dados não estiverem eivadas de conteúdo enganoso e se forem mostradas de forma clara, transparente e inequívoca.

Os casos aqui elucidados ilustram e exemplificam as delimitações das definições do consentimento trazidas por cada legislação, europeia e brasileira. De todo modo, vê-se uma clara tentativa nas duas legislações de garantia da autodeterminação informacional dos titulares de dados, a partir do momento em que se empenham em proporcionar aos indivíduos meios de exercerem essa autodeterminação por meio de seu empoderamento autorizativo frente ao tratamento e processamento de dados pessoais.

As legislações analisadas vão ao encontro, portanto, da visão do professor Danilo Doneda (2016, p. 410), no sentido de que a adoção da solução de mercado para o problema dos dados não é adequada, diante da multiplicidade de situações e interesses a eles relacionadas, que não se limitam a vetores patrimoniais.

Nesse cenário, torna-se de suma relevância compreender que a crença de que o ser humano é um sujeito completamente racional, dotado da capacidade de desempenhar um processo de verdadeira tomada decisória a fim de controlar seus dados pessoais é ameaçada por toda a complexidade envolvida no fluxo dessas informações. O titular de dados, na realidade, encontra-se em uma situação de vulnerabilidade perante os controladores, visto que há uma evidente relação assimétrica de poder entre quem disponibiliza e quem obtém esses dados (BIONI, 2019, p. 147).

Isso porque, por fim, devemos lembrar que o consentimento não é a única base legal capaz de assegurar a autodeterminação informativa dos indivíduos em um Estado Democrático de Direito, devendo haver uma conjugação de princípios e dispositivos legais favoráveis aos titulares de dados, a fim de que seu direito à proteção de dados seja devidamente observado e respeitado.

Referências bibliográficas

BIONI, B.R. Proteção de Dados Pessoais. A Função e os Limites do Consentimento. Rio de Janeiro: Forense, 2019.

BRASIL, Lei nº 13.709, de 14 ago. 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Brasília, DF. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm >, Acesso em 07 dez. 2020.

DISTRITO FEDERAL E TERRITÓRIOS. Tribunal de Justiça. Agravo de instrumento n. 0749765-29.2020.8.07.0000. Antecipação de tutela recursal. Ação Civil pública. Comercialização de cadastro de dados pessoais. Lei Geral de Proteção de Dados Pessoais. Consentimento do titular. Relator: César Loyola. Brasília, 01 de junho de 2021. Disponível em: < https://tj-df.jusbrasil.com.br/jurisprudencia/1223323853/74976529202080700000-df-0749765-2920208070000/inteiro-teor-1223324034 > Acesso em 18 set 2021.

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

MENDES, L.S. Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014.

MENDES, L.S.; FONSECA; G.C.S. da. Proteção de Dados Para Além do Consentimento: Tendências de Materialização. In: BIONI, Bruno Ricardo; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (org.). Tratado de proteção de dados pessoais. São Paulo: Gen-Forense, 2020.

TEPEDINO, G; FRAZÃO, A; OLIVA, M.D. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Revista dos Tribunais, 2019.

UNIÃO EUROPEIA. Guidelines 05/2020 on consent under Regulation 2016/679, Adopted on 4 May 2020a. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt>, Acesso em: 7 dez. 2020.

UNIÃO EUROPEIA. Tribunal de Justiça. *Reenvio Prejudicial. Processo C-61/19.* Diretiva 95/46/CE. Tratamento de dados pessoais e proteção da vida privada. Recolhimento e conservação das cópias de títulos de identidade por um prestador de serviços de telecomunicações móveis. Conceito de consentimento. Manifestação de vontade livre, específica e informada. Relator: T. von Danwitz, 2020b. Disponível em: < https://curia.europa.eu/juris/document/document.jsf;jsessionid=016DCA915515F41082B5259E51BAEE93?text=&docid=233544&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=6980149 >. Acesso em 18 set 2021.

UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

USO DE DADOS POR ÓRGÃOS DE PESQUISA: UMA ÓTICA COMPARATIVA ENTRE A LGPD E O RGPD

Fernanda Passos Oppermann Iizuka[1]

Dispositivos da LGPD	Dispositivos do RGPD
Art. 5º Para os fins desta Lei, considera-se: XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; **Art. 7º** O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: **IV** - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; **Art. 11**. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: **II** - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: **c)** realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; **Art. 13.** Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. **§ 1º** A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o	**Considerando (33)** Muitas vezes não é possível identificar na totalidade a finalidade do tratamento de dados pessoais para efeitos de investigação científica no momento da recolha dos dados. Por conseguinte, os titulares dos dados deverão poder dar o seu consentimento para determinadas áreas de investigação científica, desde que estejam de acordo com padrões éticos reconhecidos para a investigação científica. Os titulares dos dados deverão ter a possibilidade de dar o seu consentimento unicamente para determinados domínios de investigação ou partes de projetos de investigação, na medida permitida pela finalidade pretendida. **(159)** Quando os dados pessoais sejam tratados para fins de investigação científica, o presente regulamento deverá ser também aplicável. Para efeitos do presente regulamento, o tratamento de dados pessoais para fins de investigação científica deverá ser entendido em sentido lato, abrangendo, por exemplo, o desenvolvimento tecnológico e a demonstração, a investigação fundamental, a investigação aplicada e a investigação financiada pelo setor privado. Deverá, além disso, ter em conta o objetivo da União mencionado no artigo 179.o, n.o 1, do TFUE, que consiste na realização de um espaço europeu de investigação. Os fins de investigação científica deverão também incluir os estudos de interesse público realizados no domínio da saúde pública. A fim de atender às especificidades do tratamento de dados pessoais para fins de investigação científica, deverão ser aplicáveis condições específicas designadamente no que se refere à publicação ou outra forma de

[1] Fernanda P. Oppermann Iizuka é graduanda em Direita pela Universidade de Brasília, tendo cursado um semestre do programa de mobilidade Universidade de Lisboa, estudando regulação de mercados. Além disso, é diretora operacional do podcast *Talking Law and Economics* e membra do Observatório da LGPD da Universidade de Brasília.

caput deste artigo em nenhuma hipótese poderá revelar dados pessoais. **§ 2º** O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro. **§ 3º** O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências. **§ 4º** Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.	divulgação de dados pessoais no âmbito dos fins de investigação científica. Se o resultado da investigação científica designadamente no domínio da saúde justificar a tomada de novas medidas no interesse do titular dos dados, as normas gerais do presente regulamento deverão ser aplicáveis no que respeita a essas medidas. **(160)** Quando os dados pessoais sejam tratados para fins de investigação histórica, o presente regulamento deverá ser também aplicável. Deverá também incluir-se nesse âmbito a investigação histórica e a investigação para fins genealógicos, tendo em mente que o presente regulamento não deverá ser aplicável a pessoas falecidas. **(162)** Quando os dados pessoais sejam tratados para fins estatísticos, o presente regulamento deverá ser aplicável. O direito da União ou dos Estados-Membros deverá, dentro dos limites do presente regulamento, determinar o conteúdo estatístico, o controle de acesso, as especificações para o tratamento de dados pessoais para fins estatísticos e as medidas adequadas para garantir os direitos e liberdades do titular dos dados e para assegurar o segredo estatístico. Por fins estatísticos entende-se todas as operações de recolha e de tratamento de dados pessoais necessárias à realização de estudos estatísticos ou à produção de resultados estatísticos. Esses resultados estatísticos podem ser utilizados posteriormente para fins diferentes, inclusive fins de investigação científica. No fim estatístico está implícito que os resultados do tratamento para esse fim não sejam já dados pessoais, mas dados agregados e que esses resultados ou os dados pessoais não sejam utilizados para justificar medidas ou decisões tomadas a respeito de uma pessoa singular.

Introdução

A ciência é um sistema social particular orientado por imperativos institucionais guiados por crenças, fatores sociais, culturais, além de normas e regras que direcionam sua prática (MERTON, 2013).

Além dos valores universais e compromissos de conduta que a orientam, tem-se normas e valores tais quais a higidez do método e a ética, os quais estão diretamente relacionados e devem ser respeitados pelos participantes das pesquisas e comunidade científica na produção de conhecimento (ACADEMIA BRASILEIRA DE LETRAS, 2013).

Diante do desenvolvimento da ciência e dos conhecimentos por ela consolidados, é natural que o método científico também tenha evoluído para espelhar as mudanças históricas da construção de conhecimento, especialmente no contexto de uma sociedade globalizada, de modo a superar paradigmas (KUHN, 2009; SILVA, 2001).

Sendo a ciência fonte de conhecimento, é preciso que se possa constatar sua confiabilidade e a ética de sua produção, motivo pelo qual tem-se a centralidade do método científico. Nesse sentido, diante do paradigma hodierno de um Estado Democrático de Direito, cada vez mais sujeito à imersão das relações jurídicas em uma realidade mais próxima da tecnologia, é uma consequência natural que o Direito se preste a regulamentar essas novas configurações que insurgem.

Especialmente nesse contexto da sociedade da informação, tendo em vista que a produção científica é intimamente relacionada ao processo de coleta e análise de dados, é inevitável que o legislador se preocupe com o tratamento desses dados em respeito ao direito fundamental à proteção de dados pessoais.

O presente artigo, nessa senda, busca comparar a legislação de proteção de dados internacional, mais especificamente o Regulamento Geral de Proteção de Dados (RGPD), com a Lei Geral de Proteção de Dados, Lei 13.709/2018, (LGPD), no que diz respeito ao uso de dados para realização de estudos por órgãos de pesquisa.

1. Uma comparação das bases legais dos dois diplomas por um viés legislativo

1.1. O uso de dados para estudos por órgãos de pesquisa como base legal na LGPD

A LGPD é um paradigma no quadro regulatório sobre o tratamento de dados pessoais no Brasil, o qual até 2018 era insuficiente para a garantia de segurança e transparência desse processo. Mesmo que o ordenamento jurídico nacional contasse com a Lei de Acesso à

Informação, Lei 12.527 de 18 de novembro de 2011, não existia norma específica que garantisse um tratamento de dados hígido no país (GUANAES et al., 2018).

A LGPD tem como objetivo consolidar a segurança jurídica e a padronização das operações que envolvem o tratamento de dados pessoais no país, isso porque se aplica a qualquer procedimento que manipule dados pessoais, realizado por pessoa natural ou jurídica, de direito público ou privado, em território nacional.

Um dos principais conceitos que devem ser compreendidos ao tratarmos da proteção de dados é o de “base legal". As bases legais nada mais são do que as hipóteses em que os dados pessoais podem ser tratados.

No caso brasileiro, a LGPD prevê dez bases legais, quais sejam: consentimento do titular, cumprimento de obrigação legal ou regulatória, execução de políticas públicas, realização de estudos por órgãos de pesquisa, execução ou criação de contrato, exercício regular de direitos, proteção da vida, tutela da saúde, legítimo interesse e proteção do crédito.

Nesse sentido, em seu art. 7º, IV, a LGPD prevê a base legal do uso de dados para realização de estudos por órgãos de pesquisa, ressaltando que, sempre que possível, o órgão deve atentar-se à anonimização dos dados, ou seja, preferencialmente, deve-se adotar procedimentos que impossibilitem a associação direta ou indireta entre um dado e um indivíduo.

Isso porque o *modus operandi* da ciência está intimamente ligado ao processo de coleta e análise de dados pessoais, os quais são, muitas vezes, o maior recurso do estudo, especialmente quando tratamos das ciências da saúde e das ciências humanas e sociais. Esses dados, inclusive, se dividem entre dados primários - aqueles que foram coletados com a finalidade de atender ao objeto do estudo - e dados secundários ou administrativos, os quais são coletados para fins diversos e que eventualmente poderão ser usados na pesquisa científica (CONNELLY *et al.*, 2016).

Aqui, vale destacar que dispõe a lei, em seu art. 5.º, XVIII, que órgão de pesquisa representa “órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico”.

Sabe-se que os dados pessoais são usualmente coletados por agentes diversos, de modo que são acumulados independentes. Inclusive, é comum que haja o uso isolado de bases de dados pessoais de origem administrativa ou de registros do sistema de saúde, por exemplo, após a crise sanitária da Covid-19 vivida nos últimos anos.

Os dados são comumente usados na pesquisa desidentificados ou agregados em unidades administrativas, de modo que, em ambos os cenários, podem perder a condição de dados pessoais. Isso se dá pela integração de dados, a qual pode se dar tanto pela forma determinística, quanto probabilística.

É válido destacar isso justamente por conta da previsão da LGPD que dá preferência à anonimização de dados pessoais - "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" - a qual, como mencionado anteriormente, faz com que os dados coletados percam seu caráter de dados pessoais, de modo a assumir um posicionamento mais protetivo ao titular. Previsão essa similar à da legislação de proteção de dados argentina, em que se entende que sempre que possível na pesquisa científica, os dados devem ser anonimizados na coleta de dados, e que, caso não seja possível manter o anonimato, deve-se utilizar uma técnica de dissociação, para que ninguém seja identificado.

Nessa senda, tratando-se da anonimização de dados, pode-se citar como exemplo uma pesquisa de intenção de votos em período eleitoral em que são levados em consideração sexo, classe social, região geográfica e outros fatores. Resume-se o resultado da pesquisa ao ponto que é praticamente impossível saber quem foram os indivíduos que participaram dela, sendo papel do órgão que realizou o estudo a garantia da segurança e da anonimidade de seus bancos de dados.

Um dos modos de realizar tal integração é a pseudoanonimização, prevista na LGPD como "o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão através do uso de informação adicional mantida separadamente pelo responsável em ambiente controlado e seguro".

Nesse sentido, na realização de pesquisas científicas, é especialmente importante que as operações com dados enfrentem os desafios vinculados ao processo de integralização, especialmente no que se refere à confidencialidade.

No que tange à anonimização, percebe-se um aumento dos riscos, dado o desenvolvimento de algoritmos capazes de reidentificar indivíduos em base de dados, revertendo o anonimato, motivo pelo qual é necessária uma sofisticação do processo em nome da segurança desses dados, a qual envolve a combinação de vários procedimentos (HARRON; GOLDENSTEIN; DIBBEN; 2016).

Diante de todos esses desafios, uma das grandes preocupações que se deve-se ter em mente, a qual foi contemplada indiretamente pela legislação brasileira, é que os sistemas de vinculação de dados pessoais não se tornem uma *black box*, qual seja, que os bancos de dados não se tornem sistemas isolados, de modo que suas estruturas internas não se tornem desconhecidas e desprovidas de transparência.

Na pesquisa científica, é de suma importância que possa ser verificada a originalidade dos dados coletados, o tratamento a eles aplicado e a qualidade das vinculações obtidas para que seja aferida a sua confiabilidade e adequação dos dados para o propósito de sua coleta.

O entendimento consolidado quando se interpreta a legislação de proteção de dados pessoais brasileira consiste na taxatividade do rol dos artigos 7º e 11 no que se refere às hipóteses possíveis de tratamento de dados, sendo dotados de algumas previsões mais abertas e com certo grau de subjetividade (como o legítimo interesse).

Considerando essa taxatividade, o que se evidencia pela escolha do legislador brasileiro é a centralidade da coleta e tratamento de dados para pesquisas científicas e a preocupação do Estado na garantia de que o desenvolvimento da pesquisa no país se dê de forma segura, em respeito aos direitos fundamentais do titular dos dados. Nesse sentido, o sistema legal desenvolvido manifesta-se como instrumento de controle do titular sobre as suas informações pessoais e de garantia de direitos.

Indispensável, ainda, quando se trata das previsões legislativas brasileiras sobre o uso de dados para estudos por órgãos de pesquisa, mencionar as especificidades criadas para o tratamento de dados para realização de estudos em saúde pública.

Dispõe a LGPD que, na confecção de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, a serem tratados exclusivamente dentro do órgão e somente destinados à finalidade de realização de estudos e pesquisas e mantidos de forma segura, conforme práticas de segurança previstas em regulamento específico e que incluam,

sempre que possível, a anonimização ou pseudoanonimização dos dados, assim como observem os ditames éticos.

Destaca-se ainda que a divulgação dos resultados ou de qualquer trecho do estudo ou da pesquisa de que trata o caput deste artigo não pode revelar dados pessoais. O órgão de pesquisa é o responsável pela segurança da informação prevista no caput do art. 13, de modo que em cenário algum poderá permitir que esses dados sejam passados a terceiros. Prevê-se, ademais, que o acesso a esses dados cuida-se de matéria a ser regulamentada pela Autoridade Nacional de Proteção de Dados e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

A Resolução 466/2012 do Conselho Nacional de Saúde, por exemplo, referente a pesquisas envolvendo seres humanos incorpora a preocupação com a proteção de dados pessoais, contando com instrumentos como o sigilo e estipulação rígida do princípio da finalidade dos dados coletados para o estudo.

Este princípio, já supramencionado, cuida-se de uma das principais diretrizes da proteção de dados pessoais, haja vista que estabelece que os dados somente podem ser tratados para a exata finalidade que justificou sua coleta, no caso do presente artigo, a pesquisa científica.

Nesse âmbito, o Termo de Consentimento Livre e Esclarecido (TCLE) materializa-se como o principal instrumento para a coleta e tratamento de dados pessoais para pesquisa. O Processo de Consentimento Livre e Esclarecido corresponde a todas as etapas a serem observadas para que aquele que participe de uma pesquisa fornecendo seus dados possa se manifestar de maneira autônoma, livre, consciente e esclarecida (Comitê de Ética em Pesquisa com Seres Humanos, 2020). Desse modo, o TCLE trata-se de um documento que deve ser redigido pelo pesquisador em termos claros para que o participante da pesquisa possa fornecer seu consentimento para o tratamento de seus dados sem vícios.

A Resolução 466/2012 determina aspectos obrigatórios que devem estar contidos no TCLE, tais como: esclarecimento sobre forma de acompanhamento e assistência que terão direito, garantia de plena liberdade ao participante, de manutenção de sigilo, entre diversos outros requisitos.

Sobre a Resolução 466/2012, é válido destacar, ainda, que ela reconhece as especificidades éticas das pesquisas nas Ciências Humanas e Sociais e de outras que se utilizam de metodologias próprias dessas áreas, dadas suas particularidades, ou seja, reconhece que tais metodologias empregadas implicam em outra espécie de tratamento de dados pessoais.

No quadro brasileiro, destaca-se especialmente tal dispositivo normativo do Conselho Nacional de Saúde, mas há outros que tratam do tratamento de dados pessoais de forma ética na pesquisa científica, tal como a Resolução 510/2016 do Conselho Nacional de Saúde, que "dispõe sobre as normas aplicáveis a pesquisas em Ciências Humanas e Sociais cujos procedimentos metodológicos envolvam a utilização de dados diretamente obtidos com os participantes ou de informações identificáveis ou que possam acarretar riscos maiores do que os existentes na vida cotidiana, na forma definida nesta Resolução".

Tal cuidado legislativo percebido no panorama normativo do Brasil demonstra de forma clara a preocupação nacional com o estímulo da produção científica nacional dotada de ética, higidez e transparência.

1.2. A perspectiva da União Europeia: Disposições sobre o Uso de Dados para Pesquisas na RGPD

No que se refere à legislação europeia, observa-se que o uso de dados para realização de estudos por órgãos de pesquisa não é uma das bases legais do RGPD.

Observa-se, contudo, como destacado no quadro comparativo, que ainda o regulamento prevê a aplicação do diploma para a realização de investigação científica, histórica, motivo pelo qual, por mais que não haja uma regulamentação que defina a realização de pesquisa como fator que autoriza o tratamento de dados, tem-se o diploma como diretriz para a realização de políticas públicas que concernem o tratamento de dados para realização de estudos por órgãos de pesquisa.

No caso português, por exemplo, a Comissão Nacional de Proteção de Dados editou diversas orientações para o tratamento de dados pessoais de saúde, tais como as orientações referentes ao Decreto n.º 8/2020, que foi editado no contexto da pandemia para esclarecer os limites da proteção de dados para realização de pesquisas no estado de emergência a serem aplicadas a dados como de temperatura corporal e de testes diagnósticos.

Nessa orientação foram dadas também diretrizes relativas à capacidade de rastreio para realização de operações de saúde em pessoas singulares identificadas.

Foi editada, ainda no âmbito da pandemia, orientação da autoridade portuguesa no que se refere também à divulgação de informação relativa a infetados por Covid-19, limitando a possibilidade dessa publicação, por exemplo, ao determinar: "As autarquias locais não podem publicar dados de saúde com identificação das pessoas a quem os mesmos dizem respeito" (CNPD, Orientações Sobre divulgação de informação relativa a infetados por Covid-19, pág. 2).

A preocupação da autoridade portuguesa no que tange à proteção de dados é, no entanto, anterior ao RGPD e à pandemia, como pode-se observar na Deliberação n.º 1704/2015, aplicável aos tratamentos de dados pessoais efetuados no âmbito da investigação clínica. Aqui, assim como pode ser observado no RGPD, percebe-se a centralidade do consentimento do particular como chave para a realização do tratamento de dados para a investigação científica.

Para que uma pesquisa seja ética e válida no âmbito clínico, faz-se necessário que o consentimento seja expresso e esclarecido, de modo que o participante da pesquisa tenha ciência da finalidade para a qual seus dados estão sendo coletados e analisados. Valoriza-se também questões relativas ao anonimato e ao controle prévio desses dados, assim como é frisada a importância do controle desses dados em termos éticos em todas as etapas da pesquisa, mesmo no que envolve subcontratantes.

Considerações Finais

Nesse sentido, buscou o presente artigo buscou trabalhar a comparação entre ambas as políticas públicas legislativas do Brasil e da União Europeia, trazendo casos portugueses para ilustrar o panorama europeu.

A LGPD foi fortemente inspirada pelo RGPD, no entanto, no que diz respeito às bases legais dos diplomas, a legislação brasileira inovou ao prever o uso de dados para a realização de estudos por órgãos de pesquisa. O que, como demonstrado pela comparação, não significa, no entanto, que as políticas públicas europeias não protejam os sujeitos que concedem dados para a realização de investigações científicas.

O que se observa como semelhança entre as duas políticas comparadas é a centralidade do consentimento daquele que concede os dados e de que o sujeito de dados esteja esclarecido das etapas de seu uso para que a pesquisa seja realizada de forma válida e ética, preceito fundamental da metodologia científica.

Referências Bibliográficas

ACADEMIA BRASILEIRA DE CIÊNCIAS. ***Rigor e integridade na condução da pesquisa científica. Guia de Recomendação de Práticas Responsáveis.*** Rio de Janeiro: Academia Brasileira de Ciências; 2013. Disponível em: < http://www.abc.org.br/IMG/pdf/doc-4311.pdf >. Acesso em: 05 mar. 2022.

BARRETO; ALMEIDA; DONEDA. Uso de Proteção de Dados Pessoais na Pesquisa Científica. BIONI, Bruno. ***Tratado de Proteção de Dados Pessoais***. Grupo GEN, 2020. Disponível em: < https://integrada.minhabiblioteca.com.br/#/books/9788530992200/> . Acesso em: 08 mar. 2022.

BRASIL. ***Emenda Constitucional 115, de 10 de fevereiro de 2022.*** Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm>. Acesso em: 13 mar. 2022.

BRASIL, Lei nº 13.709, de 14 ago. 2018, ***Lei Geral de Proteção de Dados Pessoais (LGPD),*** Brasília, DF. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm >, Acesso em 07 dez. 2021.

COMITÊ DE ÉTICA EM PESQUISA COM SERES HUMANOS. ***Termo de Consentimento Livre e Esclarecido (TCLE).*** 2020. Disponível em: <https://cep.ufv.br/termo-de-consentimento-livre-e-esclarecido-tcle/ >. Acesso em 08 ago. 2022.

CONNELLY, R.; PLAYFORD, C. J.; GAYLE, V.; DIBBEN, C. T***he role of administrative data in the big data revolution in social science research. Social Science Research,*** v. 59, p. 1-12, 2016.

CONSELHO NACIONAL DE SAÚDE. ***Resolução n.º 466 de 12 de dezembro de 2012.*** 2012. Disponível em: <https://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf >. Acesso em 08 ago. 2022.

CONSELHO NACIONAL DE SAÚDE. ***Resolução n.º 510 de 7 de abril de 2016.*** 2016. Disponível em: <https://conselho.saude.gov.br/resolucoes/2016/Reso510.pdf >. Acesso em 08 ago. 2022.

HARRON; GOLDENSTEIN; DIBBEN. ***Methodological Developments in Data Linkage***. Wiley. 2016.

KUHN, T. S. ***A estrutura das revoluções científicas.*** 9. ed. São Paulo: Perspectiva, 2009.

MERTON, R. K. A ***ciência e a estrutura social democrática. Ensaios de sociologia da ciência.*** São Paulo: Associação Filosófica Scientiae Studia/Editora 34, 2013. p.181-198.

SILVA, E. Econ. Pesqui. ***Evolução Histórica do Método Científico, Desafios e Paradigmas para o Século XXI.*** Araçatuba, v.3. n.3, p.109-118, mar. 2001.

STRECK, Lênio Luiz; MORAIS, José Luís Bolzan. ***Ciência Política e Teoria Geral do Estado.*** Porto Alegre: Livraria do Advogado, 2000.

WEBSTER, Frank. ***Theories of Information Society.*** London and New York: Routlegde, 1995.

O LEGÍTIMO INTERESSE SOB AS LENTES BRASILEIRA E EUROPEIA

Angélica Opata Vettorazzi [1]

Dispositivos da LGPD	Dispositivos do RGPD
Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) **IX** - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou	**Art. 6º** - Licitude do tratamento **1.** O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: (...) **f)** O tratamento for necessário para efeito dos interesses legítimos perseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Introdução

É notório, hodiernamente, que o desenrolar das atividades econômicas está intimamente ligado ao fluxo de dados. No âmbito das ciências sociais, discute-se sobre o fenômeno da "datificação", um processo de transformação de todos os aspectos da vida social em dados, propiciando que essa informação tenha valor pela capacidade de análise preditiva. Nesse sentido, os agentes econômicos têm a faculdade de monetizar a matéria-prima composta pelas relações sociais cotidianas. (BIONI, ZANATTA, 2021, pp. 81-82).

É nesse contexto que se insere o legítimo interesse como uma das hipóteses autorizativas do tratamento de dados pessoais[2]. Para que se viabilizasse a atuação mercadológica no cenário de fluxo intensivo de dados, isto é, para que o mercado não dependesse necessariamente do consentimento do titular para a realização de qualquer tratamento de dados, foi criada a base legal do legítimo interesse (SOUZA, VIOLA, PADRÃO, 2019, p. 118). Contanto que o interesse do agente de mercado seja legítimo à luz das suas atividades, e atenda aos princípios da finalidade, adequação e necessidade, será possível a utilização dessa hipótese legal.

[1] Graduanda em Direito na Universidade de Brasília. Integrante do Observatório da Lei Geral de Proteção de Dados nos anos de 2021/2022.

[2] As demais bases legais que autorizam o tratamento de dados pessoais constam no rol do art. 7º da Lei 13.709/2018.

Embora a inclusão do legítimo interesse como base legal tenha sido bem-vista pelo mercado como um todo, ainda é necessária uma maior escrutinização do conceito. Isso porque a hipótese legal é dotada de subjetividade, de modo a ser necessário um esforço interpretativo para bem aplicá-la (SCHREIBER, KONDER, 2016, p. 15) e um subsídio jurisprudencial a ser construído a nível nacional. Nesse sentido, o presente artigo analisará o caso holandês GHDHA – 200.291.947/01, e o REsp 1457199/RS como aporte prático, comparando os pontos de intersecção entre as decisões.

1. Comentários

A base legal do legítimo interesse está inserida no Capítulo II da LGPD, intitulado "Do tratamento de dados pessoais". A Seção I deste capítulo, nomeada "Dos requisitos para o tratamento de dados pessoais", traz, na sequência, o art. 7º, que dispõe acerca dos fundamentos que justificam o tratamento, onde perfila no inciso IX a hipótese autorizativa do legítimo interesse do controlador ou de terceiros. No Regulamento Geral sobre a Proteção de Dados Pessoais (RGPD) , o legítimo interesse está presente na alínea f, do ponto (1), do art. 6º.

Cumpre observar que o projeto do dispositivo legal, em sua primeira versão, não possuía o legítimo interesse como uma das hipóteses legais para o tratamento. Nesse particular, o setor empresarial e a sociedade civil, por meio da segunda consulta pública, discutiram sobre a conveniência de incluir essa base legal, mediante o contexto atual de veemente fluxo de dados (JOELSONS, 2020, p. 13) e da relevância que o mercado de dados possui para diversos mercados. Sendo assim, o instituto foi desenvolvido com o intuito de evitar que a busca pelo consentimento do titular fosse um impedimento à utilização regular e legítima de dados pessoais, de forma a haver inequívoca convergência com o grande volume de dados que os agentes econômicos se deparam na contemporaneidade (SOUZA, VIOLA, PADRÃO, 2019, p. 118).

Note-se que não é autorizado ao agente de tratamento o processamento de dados pessoais sensíveis com base no legítimo interesse, dado que não consta essa hipótese autorizativa no rol do art. 9º da LGPD. Isso porque o legítimo interesse, o qual é uma exceção ao consentimento do titular, possui um caráter econômico condizente com a exploração regular de dados pessoais. Sendo assim, o legislador entendeu que a sensibilidade das informações é incompatível com a sua exploração comercial (SOUZA, VIOLA, PADRÃO, 2019, p. 118).

Cumpre destacar, nesse sentido, que o art. 10 da LGPD fornece um teste de adequação preliminar à utilização da base legal do legítimo interesse. Nesse particular, destaca-se que esse fundamento somente poderá justificar o tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: (i) apoio e promoção de atividades do controlador; e (ii) proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

O aludido fundamento jurídico enseja o tratamento somente dos dados pessoais estritamente necessários para a finalidade pretendida. Ainda, devem ser tomadas medidas que garantam a transparência do tratamento, dado que o titular tem direito ao acesso facilitado às informações sobre a utilização de seus dados, que deverão ser disponibilizadas de forma clara.

Com efeito, o art. 10 dispõe que são circunstâncias exemplificativas, cabendo ao intérprete analisar em cada caso concreto a importância do interesse para o controlador ou para terceiro. São levados em consideração a (i) proteção dos interesses por algum direito fundamental, como a liberdade de expressão e a livre iniciativa; (ii) se atendem interesses públicos; e (iii) se há reconhecimento social/cultural sobre a legitimidade do tratamento (SOUZA, VIOLA, PADRÃO, 2019, p. 125).

Importa observar, nesse sentido, a necessidade de balizamento da acepção de interesse legítimo do controlador. Afora o teste de adequação do art. 10, não consta de forma clara no texto legal demais requisitos para justificar o processamento a partir desse fundamento. Nota-se, por conseguinte, lacuna legal tendo em vista a maleabilidade do conceito, de modo a propiciar o enfraquecimento da proteção jurídica dos titulares de dados. Sendo assim, cabe à ANPD editar diretivas que supram esse vácuo.

À vista disso, considerando que o RGPD serviu como alicerce à criação da LGPD no Brasil, será observada a forma de limitação do legítimo interesse na União Europeia como possível interpretação a ser aplicada no contexto brasileiro. Neste seguimento, destaca-se a atuação do Grupo de Trabalho do Artigo 29o, cujo intuito era esclarecer questionamentos acerca de dispositivos da Diretiva nº 95/46/EC, que regula o processamento de dados pessoais da União Europeia. Dessa maneira, foi editado o Parecer 06/2014 sobre o legítimo interesse do controlador. Além de recomendações, consta também neste documento a propositura de um teste para aplicação ou não dessa base legal pelo controlador de dados.

O art. 7º, da Seção II, da Diretiva 95/46/CE, do Parlamento Europeu prevê que o tratamento de dados pessoais poderá ser efetuado se o tratamento for necessário para perseguir interesses legítimos do responsável pelo tratamento ou do terceiro a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular dos dados. Em razão da ausência de pormenores acerca da aplicação dessa base legal, houve multiplicidade de interpretações nos estados membros da União Europeia, ensejando o fator insegurança jurídica (BALBONI *et al.*, 2013, p. 253).

À vista da falta de uniformidade da aplicação dessa terminologia, o Grupo de Trabalho do Artigo 29o reconheceu a premente necessidade de delimitação e sedimentação do tema. Desse modo, na data de 09 de abril de 2014, o grupo publicou o Parecer 06/2014, cujo cerne traça diretrizes para a inequívoca aplicação do interesse legítimo do controlador. O documento é de grande relevância, dado que posteriormente o RGPDo utilizou como alicerce e introjetou acepções como a do teste de proporcionalidade.

Nessa toada, o interesse legítimo do controlador insere-se na esfera da finalidade, conquanto seja mais abrangente. Há casos nos quais o interesse circunda a finalidade do tratamento de dados, ou seja, o interesse do controlador proverá os meios pelos quais será possível atingir a finalidade de tratamento dos dados. Na falta da utilização do interesse legítimo, não será possível a concretização da finalidade. Além disso, propugnou-se pela definição clara do interesse do controlador. Deve ser interesse real e atual, que seja condizente com as atividades desenvolvidas pelo controlador. Isso porque quando o interesse é demonstrado de forma vaga, existe uma maior dificuldade na ponderação entre os interesses do controlador e os direitos fundamentais do titular.

Ainda, devem ser tomadas medidas que garantam a transparência do tratamento, dado que o titular tem direito ao acesso facilitado às informações sobre a utilização de seus dados, que deverão ser disponibilizadas de forma clara. Ademais, o Parecer 06/2014 preconizou que, a partir da evidência de interesse legítimo do controlador, deveria ser aplicado o teste de proporcionalidade, intitulado *Legitimate Interest Assessment* (LIA), entre os interesses legítimos do responsável pelo tratamento e os interesses do titular dos dados. Desse modo, estabeleceu-se uma sequência de medidas a serem tomadas no caso concreto, quais sejam: (i) identificar o fundamento jurídico aplicável; (ii) verificar se o interesse do controlador é legítimo; (iii) verificar a necessidade do tratamento para atingir o interesse visado; (iv) verificar a prevalência do direito fundamental do titular sobre o interesse do responsável pelo tratamento;

(v) verificar se os interesses do titular dos dados seriam afetados; (vi) analisar as expectativas razoáveis do titular; (vii) analisar os impactos ao titular e compará-los com os benefícios auferidos pelo controlador a partir do tratamento.; (viii) estabelecer equilíbrio final tendo em vista garantias complementares de diligência no tratamento; (ix) garantir a transparência do tratamento por meio da elaboração de relatórios que demonstram as medidas tomadas; (x) garantir a existência de um canal adequado de comunicação para que o titular possa exercer seu direito de oposição ao tratamento de seus dados.

Resumidamente, o desdobramento do teste se dá em quatro fases que devem ser cumpridas para verificar o cumprimento da hipótese de legítimo interesse. As quatro fases resumem-se em: (I) avaliação da legitimidade de interesse; (II) impacto sobre o titular dos dados (necessidade); (III) equilíbrio entre os interesses legítimos do controlador e do titular (balanceamento); e (IV) medidas para resguardar o titular dos dados (SOUZA, VIOLA, PADRÃO, 2019, p. 120).

Sendo assim, o teste de proporcionalidade fornece parâmetros objetivos para verificar a legalidade dos tratamentos de dados que realizam. A primeira fase, análise da legitimidade de interesse (I), envolve a avaliação: (i) se o interesse legítimo está resguardado por direito fundamental, como a liberdade de expressão, a livre iniciativa, o direito à segurança, o direito de propriedade, e o acesso à informação; (ii) se o interesse atua em prol de interesses públicos ou de uma comunidade, além dos seus próprios interesses; (iii) se há reconhecimento social/cultural de que os interesses são legítimos, por exemplo, a partir da edição de recomendações de entidades governamentais (SOUZA, VIOLA, PADRÃO, 2019, pp. 121-122). Outrossim, para Mattiuzzo e Ponce (2020, p. 61) o interesse será legítimo quando for claro e concreto, além de não ser ilegal.

São considerados intentos legítimos pelo Grupo de Trabalho do art. 29o a prevenção de fraude, segurança da informação, marketing direto e tratamento de dados pessoais de empregados (WPDP, 2014, p. 25). Os Considerandos 47 e 49 do RGPD também mencionam a prevenção de fraudes e a garantia de segurança das redes como justificativas legítimas para o tratamento de dados.

Na segunda fase, a necessidade (II), analisa o impacto sobre o titular dos dados. Devem ser sopesados os seguintes pontos: (i) se o tratamento poderia gerar ações de terceiro ao titular; (ii) se possui potencial discriminatório; (iii) a forma de tratamento, de forma a analisar se pequenos dados em conjunto revelam informações muito particulares do titular; e (iv)

expectativa legítima do titular dos dados pessoais, ou seja, qual tratamento seria esperado de acordo com o tipo de serviço prestado, ou ainda se as obrigações legais e contratuais que podem gerar determinada expectativa (SOUZA, VIOLA, PADRÃO, 2019, pp. 122-123).

Nesse sentido, Mattiuzzo e Ponce (2020, p. 63) citam entendimento de Alexy (2015, p. 119), no campo constitucional, de forma a salientar que a necessidade diz respeito à análise da existência de medida menos gravosa para atingir aquela mesma finalidade pretendida. Em outras palavras, é preciso avaliar se há alternativa igualmente eficaz para atingir a finalidade e que seja menos custosa ao direito fundamental afetado.

A terceira fase, balanceamento (III), demonstra o equilíbrio entre os interesses do controlador e do titular. São avaliadas as medidas adotadas pelo controlador para garantir transparência no tratamento. Um tratamento adequado reduz o impacto sobre os indivíduos, devendo também haver medidas concretas por parte do controlador como a inserção de um mecanismo de *opt-out* do tratamento, cujo intuito é transferir ao titular a escolha pela permanência no tratamento (SOUZA, VIOLA, PADRÃO, 2019, p. 123).

A quarta fase (IV) envolve medidas tomadas pelo controlador quando do tratamento de dados. Quanto mais medidas de segurança o controlador toma, mais apto ele está para processar os dados. Nessa direção, destaca-se a facilitação de acesso aos princípios da LGPD, como o livre acesso por meio de consulta facilitada, a transparência, a partir do fornecimento de informações claras e precisas (SOUZA, VIOLA, PADRÃO, 2019, pp. 123-124).

No Brasil, diante das escassas decisões judiciais acerca da matéria e da recém criação da ANPD, deve-se combinar o teste de proporcionalidade proposto pelo Grupo de Trabalho do Artigo 29o e os princípios constantes na LGPD. Sendo assim, nos próximos anos, o Poder Judiciário e a ANPD poderão dar ainda mais concretude ao teste de proporcionalidade supramencionado.

O teste de proporcionalidade, por seu turno, deve ser aplicado tendo em vista a metodologia civil-constitucional. Deve-se verificar na substancialidade qual o interesse (do controlador, de terceiro ou do titular) está mais alinhado com os ditames constitucionais e, por conseguinte, deve prevalecer no ordenamento jurídico. Portanto, não há hipótese abstrata de interesse legítimo, sendo prevalente a análise casuística (SOUZA, VIOLA, PADRÃO, 2019, p. 126).

No contexto brasileiro, de forma análoga ao LIA do RGPD, o princípio da necessidade é dotado de relevância no primeiro momento. O art. 6º da LGPD dispõe em seu inciso III que deve haver limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Por consequência, o controlador deve utilizar dados do titular apenas como última hipótese, devendo ser utilizado outro caminho se for possível alcançar da mesma forma a finalidade desejada, como propugnado pelo art. 10, §1º da LGPD.

Após essa etapa, deve haver escrutínio quanto à prevalência do interesse do controlador em detrimento do interesse do titular de dados. Isso porque somente a partir da avaliação dos pormenores do caso concreto é que se pode afirmar a preponderância do interesse legítimo do controlador. O art. 37 da LGPD demonstra a importância dessa análise particular feita pelo controlador de forma documentada, salientando que o controlador e o operador devem manter registro das operações de processamento de dados que realizarem, sobretudo quando a hipótese autorizativa for a do legítimo interesse.

A doutrina internacional, nessa toada, demonstra preocupação quanto à complexidade inerente à avaliação do teste de proporcionalidade. Em primeiro lugar, a avaliação exige alto nível de expertise legal, da qual nem sempre são dotados os controladores. Ainda, a confiabilidade dos testes é questionável, dado que o próprio controlador de dados realiza o teste de ponderação, não obstante haja conflito de interesses quando na posição do controlador de dados (FERRETTI, 2014, p. 847). Por conseguinte, nota-se a sensibilidade da situação do titular dos dados, tendo em vista que a decisão de realizar ou não o tratamento depende do juízo do controlador, cujo interesse no tratamento é notável (CORDEIRO, 2019, p. 21).

Na quarta e última etapa, o agente de tratamento deve salvaguardar o titular de dados, reduzindo possíveis impactos negativos do processo. Essas medidas estão presentes ao longo da LGPD, destacando-se a: (i) anonimização (art. 12) e pseudoanonimização (art. 13); (ii) separação funcional do acesso e da utilização dos dados dentro da instituição; (iii) utilização de técnicas que otimizam a proteção da privacidade, como a criptografia e o privacy by design (art. 49); (iv) aumento da transparência; (v) possibilidade de o titular de dados realizar *opt-out*; e (vi) portabilidade de dados.

2. Estudo de Caso

2.1. GHDHA – 200.291.947/01

Trata-se de um caso[3] julgado pela jurisdição holandesa na data de 05/10/2021, cujo cerne envolve discussão sobre o legítimo interesse do controlador. Neste caso, o tribunal recursal de Haia decidiu que o interesse do titular - ora autor da ação - de ter seus dados removidos do Sistema de Informação de Crédito não deveria prevalecer sobre o legítimo interesse da Aegon, grupo segurador, de registrar a credibilidade dos seus clientes. O interesse da companhia de crédito foi, portanto, considerado legítimo, adequado e necessário.

O titular de dados requereu que a Aegon removesse do *Central Credit Information System* (CKI, sigla em holandês) códigos relativos à sua credibilidade como devedor, já que o referido registro impediu o titular de realizar novo empréstimo. O registro dos códigos é resultado da inabilidade de pagamento de uma dívida hipotecária pelo devedor. Sendo assim, foi feita a averbação, cuja data é de setembro de 2018, tendo como validade um período de cinco anos, de forma que os dados pessoais do devedor prosseguiriam no sistema até setembro de 2023.

Além do art. 6 (1)(f) do RGPD, a corte holandesa examinou o art. 21, cujo conteúdo estipula acerca do direito de objeção ao tratamento pelo titular de dados, de modo a estabelecer que o controlador não deve processar dados pessoais em caso de objeção salvo se possuir legítimo interesse que prevaleça sobre os interesses e direitos do titular de dados. Dessa maneira, a corte examinou se a sobreposição do legítimo interesse do controlador sobre os direitos do titular é necessária para o alcance da finalidade pretendida pelo controlador (teste de adequação) e se a aludida finalidade não pode ser atingida de uma maneira menos prejudicial ao titular de dados (teste de necessidade).

No caso em cotejo, é interesse dos provedores de crédito a limitação de riscos financeiros a partir do registro das operações de crédito realizadas. Esse fator implica, por conseguinte, na contabilização do pagamento ou não do crédito concedido aos clientes. Isso porque interessa ao grupo segurador o combate à inadimplência e à fraude. Sendo assim, o sistema de registro de crédito serve a esses interesses, como informar às companhias de crédito

[3] Disponível em: GHDHA - 200.291.947/01 - GDPRhub. Acesso em: 08 dez 2021.

sobre atrasos no pagamento e outras irregularidades envolvendo os clientes, ocorridas nos últimos cinco anos.

Admitiu-se a alegação do réu de que o autor da ação estava inadimplente há um longo período e não demonstrava tomar medidas para sanar a dívida, implicando ao réu arcar com um enorme montante residual do débito. Ainda, a corte reconheceu que o réu estava submetido ao risco de empréstimo excessivo, porquanto o autor também possuía inúmeros outros débitos. À vista disso, legitimou-se a importância do registro de crédito de modo que outros credores possam ter ciência dos riscos inerentes a cada empreitada. O autor não demonstrou suficientemente que os seus interesses prevaleciam em detrimento dos interesses do controlador. A corte, portanto, concluiu que o interesse do controlador em manter o registro das atividades creditórias suplantavam o interesse do titular em ter seus dados pessoais removidos do sistema de informação sobre crédito.

2.2. REsp 1457199/RS

Em paralelo, o ordenamento jurídico brasileiro também considera legítima a prática de *credit scoring*. O Superior Tribunal de Justiça, antes mesmo da edição da LGPD, decidiu no mesmo sentido da corte holandesa. Veja-se a ementa do REsp 1457199/RS, do Tema Repetitivo 710:

> RECURSO ESPECIAL REPRESENTATIVO DE CONTROVÉRSIA (ART. 543-C DO CPC). TEMA 710/STJ. DIREITO DO CONSUMIDOR. ARQUIVOS DE CRÉDITO. SISTEMA "CREDIT SCORING". COMPATIBILIDADE COM O DIREITO BRASILEIRO. LIMITES. DANO MORAL. I - TESES: 1) O sistema "credit scoring" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito) 2) Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo). 3) Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011. 4) Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais

> valoradas. 5) O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados. II - CASO CONCRETO: A) Recurso especial do CDL: 1) Violação ao art. 535 do CPC. Deficiência na fundamentação. Aplicação analógica do óbice da Súmula 284/STF. 2) Seguindo o recurso o rito do art. 543-C do CPC, a ampliação objetiva (territorial) e subjetiva (efeitos "erga omnes") da eficácia do acórdão decorre da própria natureza da decisão proferida nos recursos especiais representativos de controvérsia, atingindo todos os processos em que se discuta a mesma questão de direito em todo o território nacional. 3) Parcial provimento do recurso especial do CDL para declarar que "o sistema "credit scoring" é um método de avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito)" e para afastar a necessidade de consentimento prévio do consumidor consultado. B) Recursos especiais dos consumidores interessados: 1) Inviabilidade de imediata extinção das ações individuais englobadas pela presente macro-lide (art. 104 do CDC), devendo permanecer suspensas até o trânsito em julgado da presente ação coletiva de consumo, quando serão tomadas as providências previstas no art. 543-C do CPC (Recurso Especial n. 1.110.549-RS). 2) Necessidade de demonstração de uma indevida recusa de crédito para a caracterização de dano moral, salvo as hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011). 3) Parcial provimento dos recursos especiais dos consumidores interessados apenas para afastar a determinação de extinção das ações individuais, que deverão permanecer suspensas até o trânsito em julgado do presente acórdão. III - RECURSOS ESPECIAIS PARCIALMENTE PROVIDOS. (REsp 1457199/RS, Rel. Ministro PAULO DE TARSO SANSEVERINO, SEGUNDA SEÇÃO, julgado em 12/11/2014, DJe 17/12/2014).

No caso em questão, a Câmara de Dirigentes Lojistas de Porto Alegre (CDL) insurgiu-se contra acórdão do Tribunal de Justiça do Estado do Rio Grande do Sul, em ação coletiva de consumo ajuizada pelo Ministério Público. A CDL criou banco de dados com um cadastro dos consumidores, em que eram armazenadas informações com o intuito de avaliar a viabilidade da

concessão do crédito a estes. Acontece que a análise da anuência ou não da concessão era baseada em critérios não divulgados à clientela. Em razão do uso do banco de dados, considerou-se que a problemática se sujeitava, à época, às regras dispostas no Capítulo V, Seção VI, do Código de Defesa do Consumidor - diploma legal que endereçava a parte majoritária dos litígios concernentes ao tratamento de dados pessoais.

No juízo *ad quo*, decidiu-se pelo cabimento da indenização por danos morais. Isso porque teriam sido atingidos direitos inerentes à personalidade dos consumidores, tais quais a reputação e a imagem destes. Esta situação decorreu do fato da parte hipossuficiente não ter sido informada da sua inscrição em cadastros ou banco de dados de avaliação de crédito, como também dos critérios estabelecidos para a pontuação no registro criado pela CDL. O dano moral, por conseguinte, estaria ínsito a tal evento, não sendo necessária a comprovação de prejuízo, mas apenas a conduta ilícita, demonstrada pela falta de comunicação prévia e sua intersecção com a avaliação negativa que impossibilitou a obtenção do crédito.

No presente julgamento, nesse sentido, o STJ entendeu que a avaliação da licitude do sistema *credit scoring* deve partir da premissa de que não se trata de um cadastro ou banco de dados de consumidores, mas de uma metodologia de cálculo do risco de crédito, utilizando-se de modelos estatísticos e dos dados existentes no mercado acessíveis via internet. Em outras palavras, a ferramenta é uma fórmula matemática para avaliação do risco de concessão do crédito.

Ainda, o STJ consolidou o entendimento que é desnecessário o consentimento do consumidor consultado para atribuição de uma nota do risco de crédito. O tribunal *ad quo* suscitava a tese que o fornecedor seria obrigado a esclarecer e divulgar todos os parâmetros que regiam a análise de risco feita. Após o julgamento do Tema Repetitivo 710, devem ser fornecidos os devidos esclarecimentos tão somente quando solicitados pelo consumidor, sendo elucidadas as fontes dos dados considerados, bem como as informações pessoais valoradas.

Ademais, cumpre destacar a Súmula 550 do STJ, firmada a partir do julgamento do REsp 1457199. Veja-se, *in verbis*:

> Súmula 550-STJ: A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.

Também entendeu que o sistema *credit scoring* trata-se de prática comercial lícita, autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei 12.414/2011, cujo uso prescinde do consentimento prévio e expresso do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico, conforme decidido pela Segunda Seção desta Corte, à unanimidade de votos, no julgamento do Recurso Especial 1.419.697/RS (REsp 1419697/RS, Rel. Ministro PAULO DE TARSO SANSEVERINO, SEGUNDA SEÇÃO, julgado em 12/11/2014, DJe 17/11/2014).

Por fim, há que se observar ressalva feita com vistas a proteger os titulares de dados pessoais. Frisa-se a ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis, bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados. São consideradas excessivas as informações que não estiverem vinculadas à análise de risco de crédito, enquanto são sensíveis as informações pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas, consoante o art. 3º, § 3º, I e II, da Lei 12.414/2011. Portanto, o legítimo interesse das concedentes de crédito prevalece tão somente quando da não configuração de abuso de direito pelo uso indevido e/ou incorreto de dados pessoais.

Considerações finais

A partir da análise dos casos e dos dispositivos legais apresentados neste artigo, é evidente que a legislação europeia serviu como alicerce para a criação da base legal do legítimo interesse no ordenamento jurídico brasileiro. Tal afirmação pode ser constatada mediante análise da literalidade da lei, cuja versão brasileira revela grande similaridade com a europeia.

No RGPD destaca-se a importância da realização do teste de proporcionalidade entre os interesses do titular de dados e o interesse do controlador, prática aconselhada pelo Parecer 06/2014, do Grupo de Trabalho do Artigo 29o. A LGPD, no mesmo sentido, pugna que o legítimo interesse do controlador será válido se atender aos princípios da finalidade, adequação e necessidade.

Os casos estudados elucidam a legitimação da prática de *credit scoring*, tendo como alicerce o RGPD, no continente europeu, e o CDC e a Lei 12.414.2011, no contexto brasileiro, tendo em vista que o Recurso Especial estudado foi julgado antes da edição da LGPD. Apesar disso, o julgado coaduna os princípios propugnados pela LGPD, na medida em que faz uma

ressalva quanto ao tratamento de dados excessivo ou de dados sensíveis pelas entidades concedentes de crédito, sinalizando a devida responsabilização em caso de tais práticas.

Por fim, frise-se o anseio das duas legislações de incentivo às atividades do controlador, de forma a respeitar o caráter econômico relativo ao tratamento de dados, em consonância com a proteção do exercício regular dos direitos do titular, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

Referências bibliográficas

ALEXY, Robert. (2015). Teoria dos direitos fundamentais (V. A. da Silva, Trad.). Malheiros Editores.

BALBONI, Paolo; COOPER, Daniel; IMPERIALI, Rosario; MACENAITE; Milda. Legitimate interest of the data controller: new data protection paradigm: legitimacy grounded on appropriate protection. International Data Privacy Law, Oxford, v. 3, n. 4, 2013. p. 244-261.

BIONI, Bruno; ZANATTA, Rafael. A Infraestrutura Jurídica da Economia de Dados: dos princípios de justiça às leis de dados pessoais. Proteção de Dados: Contexto, Narrativas e Elementos Fundantes. São Paulo : B. R. Bioni Sociedade Individual de Advocacia, 2021.

CORDEIRO, Antônio Barreto Menezes. O tratamento de dados pessoais fundado em legítimos interesses. Revista de Direito e Tecnologia, Lisboa, v. 1, n. 1, 2019. p. 1-31.

DONEDA, Danilo; SCHERTEL, Laura. Reflexões iniciais sobre a nova lei geral de proteção de dados. Revista dos Tribunais: Revista de Direito do Consumidor, v. 120/2018, p. 469-483, p. 473, nov./dez. 2018.

FERRETTI, Federico. Data protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights? Common Market Law Review, United Kingdom, v. 51, 2014. p. 843-868.

GHDHA – 200.291.947/0. Disponível em: GHDHA - 200.291.947/01 - GDPRhub. Acesso em: 08 dez 2021.

GRUPO DE TRABALHO DO ARTIGO 29º DA DIRETIVA 95/46/CE. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados da acepção do artigo 7º da Diretiva 95/46/CE. Disponível em: https://www.gpdp.gov.mo/uploadfile/2015/0803/20150803050042662.pdf. Acesso em: 13 nov 2021.

JOELSONS, Marcela. O legítimo interesse do controlador no tratamento de dados pessoais e o teste de proporcionalidade europeu: Desafios e Caminhos para uma aplicação no cenário brasileiro. Revista de Direito e as Novas Tecnologias. v 8/2020. p. 13.

MATTIUZZO, Marcela.; PONCE, Paula. O legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa. Internet&Sociedade, São Paulo, v.1, n.2, p. 54-76, dezembro, 2020. Disponível em: internetsociedade.v1n2-1.pdf (internetlab.org.br). Acesso em: 10 dez 2021.

REsp 1457199/RS, Rel. Ministro PAULO DE TARSO SANSEVERINO, SEGUNDA SEÇÃO, julgado em 12/11/2014, DJe 17/12/2014.

REsp 1419697/RS, Rel. Ministro PAULO DE TARSO SANSEVERINO, SEGUNDA SEÇÃO, julgado em 12/11/2014, DJe 17/11/2014.

SCHREIBER, Anderson; KONDER, Carlos Nelson. Uma agenda para o direito civil-constitucional. Revista Brasileira de Direito Civil, Belo Horizonte, v. 10, p. 14-16, out./dez. 2016.

SOUZA, Carlos Affonso Pereira de; VIOLA, Mario; PADRÃO, Vinícius. Considerações Iniciais sobre os Interesses Legítimos do Controlador na Lei Geral de Proteção de Dados Pessoais. RDU, Porto Alegre, v. 16, n. 90, 109-131, nov-dez 2019.

REVISÃO DE DECISÃO TOMADA COM BASE EM TRATAMENTO AUTOMATIZADO: PREOCUPAÇÕES E CONSIDERAÇÕES SOBRE A EFETIVAÇÃO DA TRANSPARÊNCIA PARA COBRIR A DISCRIMINAÇÃO ALGORÍTIMICA E O PROFILING

Shana Schlottfeldt [1]

Dispositivos da LGPD	Dispositivos do RGPD
Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) **§ 1º** O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. **§ 2º** Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. **§ 3º** (VETADO). (Incluído pela Lei nº 13.853, de 2019)	**Artigo 22º** - Decisões individuais automatizadas, incluindo definição de perfis **1.** O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. **2.** O nº 1 não se aplica se a decisão: **a)** For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; **b)** For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou **c)** For baseada no consentimento explícito do titular dos dados. **3.** Nos casos a que se referem o nº 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão. **4**. As decisões a que se refere o nº 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9º, nº 1, a não ser que o nº 2, alínea a) [titular dos

[1] Doutora em Informática pela Universidade de Brasília (UnB), Brasil. Visiting PhD student at University of York, Reino Unido, bolsista do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). Mestre em Informática pela Universidad Carlos III de Madrid, bolsista da Fundação Carolina, Espanha. Bacharel em Direito pela UnB. LLB exchange student at Australian National University, Austrália. Membro do Comitê Gestor Pró-Equidade de Gênero e Raça da Câmara dos Deputados, Brasil. Pesquisadora vinculada ao Observatório da Lei Geral de Proteção de Dados da Universidade de Brasília (Observatório LGPD/UnB), Brasil. Pesquisadora vinculada ao Grupo de Estudos em Direito das Telecomunicações da Universidade de Brasília (GETEL/UnB), Brasil.

	dados tiver dado seu consentimento] ou g) [o tratamento for necessário por motivos de interesse público relevante], do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

Considerandos relevantes

(63) Modalidades e âmbito do direito de acesso.

(71) Direito de não estar sujeito a uma decisão automatizada.

(72) Aplicabilidade do RGPD à criação de perfis.

Introdução

O uso de decisões automatizadas que afetam a vida das pessoas está se tornando dia a dia mais comum. As máquinas podem aprovar pedidos de empréstimo (FTC, 2012; HARRIS, 2018); decidir se alguém deve merecer liberdade condicional ou ficar atrás das grades (BRENNAN *et al.*, 2009; LARSON *et al.*, 2016; VAN EIJK, 2017); tomar decisões de emprego (GEE, 2017; DASTIN, 2018); excluir ou colocar em desvantagem os potenciais clientes de empresas de saúde complementar de acordo com seu histórico médico; decidir acerca da empregabilidade e assim por diante (NIKLAS *et al.*, 2015; COURT, 2019; O'NEIL, 2016; COHEN, 2020, 1398).

Essas decisões são tomadas diretamente sobre o indivíduo, mas podem estar envoltas em camadas impenetráveis de complexidade e opacidade. Por exemplo, um *score* de crédito ruim pode custar a quem vai atrás de um financiamento ou empréstimo centenas de milhares de reais a mais, mas essa pessoa nunca saberá/entenderá exatamente como esse *score* foi calculado. Pior do que isso, um algoritmo pode classificar alguém como um cliente "não confiável", mas nunca lhe "contar" sobre essa decisão (MARQUES e MUCELIN, 2021, p. 143).

O presente artigo trata do direito do titular de solicitar a revisão de decisões tomadas com base em tratamento automatizado de dados pessoais. Nesse sentido, procedeu-se à análise comparativa do art. 20 da Lei nº 13.079/2018 (Lei Geral de Proteção de Dados, LGPD) e do art. 22 do Regulamento Geral sobre a Proteção de Dados (RGPD)[1], que tratam sobre a temática

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

no Brasil e na Europa, respectivamente. Por essenciais à discussão, são tratados tópicos correlatos, como discriminação algorítmica e *profiling*. Como estudo de caso, são apresentadas três decisões sobre o tema, o Recurso Especial (Resp) 1.419.697/RS, em que se discutiu a legalidade do *credit scoring*, o Caso C/13/696010-HA ZA 21-81, do Tribunal Distrital de Amsterdã, e o Caso 2020-0.436.002, da Autoridade de Proteção de Dados Austríaca, estes dois últimos à luz do RGPD. Por fim, são apresentadas as considerações finais que dão conta da importância do estabelecimento e consolidação de um direito à revisão de decisões automatizadas e que os normativos brasileiro e europeu acerca da matéria, afora pequenos detalhes, são bastante semelhantes.

1. Comentários

1.1. O que são decisões automatizadas?

A expressão Sistemas de Decisão Automatizados (*Automated Decision Systems*, ADS), no contexto da tomada de decisão, é usada para se referir às tecnologias que apoiam ou substituem o julgamento dos tomadores de decisão humanos. Sejam de fato sistemas, algoritmos ou simplesmente a aplicação de cálculos estatísticos. Esses sistemas usam técnicas como regressão, inferência baseada em regras, raciocínio baseado em casos, análise preditiva e inteligência artificial (e.g., *deep learning*, aprendizado de máquina, algoritmos genéticos, redes neurais), geralmente em combinação uns com os outros para processar dados e encontrar correlações entre eles, fazendo previsões com base em tais correlações (AUTOMATED ASSISTANCE IN ADMINISTRATIVE DECISION-MAKING WORKING GROUP, 2007, p. 4-6; MOLNAR e GILL, 2018, p. 2; BIONI e MARTINS, 2020c).

A automatização de processos decisórios inicialmente foi vista como ferramenta capaz de trazer objetividade à decisão, superando tendências de vieses e discriminação, entretanto, logo percebeu-se que ela poderia assimilar aquelas tendências já existentes nos processos tradicionais de tomada de decisões, conduzindo, igualmente, a resultados discriminatórios agora sob uma roupagem de "verdade objetiva" (BAROCAS e SELBST, 2016, p. 677; MENDES e MATTIUZZO, 2019, p. 40).

Pesquisas mostram que os humanos são psicologicamente desencorajados a desafiar decisões baseadas em IA devido ao ônus de refutá-las (McGREGOR *et al.*, 2019, p. 317-318). Assim, ainda que a decisão automatizada sirva apenas de recomendação para tomada de

decisão, ela pode ser um elemento decisivo, pois para desconsiderá-la o operador humano teria que fundamentar sua opção em elementos aferíveis quantitativamente tanto quanto as previsões algorítmicas e todo espaço de subjetividade seria eliminado (BIONI e MARTINS, 2020a). Na prática, quem decide é o algoritmo, daí a importância de um direito à revisão.

1.2. Discriminação algorítmica

O aumento no uso de decisões automatizadas fez surgir algumas preocupações, dentre elas, o potencial discriminatório e como grupos minoritários podem acabar sendo prejudicados.

Segundo Barocas e Selbst (2016), ainda que se defenda que técnicas algorítmicas eliminam os preconceitos humanos no processo de tomada de decisão, um algoritmo é tão bom quanto os dados com os quais trabalha (conforme o conhecido adágio "*garbage in, garbage out*", literalmente "lixo entra, lixo sai", i.e., dados de entrada falhos produzem saídas falhas). E não raro, os dados frequentemente refletem padrões históricos de preconceito[2] e discriminação contra minorias, i.e., padrões preexistentes de exclusão e desigualdade. Além disso, uma vez que quase sempre a discriminação resultante é uma propriedade emergente não intencional do uso do algoritmo (e não uma escolha intencional/consciente de seus programadores), pode ser particularmente difícil identificar o problema e sua origem.

Nesse contexto, utiliza-se a termo "discriminação algorítmica" para situações que refletem afirmações inconsistentes ou em que as afirmações, ainda que lógicas, consideram pessoas não como indivíduos, mas como parte de um grupo. Mendes e Mattiuzzo (2019, p. 47) apontam que ao contrário da discriminação pensada como exclusão do indivíduo de um grupo, quando se fala em discriminação algorítmica, os efeitos se verificam pela inclusão em um grupo e o consequente julgamento desse indivíduo, não por suas características particulares, mas pelas características do grupo no qual foi classificado. Trata-se de uma generalização.

Ainda segundo Mendes e Mattiuzzo (2019, p. 51-53), seriam quatro os tipos de discriminação algorítmica: (i) por erro estatístico: geralmente decorre de um erro cometido pelo responsável pelo desenho do algoritmo (e.g., utilização de dados incorretos ou de modelos estatísticos inadequados); (ii) por generalização: decorre da própria natureza de qualquer

[2] Por exemplo, se uma empresa usa um algoritmo de contratação treinado com dados históricos que favorecem homens, brancos, de meia-idade, o resultado provavelmente desfavorecerá mulheres, pessoas de cor e pessoas mais jovens ou mais velhas que seriam igualmente qualificadas para preencher a vaga.

emprego probabilístico (e.g., não refletir os *outliers*[3]); (iii) pelo uso de informações sensíveis: embora possa ser estatisticamente correta, baseia-se em dados legalmente protegidos; geralmente, para que seja considerado discriminatório, além de utilizar dado sensível, deve embasar-se em característica endógena ou que distingue um grupo historicamente discriminado[4] (e.g., características discriminatórias e estereotipadas clássicas como nacionalidade e identidade de gênero); (iv) limitadora do exercício de direitos: o problema é resultado da relação entre a informação utilizada pelo algoritmo e a concretização de um direito (e.g., na Alemanha, aqueles que acessavam sua informação de *score*, tinham sua pontuação reduzida).

1.3. Profiling

Cada indivíduo tem o direito a não ser "simplificado, objetivado, e avaliado fora de contexto" (ROSEN *apud* RODOTÁ, 2008, p. 12). Apesar disso, não raro, os gestores precisam tomar decisões num cenário de conhecimento e recursos limitados. Assim, utilizam-se de características observáveis como substitutas (*proxies*) de características não observáveis (MENDES e MATTIUZZO, 2019, p. 50).

O *profiling* (perfilamento, perfilação ou definição de perfis[5]) de indivíduos tem o potencial de criar sérios riscos na medida em que podem diminuir ou aumentar oportunidades sociais em aspectos relevantes da vida da pessoa conforme a categorização ou o *score* atribuído ao seu perfil (MENDES e FONSECA, 2021, p. 99). E isso ocorre não devido a algo que a pessoa efetivamente tenha feito, mas por causa das inferências ou correlações feitas por algoritmos "sugerindo" que ela pode vir a se comportar de maneira que a torna "arriscada" ou "inadequada", *e.g*., para concessão de crédito ou de seguro, para uma vaga de emprego, para admissão em escolas ou outras instituições (CITRON e PASQUALE, 2014, p. 24).

[3] *Outliers* são dados que se diferenciam de todos os demais, são os "pontos fora da curva", i.e., um valor que foge do que seria considerado padrão.

[4] "[...] é um dos tipos mais perversos de discriminação, ao reforçar o tratamento discriminatório e automatizá-lo, tornando mais difícil para os membros de tais agrupamentos superarem determinada situação prejudicial" (MENDES e MATTIUZZO, 2019, p. 54).

[5] Segundo o art. 4º(4) do RGPD, entende-se por " 'definição de perfis', qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações" (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

A situação pode ser agravada quando a formação de perfis se dá baseada em dados pessoais sensíveis, pela possibilidade maior de gerar discriminações:

> (...)seja porque dados pessoais, aparentemente não 'sensíveis', podem se tornar sensíveis se contribuem para a elaboração de um perfil; seja porque a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas (RODOTÁ, 2008, p. 84).

Nossa LGPD adota um conceito amplo de dado pessoal, assim como a matriz europeia, embasada na ideia de que "todo dado pessoal tem importância e valor" (VIOLA e TEFFÉ, 2021, p. 131). Mesmo dados que pareçam irrelevantes em determinadas circunstâncias, que não referenciem uma pessoa diretamente, quando tratados, organizados e cruzados, podem resultar em informação específica sobre um indivíduo, que pode ser, inclusive, de caráter sensível, como constatado pela Corte Constitucional Alemã no paradigmático julgamento sobre a Lei do Censo de 1983 (MENDES, 2018, p. 187-192). Neste mesmo sentido, o julgamento histórico no Brasil, de maio de 2020, em sede de controle de constitucionalidade no qual o Supremo Tribunal Federal (STF) reconheceu a proteção de dados pessoais como direito fundamental autônomo, baseado na lógica que não há dados "irrelevantes, neutros ou insignificantes", afirmando a proteção constitucional ao dado pessoal (MENDES, 2020; MENDES e FONSECA, 2020; RUARO e SARLET, 2021, p. 204).

1.4. LGPD: transparência, outros princípios e direitos

A transparência é um dos temas mais críticos e debatidos quando se fala em ADS. Pasquale (2015, p. 3) usa o termo "caixa preta" como metáfora para se referir a sistemas cujo funcionamento é misterioso, no qual é possível observar dados de entradas (*inputs*) e dados de saídas (*outputs*), mas entre uma e outra instância, não se sabe o que aconteceu. Com a crescente automatização de decisões, ainda que a palavra final seja dada por um humano, o processo decisório pode ter sido baseado em uma análise algorítmica, de maneira que nem mesmo o tomador da decisão conseguiria explicá-la. Neste sentido, vêm-se defendendo o direito ao devido processo informacional, relacionado à garantia de entender (receber uma explicação) e poder contestar decisões que afetem os interesses do titular de dados (BIONI e MARTINS, 2020b). O Ministro Gilmar Mendes, no julgamento da ADI 6.389 (Caso IBGE), reconheceu a importância dessa garantia "como corolário da dimensão subjetiva do direito à proteção de

dados pessoais [...] sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos preditivos e peremptórios" (BRASIL, 2020, p. 114).

A ideia por trás do "devido processo informacional" encontra analogia com o "devido processo legal": da mesma forma que uma pessoa não pode ser privada de sua vida, liberdade, propriedade, sem o devido processo legal, certos tipos de levantamentos, usos e disseminação de informação podem ser desafiados a fim de permitir que os titulares dos dados possam entender e se posicionar frente a decisões que tenham impacto em seus interesses (CITRON e PASQUALE, 2014, p. 19-20).

A falta de transparência é um ponto de atenção no que diz respeito à discriminação algorítmica por pelo menos três motivos: (i) pode impossibilitar evidenciar que algum tipo de discriminação ocorreu; (ii) pode dificultar a prevenção de discriminações; (iii) em vez de combater resultados discriminatórios, pode acabar por reforçá-los (MENDES e MATTIUZZO, 2019, p. 47).

A LGPD é uma lei principiológica, que prevê explicitamente o princípio da transparência (art. 6º, VI), que juntamente com o princípio do livre acesso (art. 6º, IV), dá origem ao direito de acess**o** aos dados pessoais (art. 18, II), este, por sua vez, é robustecido pelo art. 19; todos estes dispositivos juntos, permitem ao titular tomar conhecimento dos dados utilizados para decisão, bem como da forma e da duração do tratamento. A esse arcabouço, se agrega o princípio da qualidade dos dados (art. 6º, V), por meio do qual o titular pode demandar atualização e correção de dados incompletos, inexatos ou desatualizados (art. 18, III). Neste contexto, também importantes os direitos à oposição e exclusão (art. 18, VI), quando algum tratamento não devesse ser feito, ou algum dado específico não devesse ser considerado/utilizado. E, tão importante quanto os demais, o princípio da não-discriminação (art. 6º, IX), e.g., acionado caso o titular suponha estar sofrendo discriminação em razão de vieses.

De uma leitura sistemática da LGPD ter-se-ia a consubstanciação de outros dois direitos (MONTEIRO, 2018, p. 3): (i) direito à explicação: verdadeiro corolário do direito à transparência, diz respeito ao direito a receber informações úteis, suficientes, claras e compreensíveis, capazes de permitir ao titular entender a racionalidade e os critérios utilizados para o tratamento de seus dados pessoais para uma determinada finalidade; (ii) direito à revisão de decisões automatizadas: direito do titular requerer a revisão de uma decisão totalmente

automatizada que impacte seus interesses, produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente (art. 20, LGPD).

1.4.1. Art. 20 da LGPD

Conforme a redação constante do Parecer ao Projeto de Lei (PL) nº 4.060/2012, o art. 20 da LGPD determinava o direito de revisão como um direito de revisão humana, *i.e*., feito por uma pessoa natural (COMISSÃO ESPECIAL, 2018, p. 71). Contudo, a Lei nº 13.853/2019, que alterou a LGPD para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados (ANPD) (conversão da Medida Provisória nº 869/2018), além de alterar a redação do *caput* do art. 20 (excluindo da redação final a expressão "por pessoa natural"), vetou seu §3º, conforme Mensagem nº 288, de 8 de julho de 2019 (BRASIL, 2019c), que dispunha, igualmente, que a revisão de que trata o *caput* do artigo deveria ser realizada por pessoa natural (BRASIL, 2019b). Daí ter-se chegado à redação atual do art. 20 da LGPD (conforme constante do início deste trabalho).

Contudo, dois importantes pontos esperam por uma melhor definição (BIONI; MARTINS, 2020): (i) quais os parâmetros do direito de revisão, já que não há mais a previsão expressa da revisão humana na LGPD; (ii) o que de fato são decisões tomadas unicamente com base em tratamento automatizado, *i.e.*, no âmbito da discussão aqui empreendida, essencial estabelecer qual será a interpretação dada ao termo "unicamente": (ii.a) literal, o que praticamente esvaziará o direito de revisão ou; (ii.b) sistemática e ampliativa, na qual se dará abertura para efetiva aplicação do direito de revisão, considerando-se o grau de automatização dos processos decisórios, ainda que não totalmente automatizados. Entende-se que esta última seria uma interpretação possível e adequada, capaz de permitir ao cidadão, de maneira mais propícia, o exercício de seus direitos e garantias fundamentais.

Corrobora esse entendimento, discussão internacional acerca da temática de revisão de decisões automatizadas, como o posicionamento do *Information Commissioner's Office* (ICO) do Reino Unido, segundo o qual para descaracterizar uma decisão tomada unicamente com base em tratamento automatizado, o envolvimento humano deve ser ativo e não apenas um gesto simbólico, *i.e.*, se um humano revisa a decisão antes de ela ser aplicada e tem discricionariedade para alterá-la, e não simplesmente aplica a decisão tomada pelo sistema automatizado (ICO, 2021).

Segundo Juliana Sakai, em levantamento que buscou mapear a maneira como sistemas de decisão automatizada têm sido utilizados no âmbito do Poder Público (Projeto Transparência Algorítmica), todos os órgãos consultados informaram que ADS têm sido usados somente para dar suporte à tomada de decisão humana, e não eles mesmos como tomadores de decisão (SAKAI *et al.*, 2020; TRANSPARÊNCIA BRASIL, 2020, p. 19-21). Isso evidencia a disputa entre três eixos: (i) o conceito de "decisão unicamente automatizada"; (ii) a prática corrente no uso de sistemas de decisão; e (iii) a viabilização do exercício de direito de revisão. Ou seja, para dar alguma efetividade ao art. 20 da LGPD, sua interpretação necessariamente deveria ser ampliativa.

Diante do exposto, entende-se que a LGPD garante (MONTEIRO, 2018, p. 14):

1. Acesso aos tipos de dados pessoais e aos dados propriamente ditos usados como entrada do sistema responsável pelo processo de decisão automatizada;
2. Se o processo automatizado tiver por finalidade formar um perfil comportamental, ou se utilizar de um perfil comportamental para tomada de decisão, o direito de acesso aos dados poderá incluir, os dados anonimizados utilizados para enriquecer tais perfis (art. 12, §2º, LGPD);
3. O direito de receber explicações claras acerca dos critérios utilizados para tomar a decisão automatizada, observados os segredos comercial e industrial (art. 20, §1º, LGPD), que devem ser analisados no caso concreto, pois estes conceitos não se encontram definidos na LGPD (vide Seção 1.4.2);
4. A possibilidade de auditoria pela ANPD para verificação de aspectos discriminatórios (art. 20, §2º, LGPD).
5. O direito de requerer revisão (que se entende deva ser promovida por pessoa natural, em consonância com os debates doutrinários nacionais e internacionais a respeito do assunto, apesar de não garantida pela legislação brasileira atual), caso a decisão automatizada tenha consequências nos interesses do titular, o que se presumiria, no caso de perfis.

Por fim, independentemente do direito à revisão de decisões automatizadas, em havendo dano em razão do tratamento de dados pessoais, surge a obrigação de reparação. Quanto a isso, cumpre mencionar a Seção III do Capítulo VI, da LGPD, que trata "Da Responsabilidade e do Ressarcimento de Danos", em especial o *caput* do art. 42, que dispõe que o "controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a

outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (BRASIL, 2019a).

1.4.2. Segredo comercial e industrial

Apesar de poder-se ocultar a lógica do processamento com base no segredo, o direito à revisão pode ser articulado ao acesso à informação analisada para se chegar à categorização/pontuação, permitindo ao titular promover a correção e/ou atualização dos dados que levaram à definição do perfil, o que lhe possibilitaria obter classificação eventualmente mais vantajosa.

Diante disso, importa destacar que a ideia de explicabilidade quando aplicada ao processo decisório, geralmente se refere às "razões ou justificativas para aquele resultado em particular, e não a uma descrição do processo decisório em geral" (DOSHI-VELEZ e KORTZ, 2017)

Destarte, existem alguns mecanismos indiretos que permitem analisar se decisões automatizadas estão sendo tomadas de forma justa, com respeito aos princípios legais, sem a quebra do segredo de negócio: (i) informação sobre os tipos de dados usados para alimentar a base de dados; (ii) quais decisões são realmente tomadas por ADS; (iii) como tais decisões podem afetar direitos fundamentais; (iv) quais populações são afetadas pela decisão automatizada; (v) quais testes foram feitos com o ADS para evitar discriminações (BIONI; MARTINS, 2020).

1.4.3. Evolução do direito à revisão no Brasil

No Brasil, o direito à revisão de decisões automatizadas evoluiu de uma proteção setorial para uma geral.

A Lei nº 8.978/1990 (Código de Defesa do Consumidor, CDC) enuncia o direito à transparência associada ao dever de informação derivado da boa-fé objetiva (art. 4º, *caput*; art. 4º, III; art. 6º, III; art. 8º, todos do CDC). Assim, caso tenha havido uma decisão automatizada numa relação de consumo, o consumidor tem direito a conhecer os dados utilizados na tomada de decisão.

Com base no direito à transparência e à não-discriminação, a Lei nº 12.414/2011 (Lei do Cadastro Positivo) já previa o direito à explicação e à revisão de decisões automatizadas, no

microssistema do setor de crédito (art. 5º, IV a VII, Lei do Cadastro Positivo), formando o arcabouço de tais direitos nas relações de consumo (MONTEIRO, 2018, p. 8). Além disso, a Lei do Cadastro Positivo buscou limitar os tipos de dados que poderiam ser utilizados para o *credit scoring*, proibindo a utilização de informações "que não estiverem vinculadas à análise de risco de crédito e aquelas relacionadas à origem social e étnica, à saúde, à informação genética, ao sexo e às convicções políticas, religiosas e filosóficas" (art. 7º, I) *i.e.*, dados pessoais sensíveis na atual inteligência da LGPD (art. 5º, II).

Contudo, o CDC e a Lei do Cadastro Positivo formam um microssistema de proteção de dados pessoais, restrito, malogradamente, à concessão de crédito (MONTEIRO, 2018, p. 8).

Neste sentido, a LGPD a veio para dar uma abrangência maior ao direito à revisão, não só quanto ao universo de sua incidência (qualquer decisão tomada unicamente com base em tratamento automatizado de dados pessoais que afetem os interesses do titular, incluída a concessão de crédito, mas agora não só limitada a ela), mas quanto ao momento anterior de seu exercício, incluindo "as decisões destinadas a definir o [...] perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade" (art. 20, *caput*), assegurando um compromisso maior com a transparência da trilha decisória percorrida para se chegar à deliberação final.

1.5. Art. 22 do RGPD

O art. 22 do RGPD tem as suas raízes nos art. 12(a) e art. 15 da Diretiva de Proteção de Dados 95/46/CE[6]. Uma das principais diferenças é que o RGPD tem um escopo de aplicação mais amplo, pois incide no "processamento automatizado, incluindo criação de perfil", enquanto a legislação anterior dispunha só ser aplicável se uma forma de criação de perfil estivesse envolvida. Além disso, o art. 22(4), do RGPD, aborda explicitamente a utilização de dados sensíveis, estabelecendo uma proibição qualificada de decisões baseadas nas categorias de dados enumeradas no art. 9º(1), do RGPD (que trata exatamente de dados sensíveis).

As "Diretrizes sobre tomada de decisão individual automatizada e criação de perfil" (WP 251 ver.01) do *Article 29 Data Protection Working Party* (WP29), recepcionadas pelo *European Data Protection Board* (EDPB), apontam que o art. 22(1) do RGPD pode ser

[6] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, "relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados", foi revogada em 2018 pelo RGPD.

enquadrado como uma proibição geral de "decisões individuais automatizadas, incluindo definição de perfis". Nesse sentido, afirma que (WP29, 2018, p. 19):

> O termo "direito" na disposição não significa que o art. 22(1), se aplica apenas quando ativamente invocado pelo titular dos dados. O art. 22(1) estabelece uma proibição geral para a tomada de decisões baseada exclusivamente no processamento automatizado. Esta proibição aplica-se quer o titular dos dados tome ou não medidas em relação ao tratamento dos seus dados pessoais (livre tradução).

Tal interpretação é embasada tanto nos princípios do RGPD, quanto no objetivo de dar aos titulares o controle sobre seus dados pessoais (autodeterminação informativa), que pauta o Regulamento como um todo. Além disso, o WP29 faz referência ao Considerando 71 do RGPD, o que implica que o Regulamento não impede a utilização de ADS ou a definição de perfis, contanto que o processamento atenda à definição do art. 22(1), caso em que será necessário garantir que se está coberto por ao menos uma das exceções constantes do art. 22(2).

O primeiro elemento capaz de acionar o art. 22 do RGPD é a presença de uma "decisão", que pode ser interpretada em sentido amplo, e.g., atos oficiais de autoridades públicas, como decisões sobre declarações de impostos (BRKAN, 2019, p. 102); recusas automáticas de pedidos de crédito *online* ou decisões semelhantes no contexto de práticas de recrutamento eletrônico. Em um sentido mais geral, as decisões também podem ser vistas como uma atitude ou posição particular tomada em relação a uma pessoa, se essa posição tiver, pelo menos, probabilidade de ser posta em prática (MENDOZA e BYGRAVE, 2017, p. 10-11).

Outro elemento de atenção é a palavra "exclusivamente" na expressão "decisão tomada exclusivamente com base no tratamento automatizado". Sua avaliação depende se a intervenção humana é possível de uma perspectiva técnica ou se o processo de tomada de decisão é construído de forma exclusivamente algorítmica, sem espaço para o envolvimento humano.

Se o processo permitir tecnicamente a intervenção humana, então deve-se avaliar se a ação realizada por pessoa natural é "significativa" ou apenas um "gesto simbólico" procedimental (WP29, 2018, p. 21). Para cumprir este critério, a intervenção deve ser "realizada por quem tenha autoridade e competência para alterar a decisão". Além disso, o ser humano envolvido não deve apenas ter o poder de mudar a decisão, mas realmente exercer essa

competência "considerando todos os dados relevantes" e verificando a substância e a exatidão da decisão gerada pela máquina (WP29, 2018, p. 8).

A decisão deve "produzir efeitos jurídicos" sobre o titular dos dados o que ocorre quando ela é vinculativa e afeta os direitos ou interesses jurídicos da pessoa, *e.g.*, o cancelamento de um contrato, a decisão de uma autoridade tributária sobre a declaração de imposto de renda de um indivíduo ou a recusa de um benefício social concedido por lei. Ou pode "afetar significativamente o titular dos dados de forma similar" (à produção de efeitos jurídicos). Em princípio, satisfazer este critério significa que os impactos da decisão devem ser suficientemente grandes, apesar de não alterar a posição jurídica do indivíduo. Alguns critérios para efeitos significativos incluem: (i) afetar significativamente as circunstâncias, comportamento ou escolhas dos indivíduos em questão; (ii) ter um impacto prolongado ou permanente no titular dos dados; ou (iii) no seu extremo, levar à exclusão ou discriminação de indivíduos (WP29, 2018, p. 21).

O art. 22(3), do RGPD estabelece uma lista não exaustiva de salvaguardas aos titulares dos dados, ainda que não esteja claro como estas salvaguardas serão operacionalizadas e qual seu efeito prático, *e.g.*, como seria a intervenção humana na prática, quando o site ou a plataforma tecnicamente não o permitir; caso o titular dos dados, apresente seus pontos de vista ou conteste uma decisão, isso conduzirá a sua anulação? (BRKAN, 2019, p. 108).

Por fim, o art. 22(4) traz uma proibição qualificada quanto ao uso de dados sensíveis.

2. Estudos de Caso

2.1. Brasil – Resp 1.419.697/RS (*score crediting*)

Apenas recentemente a LGPD entrou totalmente em vigor (à exceção das sanções – art. 52 a 54 –, que só vigoraram em agosto de 2021, o restante da Lei teve sua vigência a partir de setembro de 2020), seus detalhes e adequações devem ser promovidos pela ANPD, pelo Legislativo e pelo Judiciário, ao longo do tempo. Em que pese o Judiciário ter sido progressivamente mais mobilizado para definir os alcances e limites da LGPD, não se tem ciência, até o momento, de caso acionando a incidência do art. 20. Neste sentido, será trazida à discussão caso anterior à vigência da LGPD, mas que trata da temática, ainda que no microssistema da concessão crédito (do sistema de *score crediting*).

O *credit scoring* é um método de avaliação do risco de concessão de crédito com base em modelos estatísticos[7], *i.e.*, uma análise para determinar se o "perfil" do tomador da dívida é ou não o de um "bom pagador". Em tal análise são observados diversos dados (*e.g.*, idade, profissão, estado civil, endereço, renda, raça, gênero, informações cadastrais como protestos, cheques sem fundo, pendências financeiras e bancárias, ações judiciais, participação societária etc.), alguns deles irrelevantes para aquela decisão específica, inclusive com potencial de representar correlações[8] que reproduzem preconceitos estruturais.

O julgamento do Recurso Especial (REsp) 1.419.697/RS, de relatoria do Ministro Paulo de Tarso Sanseverino, julgado na Segunda Seção do Superior Tribunal de Justiça (STJ) serviu de paradigma para controvérsia tratada pelo Tema 710, "acerca da natureza dos sistemas de *scoring* e a possibilidade de violação a princípios e regras do Código de Defesa do Consumidor capaz de gerar indenização por dano moral", no qual ficou firmada a tese que (BRASIL, 2014, grifos nossos):

> I - O sistema "**credit scoring**" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de **modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado** (nota do risco de crédito). [...] III - Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da **tutela da privacidade e da máxima transparência nas relações negociais**, conforme previsão do CDC e da Lei n. 12.414/2011. IV - Apesar de **desnecessário o consentimento do consumidor consultado**, devem ser a ele **fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas**. V - O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), **pode ensejar a responsabilidade objetiva e solidária** do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de **utilização de informações excessivas ou sensíveis** (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de **comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados**.

[7] Como visto na Seção 1.1, a simples aplicação de cálculos estatísticos já seria suficiente para caracterizar o emprego de um ADS.
[8] Cumpre lembrar uma das regras de ouro da estatística que enuncia que "correlação não é igual a causalidade".

Também como resultado do julgamento, foi enunciada a Súmula nº 550/STJ que dispõe que "[a] utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, **que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo**" (BRASIL, 2015, grifos nossos).

Segundo o relator, já se tinha à época um: (i) direito de acesso do consumidor às informações existentes sobre ele em cadastros e bancos de dados, além das respectivas fontes; (ii) dever de clareza dos arquivos; (iii) direito de retificação de informações incorretas; (iv) fixação de uma vida útil para essas informações (cinco anos). O que poderia ser sintetizado em cinco deveres a serem cumpridos pelo fornecedor do serviço: (a) dever de veracidade; (b) dever de clareza; (c) dever de objetividade; (d) vedação de informações excessivas; (e) vedação de informações sensíveis (a fim de evitar a utilização discriminatória da informação) (BRASIL, 2014, p. 34-36).

Ao decidir sobre o *credit scoring*, o STJ afirmou indiretamente o direito à revisão, ao aplicar direitos básicos do CDC, como o "dever de informação" e a "transparência". Além disso, o STJ levou em consideração os princípios da "necessidade" e da "não-discriminação" ao balizar os dados que poderiam ser usados para fins de score de crédito (BRASIL, 2014, p. 39, grifo do original):

> Não podem ser valoradas pelo fornecedor do serviço de "*credit scoring*" **informações sensíveis**, como as relativas à cor, à opção sexual ou à orientação religiosa do consumidor avaliado, **ou excessivas**, como as referentes a gostos pessoais, clube de futebol de que é torcedor etc.

Esta decisão firma o entendimento que para fins de análise de concessão de crédito (princípio da finalidade) está vedada a utilização de quaisquer informações de natureza personalíssima, não relacionada à finalidade esperada com a análise de crédito (princípio da não discriminação) (MULHOLLAND, 2018, p. 166)

A decisão afirmou ainda que, apesar da "metodologia em si de cálculo da nota de risco de crédito [...] constitui[r] segredo da atividade empresarial, cujas fórmulas matemáticas e modelos estatísticos naturalmente não precisam ser divulgadas" (BRASIL, 2014, p. 37), essas informações, quando solicitadas, devem ser prestadas ao consumidor avaliado, com a indicação clara e precisa dos bancos de dados utilizados possibilitando o exercício do controle da

veracidade dos dados, inclusive para poder retificá-los ou melhorar a sua performance. Ademais, devem ser prestadas também as informações pessoais do consumidor que foram consideradas para que ele possa exercer o direito de controle quanto às informações excessivas ou sensíveis (BRASIL, 2014, p. 38).

A importância desse julgamento está em consagrar princípio e deveres para com o titular dos dados (*e.g.*, transparência, livre acesso, não-discriminação, explicação, revisão de decisões), os quais foram robustecidos e ampliados pela LGPD, criando mecanismos que permitem coibir, mitigar ou ao menos lidar com problemas relacionados à tomada de decisão com base em tratamento automatizado.

2.2. Europa – Caso C/13/696010-HA ZA 21-81 (Uber-Amsterdã) e Caso 2020-0.436.002 (score - Áustria)

Em fevereiro de 2021, no Caso C/13/696010-HA ZA 21-81, o *Rechtbank Amsterdam* (Tribunal Distrital de Amsterdã) condenou a Uber, à revelia, a reintegrar 6 motoristas por entender que a decisão de demissão foi baseada exclusivamente em processamento automatizado, com consequências jurídicas para os requerentes, afetando-os significativamente, nos termos do art. 22(1) do RGPD (RB AMSTERDAM, 2021a, §3.1). A sentença determinou também à Uber pagamento de multa de 5 mil euros por dia de não cumprimento da ordem, bem como mais de 100 mil euros por danos. A Uber agora está fazendo um pedido para que a sentença à revelia seja julgada improcedente e seu caso seja ouvido (BUTLER, 2021).

Essa foi a primeira vez que um tribunal ordenou a anulação de uma decisão automatizada de demitir trabalhadores do emprego (RB AMSTERDAM, 2021b), daí sua importância. Sem embargo, tendo em vista que o julgamento ocorreu à revelia da ré, não há muitos elementos de disputa/discussão, motivo pelo qual apresenta-se adicionalmente outro caso à luz do RGPD, que, apesar de não decidir pela incidência explícita do art. 22 do RGPD, faz uma série de afirmações importantes acerca de direitos aqui tratados.

No Caso 2020-0.436.002, apresentado junto à *Datenschutzbehörde* (DSB), Autoridade de Proteção de Dados Austríaca, a ré teria calculado um *marketing score* chamado "Dominanten Geo Milieus" em relação ao autor (DSB, 2020). Esse *score* consistiria em supostas

probabilidades (expressas em um número percentual)[9] de que o autor pertenceria a um determinado grupo dentre "conservadores", "tradicionalistas", "hedonistas" ou "individualistas digitais". Em maio de 2019, o autor enviou à ré uma solicitação de acesso sobre como o *score* foi calculado, com base no art. 15(1)(h) do RGPD. Em junho de 2019, a ré recusou-se a fornecer a informação por entender que se qualificava como segredo comercial. Diante disso, o autor apresentou uma queixa junto à DSB.

Em 2020, quando decidiu o caso, a DSB inicialmente considerou que o *score* em questão constitui dado pessoal nos termos do art. 4(1) do RGPD, uma vez que foi atribuído a pessoas singulares. Além disso, considerou que as atividades de processamento que conduzem à criação desse *score* constituem perfis, conforme art. 4(4) do RGPD. Tendo em vista o Considerando 71 do RGPD e as diretrizes constantes do WP 251 rev.01, a DSB enfatizou que o RGPD diferencia entre a criação de perfis nos termos do art. 4(4) e a tomada de decisão automatizada nos termos do art. 22: para uma atividade de processamento ser qualificada como criação de perfis, não é necessário que esta atividade seja realizada exclusivamente de maneira automatizada.

Em seguida, o DSB avaliou se o reclamante tinha direito à informação nos termos do art. 15(1)(h) do RGPD em relação ao *score* e se a ré havia infringido esse direito. De acordo com a DSB, o direito ao abrigo do art.15(1)(h) do RGPD não se limita aos casos de tomada de decisão automatizada do art. 22(1) e (4) do RGPD, mas também abrange outros casos, como o perfil em questão: a utilização da expressão "pelo menos nesses casos", no art. 15(1)(h), aponta para um âmbito amplo de aplicação. Consequentemente, a DSB não viu necessidade de avaliar mais se o *score* também se qualificava como tomada de decisão automatizada de acordo com o art. 22 do RGPD.

Por último, a DSB entendeu que a ré não é obrigada a divulgar o algoritmo, código-fonte ou código compilado que foi usado ao criar o *score*. Em vez disso, deve fornecer as seguintes informações conexas ao cálculo da pontuação: (i) parâmetros/variáveis de entrada e como eles surgiram (*e.g.*, usando informações estatísticas); (ii) efeito dos parâmetros/variáveis de entrada na pontuação; (iii) explicação do motivo pelo qual ao titular dos dados foi atribuído um determinado resultado de avaliação; (iv) lista de possíveis categorias de perfil; ou (v)

[9] Em que pese, como será visto adiante, a análise da questão pela DSB ter prescindido de decidir se a atividade foi realizada exclusivamente de maneira automatizada, como visto na Seção 1.1, entende-se que a aplicação de cálculos de probabilidade e estatística já caracterizaria o emprego de um ADS (apesar de isso não significar que alguma decisão tenha sido tomada de maneira exclusivamente automatizada).

informações equivalentes que permitam ao titular dos dados exercer os seus direitos de retificação e eliminação, bem como examinar a legalidade do processamento.

Igualmente, a importância desse julgamento consiste na consolidação de princípios e deveres para com o titular dos dados relacionados à transparência, ao livre acesso, à explicação de decisões tomadas com base no tratamento de dados pessoais capazes de enquadrar o titular em perfis e com isso afetá-lo. Mas mais do que isso, estabelece que estes são parâmetros mínimos de proteção, prescindindo, inclusive, da verificação se a decisão foi ou não automatizada (o que atrairia a incidência de prerrogativas adicionais, como a de "obter intervenção humana por parte do responsável").

Considerações finais

A LGPD é uma lei principiológica, da qual derivam (implícita e explicitamente) diversos direitos, um deles diz respeito ao direito à revisão de decisões automatizadas, previsto no art. 20. Este direito se reveste de especial importância diante de problemas relacionados à utilização de ADS, tais como a falta de transparência, dificuldade de identificar e corrigir erros, reforço de desigualdades (vieses).

Na Europa, esse direito é tratado, principalmente, pelo art. 22 do RGPD. Ambos normativos apresentam diversas similaridades (o que é natural, tendo em vista que o RGPD serviu de inspiração para a LGPD). Entretanto, há certas distinções importantes: (i) o RGPD impõe algumas restrições não presentes na LGPD: (i.a) não inclui o caso dos dados anonimizados (previstos no art. 12, §2º, LGPD); (i.b) limita o direito de oposição quando a base legal para tratamento dos dados for o consentimento explícito ou a execução de um contrato (art. 22(2), RGPD); (ii) mas, o RGPD prevê explicitamente a intervenção humana (art. 22(3), RGPD), enquanto da LGPD não consta tal previsão.

De qualquer forma, no Brasil ou na Europa, percebe-se que definir os contornos, limites e conferir efetividade ao direito à revisão automatizada será papel das Autoridades de Proteção de Dados, da doutrina e da jurisprudência.

Referências bibliográficas

ACLU, American Civil Liberties Union; CENTER FOR DEMOCRACY & TECHNOLOGY; ELECTRONIC FRONTIER FOUNDATION; NEW

AMERICA'S OPEN TECHNOLOGY INSTITUTE; RAICU, Irina; SUZOR, Nicolas; WEST, Sarah Myers; ROBERTS, Sarah T. Santa Clara Principles on transparency and accountability in content moderation. 7 mai. 2018. Disponível em: https://santaclaraprinciples.org/. Acesso em: 28 ago. 2021.

AUTOMATED ASSISTANCE IN ADMINISTRATIVE DECISION-MAKING WORKING GROUP. Automated Assistance in Administrative Decision-Making Better Practice Guide. Canberra: Australian Government, 2007.

BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. California Law Review, v. 104, n. 3, p. 671-732, jun. 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899.#. Acesso em: 30 ago. 2021.

BIONI, Bruno; MARTINS, Pedro. Devido processo informacional: um salto teórico-dogmático necessário? . 2020a. Disponível em: https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F108127%2F1599509820Ensaio_Devido_Processo_Informacional_-_V2.pdf. Acesso em: 10 jun. 2021.

BIONI, Bruno; MARTINS, Pedro. O que você precisa ler para entender sobre o devido processo informacional. Data Privacy Brasil, 2020b. Disponível em: https://conteudo.dataprivacy.com.br/devido-processo-informacional. Acesso em: 29 jun. 2021.

BIONI, Bruno; MARTINS, Pedro. Série LGPD em Movimento: LGPD e Decisões Automatizadas. 14 dez. 2020c. Disponível em: https://www.observatorioprivacidade.com.br/2020/12/14/serie-lgpd-em-movimento-lgpd-e-decisoes-automatizadas/. Acesso em: 29 jun. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). 2019a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 jun. 2021.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. (Conversão da Medida Provisória nº 869, de 2018). 2019b. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 22 jun. 2021.

BRASIL, Presidência da República. Mensagem nº 288, de 8 de julho de 2019. Comunica veto parcial ao Projeto de Lei de Conversão nº 7, de 2019 (MP nº 869/2018), que "Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências". 2019c. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-288.htm. Acesso em: 22 jun. 2021.

BRASIL, Superior Tribunal de Justiça (Segunda Seção). Resp nº 1.419.697/RS. Relator: Min. Paulo de Tarso Sanseverino, julgado em 12/11/2014, DJe 17/11/2014. . 2014. Disponível em: https://bdjur.stj.jus.br/jspui/bitstream/2011/114173/REsp1419697.pdf. Acesso em: 10 jun. 2021.

BRASIL, Superior Tribunal de Justiça (Segunda Seção). Súmula nº 550. 2015. Disponível em: https://scon.stj.jus.br/SCON/sumanot/toc.jsp?livre=(sumula%20adj1%20%20550).sub. Acesso em: 15 ago. 2021.

BRASIL, Supremo Tribunal Federal (Plenário). *R*eferendo na Medida Cautelar na Ação Direta de inconstitucionalidade (ADI) nº 6.389/DF. Ementa medida cautelar em ação direta de inconstitucionalidade. Referendo. Medida provisória nº 954/2020. Emergência de saúde pública de importância internacional decorrente do

novo coronavírus (covid-19). Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o instituto brasileiro de geografia e estatística. Fumus boni juris. Periculum in mora. Deferimento. Relatora: Min. Rosa Weber, julgado em 07/05/2020, processo eletrônico dje-270, divulg 11-11-2020, public 12-11-2020. 12 nov. 2020. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344950131&ext=.pdf. Acesso em: 29 jun. 2021.

BRENNAN, Tim; DIETERICH, William; EHRET, Beate. Evaluating the Predictive Validity of the Compas Risk and Needs Assessment System. Criminal Justice and Behavior, v. 36, n. 1, p. 21-40, 2009. Disponível em: https://doi.org/10.1177/0093854808326545. Acesso em: 30 ago. 2021.

BRKAN, Maja. Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. International Journal of Law and Information Technology, v. 27, n. 2, p. 91–121, Summer 2019. Disponível em: https://doi.org/10.1093/ijlit/eay017. Acesso em: 1 set. 2021.

BUTLER, Sarah. Court tells Uber to reinstate five UK drivers sacked by automated process. The Guardian, 14 abr. 2021. Disponível em: https://www.theguardian.com/technology/2021/apr/14/court-tells-uber-to-reinstate-five-uk-drivers-sacked-by-automated-process. Acesso em: 1 set. 2021.

CITRON, Danielle Keats; PASQUALE, Frank A. The Scored Society: Due Process for Automated Predictions. Washington Law Review, v. 89, p. 1-31, 2014. Disponível em: https://ssrn.com/abstract=2376209. Acesso em: 29 jun. 2021.

COHEN, Julie E. Examined Lives: Informational Privacy and the Subject as Object. Stan. L. Rev., v. 52, p. 1373-1438, 2000. Disponível em: https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1819&context=facpub. Acesso em: 7 set. 2021.

COMISSÃO ESPECIAL, destinada a proferir parecer ao Projeto de Lei nº 4.060, de 2012. Parecer ao Projeto de Lei nº 4.060, de 2012 (Tratamento e Proteção de Dados Pessoais) (Apenso PLs nº 5.276/16 e 6.291/16). Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Autor: Deputado Milto Monti. Relator: Deputado Orlando Silva., 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305

http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1664206. Acesso em: 22 jun. 2021.

COURT hearing in lawsuit against System Risk Indication (SyRI). Privacy First, 2019. Disponível em: https://www.privacyfirst.eu/court-cases/680-court-hearing-in-lawsuit-against-system-risk-indication-syri.html. Acesso em: 22 ago. 2021.

DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. Reuters, 10 out. 2018. Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G . Acesso em: 30 ago. 2021.

DOSHI-VELEZ, Finale; KORTZ, Mason A. Accountability of AI Under the Law: The Role of Explanation. Berkman Klein Center Working Group on Explanation and the Law, Berkman Klein Center for Internet & Society working paper, p. 1-15, 2017. Disponível em: http://nrs.harvard.edu/urn-3:HUL.InstRepos:34372584. Acesso em: 30 ago. 2021.

DSB, Datenschutzbehörde. (Austria) - GZ: 2020-0.436.002 of September 8, 2020 (case number: DSB-D124.909). Machine translation of the German original. European Case Law Identifier (ECLI)

ECLI:AT:DSB:2020:2020.0.436.002. GDPRHub, 8 set. 2020. Disponível em: https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2020-0.436.002. Acesso em: 1 set. 2021.

FTC, Federal Trade Commission. Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003. dez. 2012. Disponível em: https://www.ftc.gov/sites/default/files/documents/reports/section-319-fair-and-accurate-credit-transactions-act-2003-fifth-interim-federal-trade-commission/130211factareport.pdf. Acesso em: 30 ago. 2021.

GEE, Kelsey. In Unilever's Radical Hiring Experiment, Resumes Are Out, Algorithms Are In. The Wall Street Journal, 26 jun. 2017. Disponível em: https://www.wsj.com/articles/in-unilevers-radical-hiring-experiment-resumes-are-out-algorithms-are-in-1498478400. Acesso em: 30 ago. 2021.

HARRIS, John. The tyranny of algorithms is part of our lives: soon they could rate everything we do. The Guardian, Opinion, Big Data, 5 mar. 2018. Disponível em: https://www.theguardian.com/commentisfree/2018/mar/05/algorithms-rate-credit-scores-finances-data. Acesso em: 28 jun. 2021.

ICO, Information Comissioner's Office. In the picture: A data protection code of practice for surveillance cameras and personal. Version 1.2. London: ICO, Information Comissioner's Office, 2017. Disponível em: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf. Acesso em: 13 jul. 2021.

ICO, Information Comissioner's Office. What does the UK GDPR say about automated decision-making and profiling?, 2021. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/. Acesso em: 9 set. 2021.

LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren; ANGWIN, Julia. How We Analyzed the COMPAS Recidivism Algorithm. ProPublica, 23 mai. 2016. Disponível em: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. Acesso em: 28 jun. 2021.

MARQUES, Claudia Lima; MUCELIN, Guilherme. Novo Mercado de Consumo 'Simbiótico' e a Necessidade de Proteção de Dados dos Consumidores. In: SARLET, G. B. S.;TRINDADE, M. G. N., et al (Ed.). Proteção de dados: temas controvertidos. Indaiatuba: Foco, 2021. p.133-183.

McGREGOR, Lorna; MURRAY, Daragh; NG, Vivian. International Human Rights Law as a Framework for Algorithmic Accountability. International & Comparative Law Quarterly, v. 68, n. 2, p. 309 - 343 2019. Disponível em: https://doi.org/10.1017/S0020589319000046. Acesso em: 29 jun. 2021.

MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. Revista de Direito do Consumidor, v. 102, p. 19-43, nov./dez. 2015.

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. Jota, 10 mai. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em: 22 jun. 2021.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais e Justiça*, v. 12, n. 39, p. 185-216, jul./dez. 2018.

MENDES, Laura Schertel; FONSECA, Gabriel ampos Soares da. Proteção de dados

para além do consentimento: tendências de materialização. (cap. 4). In: DONEDA, D.;SARLET, I. W., et al (Ed.). Tratado de Proteção de Dados. Rio de Janeiro: Forense, 2021.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados. Revista de Direito do Consumidor, v. 130, p. 471-478, jul./ago. 2020.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. RDU, v. 16, n. 90, p. 39-64, nov.-dez. 2019.

MENDOZA, Isak; BYGRAVE, Lee A. The Right Not to Be Subject to Automated Decisions Based on Profiling. University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855. Acesso em: 1 set. 2021.

MOLNAR, Petra; GILL, Lex. Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System. International Human Rights Program, Faculty of Law, University of Toronto and the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, 2018.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? Instituto Igarapé - Artigo Estratégico, v. 39, dez. 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. Acesso em: 29 jun. 2021.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (lei 13.709/18). R. Dir. Gar. Fund, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: http://dx.doi.org/10.18759/rdgf.v19i3.1603. Acesso em: 15 ago. 2021.

NIKLAS, Jędrzej; SZTANDAR-SZTANDERSKA, Karolina; SZYMIELEWICZ, Katarzyna. Profiling the unemployed in Poland: social and political implications of algorithmic decision making. Warsaw: Fundacja Panoptykon, 2015. Disponível em: https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf. Acesso em: 29 jun. 2021.

O'NEIL, Cathy. Weapons of math destruction: how big data increases inequality and threatens democracy. 1 ed. New York: Crown, 2016.

PARLAMENTO EUROPEU. Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial nº L 281 de 23/11/1995 p. 0031 - 0050. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. Acesso em: 1 ago. 2021.

PARLAMENTO EUROPEU; CONSELHO EUROPEU. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE . EUR-Lex, Access to European Union Law, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 10 jul. 2021.

PASQUALE, Frank. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge (Massachusetts), London: Harvard University Press, 2015.

RB AMSTERDAM, Rechtbank Amsterdam [District Court of Amsterdam]. C/13/696010 / HA ZA 21-81. European Case Law Identifier: ECLI:NL:RBAMS:2021:1415. GDPRHub, 24 fev. 2021a. Disponível em: https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/696010_/_HA_ZA_21-81. Acesso em: 1 set. 2021.

RB AMSTERDAM, Rechtbank Amsterdam [District Court of Amsterdam]. C/13/696010 / HA ZA 21-81. European Case Law Identifier: ECLI:NL:RBAMS:2021:1415. Rechtspraak, 24 fev. 2021b. Disponível em: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1415&showbutton=true&keyword=ECLI%3ANL%3ARBAMS%3A2021%3A1415. Acesso em: 1 set. 2021.

RODOTÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden; SARLET, Gabriele Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) - Lei 13. 709/2018. In: DONEDA, D.;SARLET, I. W., et al (Ed.). Tratado de Proteção de Dados. Rio de Janeiro: Forense, 2021.

SAKAI, Juliana; BUTALLA, Vanessa; ROBERTO, Enrico; BIONI, Bruno; MARTINS, Pedro. LGPD e decisões automatizadas. [1h53min26seg]. Data Privacy Brasil, LGPD em Movimento, 3 dez. 2020. Disponível em: https://www.youtube.com/watch?v=SNg8N7eCU6k. Acesso em: 17 jul. 2021.

TRANSPARÊNCIA BRASIL. Recomendações de governança: uso de inteligência artificial pelo poder público. fev. 2020. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_IA_PoderPublico.pdf. Acesso em: 28 ago. 2021.

VAN EIJK, Gwen Socioeconomic marginality in sentencing: The built-in bias in risk assessment tools and the reproduction of social inequality. Punishment & Society, v. 19, n. 4, p. 463-481, 2017. Disponível em: https://doi.org/10.1177/1462474516666282. Acesso em: 30 ago. 2021.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.º e 11. In: DONEDA, D.;SARLET, I. W., et al (Ed.). Tratado de Proteção de Dados. Rio de Janeiro: Forense, 2021.

WP29, Article 29 Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. WP251rev.01. 6 fev. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/redirection/document/49826. Acesso em: 15 ago. 2021.

OBRIGAÇÕES DOS AGENTES DE TRATAMENTO DE DADOS: INTERFACES ENTRE A REGULAÇÃO BRASILEIRA E EUROPEIA

Sofia de Medeiros Vergara[1]

Dispositivo LGPD	Dispositivo RGPD
Art. 5º (definições dos agentes de tratamento); **Art. 42 (responsabilidade dos agentes de tratamento);** **Art. 6º** As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – finalidade; II – adequação; III - necessidade; IV - livre acesso; V - qualidade dos dados; VI - transparência; VII - segurança; VIII - prevenção; IX - não discriminação; X - responsabilização e prestação de contas. **Art. 7º (hipóteses de tratamento de dados pessoais);** **Art. 14. (O tratamento de dados pessoais de crianças e de adolescentes).** **Art. 20, § 1º** O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. **Art. 37.** O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. **Art. 39.** O operador deverá realizar o tratamento segundo as instruções fornecidas	**Art. 4 (7)** «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro; **Art. 4 (8)** «Subcontratante», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes **Art. 26 (1)** Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento. Estes determinam, por acordo entre si e de modo transparente as respetivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respetivos deveres de fornecer as informações referidas nos artigos 13.º e 14.º, a menos e na medida em que as suas responsabilidades respetivas sejam determinadas pelo direito da União ou do Estado-Membro a que se estejam sujeitos. O acordo pode designar um ponto de contacto para os titulares dos dados. **Art. 5 (Princípios relativos ao tratamento de dados pessoais);** **Art. 6 (Licitude do tratamento);** **Art. 7 (condições aplicáveis ao consentimento);** **Art. 12 (1)** O responsável pelo tratamento toma as

[1] Graduanda em Direito na Faculdade de Direito da Universidade de Brasília (UnB); Editora-Assistente na Revista dos Estudantes de Direito da UnB; membra do Grupo de estudos em Empresarial e Arbitragem da UnB (GEA), membra do Grupo de Estudos sobre Constituição, Empresa e Mercado da UnB (GECEM); membra do Observatório de LGPD; e membra do Women Inside Trade Starters (WIT Starters).

pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. **Art. 41**. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. **Art. 46.** Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. **Art. 47.** Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. **Art. 42.** O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. **Art. 48.** O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.	medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.º e 14.º e qualquer comunicação prevista nos artigos 15.º a 22.º e 34.º a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios. **Art. 8 (Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação)** **Art. 15 (1) (h)** A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n. 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados. **Art. 30. (Registos das atividades de tratamento)** **Art**. **29**. O subcontratante ou qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, não procede ao tratamento desses dados exceto por instrução do responsável pelo tratamento, salvo se a tal for obrigado por força do direito da União ou dos Estados-Membros. **Art. 37 (Designação do encarregado da proteção de dados)** **Art. 24 (1)** Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades. **Art. 25 (Proteção de dados desde a conceção e por defeito;)** **Art. 28 (Subcontratante);** **Art. 32 (Segurança do tratamento);** **Art. 31.** O responsável pelo tratamento e o subcontratante e, sendo caso disso, os seus

	representantes cooperam com a autoridade de controlo, a pedido desta, na prossecução das suas atribuições. **Art. 33. Notificação de uma violação de dados pessoais à autoridade de controlo** **Art. 34. Comunicação de uma violação de dados pessoais ao titular dos dados**

Introdução

Com a globalização e digitalização da sociedade atual, a preocupação com o tratamento de dados pessoais cresce cada vez mais, principalmente diante dos grandes conglomerados de tecnologia que têm livre acesso e controle aos dados de milhões de usuários. Nesse contexto, diversas jurisdições têm iniciado sua trajetória para regulamentação do tratamento de dados pessoais, dentre as quais não se pode deixar de mencionar a União Europeia e o Brasil.

O bloco europeu foi um dos pioneiros na busca pela proteção de dados, editando ainda no ano de 1995 a Diretiva de Proteção de Dados Pessoais (95/46/CE), que, em 2016, foi substituída pelo Regulamento Geral sobre a Proteção de Dados (RGPD). A diretiva abriu o caminho para a discussão acerca da segurança de dados na rede e dos deveres e regras que esses agentes que realizam o tratamento de dados devem se ater. Foi justamente inspirado no RGPD, que o congresso brasileiro promulgou a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados ou LGPD) no ano de 2019, com clara influência do normativo europeu.

Nesse contexto, o presente artigo pretende perpassar pelas principais obrigações dos agentes de tratamento diante dessa nova era de regulamentação da internet que se mostrou extremamente necessária no mundo digital, traçando um paralelo entre o que é definido pelo RGPD e pela LGPD. A fim de aprofundar a discussão legislativa, serão abordados também dois casos práticos envolvendo a empresa Whatsapp Inc. em que essas obrigações foram evidenciadas pelas autoridades de proteção de dados responsáveis, um brasileiro e outro no âmbito da União Europeia.

1. Comentários

O tratamento de dados corresponde a "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento,

eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (art. 5º, inciso X, da LGPD).

Como ensina Mario Viola e Chiara de Teffê (2020, p. 131), o pressuposto para a regulação do tratamento de dados é justamente a proteção do titular, de forma que na "Lei Geral de Proteção de Dados, parte-se da ideia de que todo dado pessoal tem importância e valor. Por essa razão, adotou-se conceito amplo de dado pessoal, assim como estabelecido no Regulamento europeu 2016/679, sendo ele definido como informação relacionada a pessoa natural identificada ou identificável". Nesse sentido, um passo importante para a proteção do dado pessoal é a identificação de quais são os agentes que poderão tratá-lo, bem como quais são os parâmetros e diretrizes que deverão ser seguidas nesse tratamento.

Conforme estipula a Lei Geral de Proteção de Dados, são considerados agentes de tratamento: o controlador e o operador. Embora essa classificação como "agente de tratamento de dados", enquanto categoria aglutinadora dos conceitos supra, não seja feita no âmbito da União Europeia, o RGPD também apresenta as categorias de controlador ("*controller*") e processador ("*processor*"), de forma que, para os fins deste artigo, serão analisados como equivalentes aos agentes definidos na LGPD.

Assim, antes de adentrar na discussão acerca das obrigações dos agentes de tratamento, faz-se necessário indicar, primeiro, como a LGPD e o RGPD classificam esses agentes e quem são as pessoas físicas ou jurídicas que se enquadram nessa categoria.

No âmbito da LGPD, os agentes de tratamento são considerados a partir de seu caráter institucional, isto é, "não são considerados controladores (autônomos ou conjuntos) ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento" (ANPD, 2021b, p. 5). Tanto pessoas jurídicas quanto pessoas físicas podem ser abarcadas por essas categorias. Ressalta-se, porém, que a pessoa física apenas poderá ser considerada controladora quando agir em prol de seu próprio interesse, dispondo de autonomia para determinar as finalidades e elementos essenciais do tratamento. Por outro lado, poderá ser considerada operadora quando atuar de acordo com os interesses do operador, com a autonomia para definição de elementos não essenciais à finalidade do tratamento (ANPD, 2021b).

No contexto da pessoa jurídica, é a própria organização que será considerada como agente de tratamento, de forma que os funcionários que atuam em subordinação às decisões do

controlador, representando-o, não deverão ser confundidos com operadores. Outrossim, a caracterização como controlador ou operador não é permanente, sendo definida a cada operação de tratamento de dados pessoais. Isto é, uma mesma empresa ou entidade poderá desempenhar os papéis de controlador ou operador a depender do seu papel em determinado tratamento de dados (ANPD, 2021b).

Pois bem, passado para as diferenças entre controlador e operador/processador, tem-se que a LGPD define que o controlador será aquele a "quem compete tomar as decisões referentes ao tratamento de dados pessoais" (art. 5º, VI, LGPD), de forma similar ao controlador do RGPD, que consiste na "pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que, isoladamente ou em conjunto com outros, determine os fins e os meios de tratamento dos dados pessoais" (art. 4 (7), RGPD). Embora seja possível identificar uma diferença conceitual — a explicitação da possibilidade de controladores conjuntos —, é possível perceber a similitude quanto à característica principal dessa categoria de agente: o poder de decisão — isto é, o controle dos elementos essenciais para o cumprimento da finalidade do tratamento.

A diferente classificação de controladores e operadores/processadores tem relevância não somente teórica, mas também prática. Isso porque tanto o RGPD quanto a LGPD atribuem responsabilidades diferenciadas e específicas para cada um desses.

No âmbito nacional, são exemplos de obrigações específicas do controlador: (i) a elaboração de relatório de impacto à proteção de dados pessoais (art. 38, LGPD); (ii) a comunicação à ANPD sobre eventual ocorrência de incidentes de segurança (art. 48); e (iii) a comprovação de que o consentimento obtido atende às exigências legais (art. 8, § 2º, LGPD). Tal distinção também se aplica à responsabilidade em relação à reparação por danos ilícitos, definida nos arts. 42 a 45 da LGPD, que é aplicada de forma diferente de acordo com a qualificação do agente (ANPD, 2021b).

Ressalta-se, a título de exemplo, que o operador será solidariamente responsável para com o controlador pelos danos causados aos titulares quando houver descumprido a legislação ou quando aquele não tiver seguido as instruções lícitas desse (art. 42, §1º, I). Por outro lado, os controladores serão sempre responsáveis solidários entre si quando ocorrerem danos ao titular de dados (art. 42, §1º, II). Veja que, quanto ao operador, deverá ser comprovada a atividade ilícita ou descumprimento de instruções, enquanto o controlador responderá objetivamente, aos moldes da responsabilização por atividades de risco disposta no art. 927,

Parágrafo Único, do Código Civil. Quanto às matérias de defesa que poderão ser alegadas, essas estão restritas à comprovação das exceções descritas no art. 43 para os controladores. Por outro lado, o operador poderá, além das exceções retro, comprovar que cumpriu os dispositivos legais, que a instrução do controlador foi cumprida e/ou que essa era ilegal (justificando o seu descumprimento).

Enquanto isso, no âmbito da União Europeia, o controlador será responsável por realizar e demonstrar o *compliance*, em alinhamento ao princípio da "*accountability*" (art. 5 (2), RGPD); bem como pela realização da avaliação do impacto da proteção de dados para examinar, em particular, a origem, natureza, particularidade e gravidade desse risco (Consideração nº 84, RGPD). O controlador também será responsável, entre outros, por demonstrar que o processamento ocorreu com o consentimento do titular de dados (art. 7 (1), RGPD), facilitar o exercício dos direitos dos titulares de dados, ressalvadas as hipóteses de não identificação do titular e providenciar cópias dos dados pessoais que passam pelo tratamento de dados (art. 15 (3), RGPD).

Em relação aos controladores conjuntos, embora não esteja expresso na LGPD, a ANPD, no exercício de sua função regulamentar, reconheceu essa possibilidade para o ordenamento jurídico brasileiro. Para tanto, apontou os seguintes critérios para que esteja configurada uma controladoria conjunta: (i) mais de um controlador possui poder de decisão sobre o tratamento de dados pessoais; (ii) há interesse mútuo de dois ou mais controladores, com base nas finalidades próprias, sobre um mesmo tratamento; e (iii) dois ou mais controladores tomam decisões comuns ou convergentes sobre as finalidades de tratamento (ANPD, 2021b, p. 13).

De forma análoga, o Comitê Europeu para Proteção de Dados (EDPB, 2020, p. 18) indicou que duas decisões podem ser consideradas convergentes quando complementam uma à outra e quando for necessário para que o processamento ocorra de forma a impactar, de modo tangível, a determinação dos propósitos e meios de processamento.

Por sua vez, o operador será aquele que que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII, LGPD), de forma similar ao processador do RGPD, que consiste na "pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que processa dados pessoais em nome do responsável pelo tratamento" (art. 4 (8), RGPD). "Isso demonstra a principal diferença entre o controlador e operador, qual seja, o poder de decisão: o operador só pode agir no limite das finalidades determinadas pelo controlador" (ANPD, 2021b,

p. 16). Conforme explica o Parecer 1/2010 (WP29, 2010, p. 25) a “existência de processador depende de decisão do controlador, que pode decidir processar dados dentro de sua organização [...] ou delegar todas ou parte das atividades de processamento a uma organização externa, ou seja, [...] para pessoa separada legalmente agindo em seu nome".

Um aspecto relevante no ordenamento jurídico brasileiro é a questão vinculada às obrigações de tratamento da pessoa jurídica de direito público, isso porque em muitos casos existirá apenas uma pessoa jurídica (entidade da administração pública direta ou indireta) dividida internamente em vários órgãos (entes despersonalizados). Quando estes órgãos realizam o tratamento de dados, surge um problema para a identificação do controlador. A ANPD (2021b) dispõe que nesses casos deverão ser considerados dois aspectos: de um lado, conforme o art. 5º, VI, da LGPD, o controlador é a União, que detém personalidade jurídica; por outro, a LGPD atribuiu aos órgãos públicos obrigações típicas de controlador, de forma que suas atribuições são exercidas pelos órgãos públicos que desempenham funções em nome da pessoa jurídica da qual fazem parte. O mesmo raciocínio pode, regra geral, ser aplicado analogamente para os estados e municípios, detentores de personalidade jurídica, suas secretarias e demais órgãos públicos a eles vinculados.

Detalhados os conceitos de controlador e operador, bem como suas funções, cumpre analisar, de modo geral, dada a grande amplitude do tema, as principais obrigações dos agentes de tratamento de dados — buscando, sempre que possível, traçar um paralelo entre as duas jurisdições. Para tal, considera-se que “o modelo de tratamento de dados instituído pela LGPD se ampara nas seguintes características básicas: a ampliação do conceito de dado pessoal; o respeito à base legal; e o legítimo interesse como hipótese autorizativa e necessidade de realização de um teste de balanceamento de interesses” (MENEZES; COLAÇO, 2019). Isso porque,

> A LGPD é categórica em relação às hipóteses que autorizam o tratamento de dados pessoais, ainda que os arts. 7.º (tratamento de dados pessoais), 11 (tratamento de dados pessoais sensíveis) ou 14 (tratamento de dados pessoais de crianças e adolescentes) do diploma arrolem conceitos jurídicos indeterminados (como “legítimo interesse”, nos termos do art. 7.º, IX, da LGPD) e confiram margem para inovações regulatórias ou contratuais (arts. 7.º, II, V, e 11, II, “a”, da LGPD) não minudenciadas na lei (ALVES JR., 2020).

Importante ressaltar que princípios legais como legítimo interesse, bem como a adequação, finalidade, proporcionalidade e necessidade são conceitos que permitem uma amplitude de interpretações, de modo que as expectativas dos titulares recebem um peso considerável na aplicação desses princípios. Assim, quanto "mais invasivo, inesperado ou genérico for o tratamento, menor será a probabilidade de que seja reconhecido o legítimo interesse" (VIOLA; TEFFÊ, 2020).

Outra obrigação importante e que parece embasar as demais obrigações dos agentes de tratamento é a obrigação de transparência. O princípio da transparência é entendido como um dos pilares no tratamento de dados, conforme evidenciou a Convenção nº 108 do Conselho da Europa. Tal princípio foi recepcionado tanto pelo RGPD, em seu art. 12º, em consonância com o Considerando nº 58 — ao aduzir que "o princípio da transparência exige que qualquer informação dirigida ao público ou ao titular dos dados seja concisa, facilmente acessível e fácil de entender, com linguagem clara e simples e, além disso, onde apropriado, a visualização deve ser usada"[2] — quanto como pela LGPD, em seu art. 6º, VI, a qual garante aos titulares dos dados informação clara, precisa e facilmente acessível sobre a realização do tratamento.

A obrigação de transparência não apenas adquire um papel importante na garantia de *accountability* das empresas que realizam o tratamento de dados, mas também aduz um importante papel social, especialmente quando contraposta aos princípios da dignidade humana e não discriminação. Essa relação é resumida com clareza na seguinte afirmação dos pesquisadores Bruno Bioni, Marina Kitayama e Mariana Rielli (2021, p. 35):

> Adotando a perspectiva de que a proteção de dados tutela bens jurídicos de interesse da coletividade, como a não discriminação e a dignidade humana, a publicidade sobre as práticas de tratamento é de extrema importância. Há casos em que o tratamento abusivo de dados leva a violações de direitos afetos a todos de um segmento populacional, sendo conhecidas as situações de discriminação por raça, gênero e perfil socioeconômico em virtude de usos abusivos de dados pessoais. A transparência ativa das empresas desempenha também um papel de responsabilidade social, sujeitando suas próprias práticas à apreciação pública de um lado; e criando uma cultura que padroniza essa atitude nos mercados, de outro.

[2] Tradução livre.

Ademais, o capítulo VI da LGPD trata especificamente dos agentes de tratamento de dados, dispondo algumas das obrigações específicas desses agentes perante a nova legislação em vigor. Nesse sentido, dispõe que caberá ao controlador e ao operador manter o registro das operações de tratamento de dados pessoais que realizarem (art. 37, LGPD). De forma similar, o RGPD estipula, em seu art. 30, a necessidade de documentação dos processos. Contudo, diferentemente da LGPD, o RGPD aprofunda nesse tema ao dispor sobre a obrigação de revisão e de atualização dos procedimentos adotados de acordo com as necessidades que esses apresentem (PECK, 2020).

As obrigações dos agentes de tratamento de dados não são determinadas apenas durante o período de processamento dos dados, mas também quando esse tratamento é finalizado. Assim, os arts. 15 e 16 da LGPD definem as hipóteses do término do tratamento de dados e a obrigação dos agentes em eliminá-los, ressalvadas as hipóteses legais. O término poderá ocorrer por diversas situações, dentre as quais: (i) o alcance da finalidade pretendida; (ii) os dados pessoais deixam de ser necessários ou pertinentes para o alcance da finalidade específica; (iii) determinação da autoridade nacional de proteção de dados; (iv) manifestação do titular requerendo o término do tratamento, entre outros (ALVES JR., 2020).

Por sua vez, o RGPD define de forma expressa a necessidade de prazos para o apagamento dos dados ou revisão periódica, introduzindo uma limitação temporal para o tratamento de dados — que não aparece de forma expressa na LGPD — ao determinar que:

> Considerando (39) (...) A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica.
> Artigo 5.º Princípios relativos ao tratamento de dados pessoais
> 1. Os dados pessoais são:
> (...)
> e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados (“limitação da conservação”);

Verificou-se, portanto, que o conjunto de obrigações e condutas sobre as quais devem se pautar os agentes de tratamento é extensa, apresentando tanto um conjunto de parâmetros gerais que devem ser observados, como os princípios da finalidade, consentimento, adequação, transparência, dentre outros; quanto responsabilidades específicas, como a apresentação de relatórios de impacto, entre outros. Assim, diante da dificuldade de perpassar pormenorizadamente por cada uma das obrigações legais, optou-se por realizar a análise dos normativos sob uma perspectiva geral.

Com a finalidade de aprofundar essa análise, realizar-se-á, no próximo tópico, estudo de dois casos que foram julgados ou discutidos nas duas jurisdições analisadas, buscando apontar como essas obrigações se traduzem na prática e qual o papel da autoridade na fiscalização e observância destas.

2. Estudos de Caso

Com a finalidade de melhor aprofundar o estudo sobre as obrigações dos agentes de tratamento ante aos comandos e diretrizes da Lei Geral de Proteção de Dados e do Regulamento Geral sobre a Proteção de Dados, principalmente diante da necessidade de transparência desse tratamento, o presente tópico se ocupará da análise de dois casos práticos envolvendo a política de privacidade de uma mesma empresa: WhatsApp Inc. (“WhatsApp”).

A escolha pelos casos se deu com o intuito de traçar um paralelo consistente entre os contextos analisados, buscando, tanto quanto possível, explorar condutas semelhantes sob o escopo das duas jurisdições. Para tal, optou-se por comparar possíveis violações às obrigações legais dos agentes de tratamento de dados por parte da empresa WhatsApp segundo apontaram as investigações pela Autoridade Nacional de Proteção de Dados (ANPD), no Brasil, e pelo *Irish Data Protection Commission* (DPC), principal responsável por supervisionar as atividades do grupo Facebook no âmbito da União Europeia.

Cabe apontar que atualmente a Política de Privacidade vigente na União Europeia, Estados Unidos e Canadá é distinta dos demais países, uma vez que o provimento é realizado por diferentes subsidiárias: WhatsApp Ireland na Europa e WhatsApp LLC no Brasil (ANPD, 2021), por exemplo. Em que pese pontuais divergências entre as políticas, o escopo maior do tratamento de dados diante das políticas de privacidade permite realizar a comparação pretendida.

2.1. *Irish Data Protection Comission* v. *Facebook Ireland Limited*: Ausência de transparência na política do WhatsApp

Em 2018, o *Data Protection Comission* (DPC) iniciou uma investigação contra o WhatsApp a fim de verificar o cumprimento das obrigações de transparência em sua política de privacidade, especialmente no que tange à prestação de informações suficientes acerca de como os dados dos titulares eram processados. A investigação não foi vinculada a nenhuma denúncia, de forma que, definindo seus próprios parâmetros de investigação, o DPC buscou determinar se as ações do Facebook Ireland Ltd. (controladora do WhatsApp) no que se referem à transferência de dados pessoais de indivíduos da União Europeia eram legítimas e legais.

Em consonância com a discussão travada no tópico anterior acerca de controladores e processadores/operadores, o DPC reservou uma sessão na decisão final para definir em qual dessas categorias se enquadrava o WhatsApp quando do processamento de dados pessoais. Entendeu a autoridade que apenas o WhatsApp teria tomado todas as decisões relacionadas aos aspectos centrais do processamento de dados de não-usuários, bem como serie ele o único que poderia implementar alguma modificação no referido processamento, seja por novo código ou por emendas aos termos e condições de serviço, configurando-se, portanto, como um controlador (DPC, 2021).

A partir da definição acerca do tipo de agente de tratamento, o DPC pôde analisar quais obrigações específicas do controlador estariam sendo ou não cumpridas pela empresa. Assim, a investigação foi dividida em três principais seções: (i) transparência no contexto de não usuários; (ii) transparência no contexto de usuários; (iii) transparência no contexto de compartilhamento de dados pessoais entre o WhatsApp e as empresas pertencentes ao grupo Facebook.

Pautando-se na obrigação de transparência, a investigação entendeu que, quando há coleta de dados pessoais, é obrigação do agente de tratamento providenciar informações acerca do processamento desses dados, havendo "um requisito cumulativo, que resulta nos artigos 13 (1) (c) e 13 (1) (d) operando em conjunto para aplicar ao controlador de dados um requisito para estabelecer os objetivos do processamento em relação à base jurídica do legítimo interesse, juntamente com os interesses legítimos perseguidos na realização das operações de tratamento" (EDPB, 2021, p. 11).

O DPC indicou haver diversas violações ao RGPD, principalmente aos artigos de 12 a 14, isto é, violações aos direitos dos titulares de dados. Entendeu o departamento irlandês que a questão estava atrelada diretamente à autonomia individual do titular em compartilhar os seus dados pessoais, de modo que "se as informações necessárias não foram fornecidas, o titular dos dados foi privado da capacidade de tomar uma decisão totalmente informada sobre se deseja ou não se tornar um usuário do Serviço" (DPC, 2021, p. 203). O princípio da transparência é aqui tomado como o fundamento para um regulamentar o tratamento de dados, não apenas porque reforça outros princípios, como o da *accountability*, mas também porque é dele que grande parte das obrigações do RGPD derivam (DPC, 2021).

Ademais, ao analisar se havia intenção (dolo) ou negligência (culpa) na conduta do WhatsApp, embora essa classificação não exista no RGPD — mas apenas nas "*Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679*"— , o DPC apontou que o WhatsApp já havia sido alvo de outra investigação realizada em conjunto entre o "*Office of the Privacy Commissioner of Canada*" (OCO) e a autoridade de proteção de dados da Holanda em 2012. Considerando, então, que as mesmas violações foram apontadas nas duas investigações, o DPC entendeu que o WhatsApp possuía conhecimento de que estaria infringindo as obrigações delineadas no RGPD.

Diante das irregularidades verificadas, o DPC determinou a condenação do WhatsApp, indicando que a empresa teria deixado de cumprir com as obrigações dos artigos 13, (1), (c), (d), (e) e (f), 12 (1), 13 (2), (a), (c), e (e) do RGPD, que tratam principalmente da obrigação de transparência. O caso acabou sendo alçado para a alta corte europeia, quando foi confirmada a regularidade da investigação que reconheceu existência de ilegalidades no tratamento de dados realizado pelo WhatsApp, culminando na condenação em 225 milhões de euros em multa (HIGH COURT, 2021).

Não obstante, o WhatsApp informou que, desde então, diversas atualizações foram feitas na política de privacidade (BBC, 2021). Uma das alterações mencionadas pelo WhatsApp diz respeito a uma atualização geral na Política de Privacidade que ocorreu em todas as regiões do globo em que a plataforma opera. Importa frisar que, como apontou a própria Autoridade Nacional de Proteção de Dados (2021a), em razão da vigência do RGPD, a atualização que ocorreu nos países da União Europeia foi significativamente diferente da que tomou lugar no Brasil. Tais diferenças se deram essencialmente quanto à base legal para o tratamento de dados, à forma como ocorre esse tratamento de dados e à disposição de como exercer os direitos do

titular, todas essas obrigações dos agentes de tratamento que foram incluídas na política de privacidade europeia, mas não tiveram correspondentes no Brasil.

Em que pese a grande influência do RGPD na legislação de proteção de dados brasileira, tais disposições não parecem ter sido observadas no caso em questão. A fim de melhor explorar os pontos que foram deixados de fora da política de privacidade do WhatsApp no Brasil, bem como discutir quais são as obrigações dos agentes de tratamento no âmbito da LGPD a partir de uma das primeiras manifestações da ANPD, parte-se para a análise da Nota Técnica nº 02/2021/CGTP/ANPD, na qual são realizados apontamentos técnicos da autoridade acerca da referida política.

2.2. Nota Técnica nº 02/2021/CGTP/ANPD: Política de Privacidade do WhatsApp em face das obrigações definidas pela LGPD

Em janeiro de 2021, o Whatsapp notificou seus usuários acerca de atualizações na sua Política de Privacidade e Termos de Serviço, que seriam implementadas a partir de 15.05.2021. Em razão da grande base de dados a qual tem acesso, principalmente considerando fazer parte do grupo econômico do Facebook (com o qual compartilha metadados desde 2016), as alterações na política do WhatsApp geraram forte repercussão nacional e internacional (ANPD, 2021a).

Nesse contexto, a ANPD acompanhou de perto essa atualização, solicitando informações adicionais e realizando reuniões com as representantes da empresa e outros órgãos públicos. Assim, a referida autoridade elaborou dois documentos, a Nota Técnica nº 02/2021 e a Recomendação Conjunta, nos quais são apresentadas recomendações de adequação da Política de Privacidade do WhatsApp à LGPD, orientando e esclarecendo quais seriam os direitos dos usuários nesse cenário (BRASIL, 2021b).

No decorrer da Nota Técnica nº 02/2021 e também na Recomendação Conjunta, a Autoridade Nacional de Proteção de Dados, em colaboração com o Ministério Público, Conselho Administrativo de Defesa Econômica e Ministério da Justiça e Segurança Pública, fez apontamentos importantes sobre o enquadramento do tratamento de dados realizado pela empresa na recém promulgada Lei Geral de Proteção de Dados, dando um importante direcionamento para verificar como essa autoridade se colocará diante das obrigações dos

agentes de tratamento de dados. Por essa razão, serão aqui analisados os principais pontos tratados nas duas manifestações.

Diferentemente, porém, do que ocorreu no âmbito da União Europeia, importa frisar que quando essa Nota Técnica foi formulada pela ANPD, as sanções administrativas (arts. 52 a 54) ainda não estavam em vigor, conforme determinação do art. 65, I-A, da LGPD. Desse modo, o objeto do processo administrativo não foi apurar a ocorrência de infrações, mas sim balizar a atuação de um importante agente de tratamento de dados, uma vez que as demais obrigações constantes na LGPD não se submetiam ao período de *vacatio legis*. Dessas obrigações, a Nota Técnica nº 02/2021 ressalta:

> Normas relativas a indicação de base legal adequada para o tratamento de dados pessoais (arts. 7º, 8º. 10, 11 e 33), à transparência na relação entre os agentes de tratamento e titulares (art. 6º, IV e VI; art. 9º), à adoção de medidas de prevenção e segurança (arts. 6º, VII e VIII; arts. 46 a 51) e à garantia de direitos dos titulares (arts. 17 a 22), inclusive de crianças e adolescentes (art. 14). (ANPD, 2021, p. 4)

Assim, diante das obrigações elencadas na LGPD, a referida autoridade discorreu sobre alguns pontos que levantaram preocupações na nova política de privacidade, dentre os quais, evidenciou os seguintes: tratamento de dados realizado pela empresa desde 2016; as novas práticas de compartilhamento em razão do uso da ferramenta WhatsApp Business, que permite que o conteúdo de mensagens e dados de usuários saiam do domínio do WhatsApp e entrem em domínio de terceiros; e o compartilhamento de dados de usuários de seu aplicativo com a plataforma do Facebook.

A fim de instruir o processo, a ANPD (2021a) requisitou uma série de esclarecimentos acerca do compartilhamento de dados, sendo possível inferir quais as principais áreas de preocupação no tratamento de dados e merecem maior atenção pelos agentes de tratamento. São elas: (i) tipos de dados compartilhados; (ii) informações adicionais sobre os agentes de tratamento com os quais os dados são compartilhados; (iii) fonte dos dados pessoais; (iv) forma de armazenamento e compartilhamento; (v) finalidade do compartilhamento e do tratamento de dados subsequente realizado pelos agentes com os quais os dados são compartilhados; (vi) base legal da LGPD que autoriza o compartilhamento dos dados pessoais; (vii) justificativa para a aplicação da referida base legal; (viii) forma de obtenção e de armazenamento de consentimento; (ix) forma e consequências da recusa de concessão de consentimento pelos titulares dos dados pessoais compartilhados; (x) forma de concessão dos direitos determinados

no art. 18 da LGPD, aos titulares em relação ao compartilhamento de dados pessoais; (xi) mecanismos de segurança adotados para o compartilhamento.

Apontou a ANPD que a nova política de privacidade do WhatsApp padece de algumas irregularidades perante a LGPD, principalmente ao retirar da sua política de privacidade a possibilidade de restrição de compartilhamento dos dados com as empresas da família Facebook, seja para a finalidade de anúncios ou outra correlata; não apresentar informações suficientes quanto à dupla coleta de informação do lado do usuário e empresa; não informar com clareza quanto à coleta de dados de localização; não trazer as bases legais nas quais se embasam as finalidades do tratamento; e omitir questões de compartilhamento de dados que constavam na política de privacidade anterior.

Ao comparar a Política de Privacidade da empresa no Brasil e na União Europeia, a ANPD também notou um descompasso importante acerca das obrigações firmadas. Dentre essas, destacam-se as seguintes seções que restaram presentes na União Europeia, mas ausentes na política brasileira, apesar de constarem previsões na LGPD: (i) "Como tratamos seus dados", obrigação que consta no art. 10, § 2º da LGPD; (ii) "Nossa base legal para tratar dados", adequando-se ao disposto no art. 7º da LGPD; (iii) "Como exercer seus direitos", conforme dispõe o art. 18 da LGPD.

Nesse contexto, a ANPD utiliza o princípio da transparência como elemento-chave para a análise efetuada na Nota Técnica. Para tal, traçou um paralelo com caso julgado pela *Comission Nacionale I'Informatique et des Libertés* (CNIL) — autoridade francesa de proteção de dados — que condenou o Google, entre outras empresas, pela ausência de informações acessíveis aos usuários ou, quando presentes, havendo dificuldade de acessá-las, desconformidade com o RGPD; finalidades descritas de forma genérica e vaga; falta de clareza na base legal; e ausência de informação sobre o período de retenção de dados. Assim, seria somente com a transparência que "os titulares poderão [poderiam] exercer a chamada autodeterminação informacional e exercer seus direitos, em especial o de livre acesso" (ANPD, 2021a, p. 21).

Isso porque, embora o WhatsApp afirmasse que a atualização garantiria a transparência do processamento de dados, existem alguns requisitos para que realmente possa se considerar um tratamento de dados transparente que não foram devidamente cumpridos, como: informação clara, precisa e facilmente acessível. A autoridade aponta, entre outras considerações, que a análise de precisão e clareza da informação no Brasil deve considerar a cultura de privacidade

do país, o que, por ainda não ser amadurecida, dificulta o completo entendimento dos usuários acerca dos riscos envolvidos no tratamento. Tal análise deverá atrelar-se à ponderação do poder do tratamento de dados pessoais quantitativa e qualitativamente, bem como à capacidade de assimilação dos titulares dos novos produtos e serviços apresentados para seu uso. Quanto à facilidade de acesso, indica a importância de as informações sobre privacidade serem destacadas das outras provisões contratuais.

A autoridade apresenta também como importantes parâmetros de análise o princípio da necessidade e o legítimo interesse, pontuando as diferenças entre os dois conceitos. Afirmou a ANPD (2021a) que o legítimo interesse só pode ser justificado se não for sobreposto pelos direitos e liberdades fundamentais do titular, não sendo, portanto, absoluto. Para verificar a sobreposição, é necessário fazer um teste de sopesamento entre as razões para que se verifique se prevalece o legítimo interesse do controlador sobre os direitos do titular no caso concreto, sendo necessária uma interpretação conjunta do princípio da necessidade e do legítimo interesse.

Ao fim, a autoridade teceu diversas recomendações visando a assegurar que o WhatsApp tome as providências necessárias para regularizar a situação, a saber: (i) condução de Relatório de Impacto de Proteção de Dados sobre a integração dos serviços do WhatsApp Business e WhatsApp; (ii) criação de seções na Política de Privacidade que informem aos titulares as bases legais utilizadas e correlacione às finalidades e categorias de dados pessoais tratados; (iii) posição de destaque na Política de Privacidade do link que informa quais dados o WhatsApp compartilha com as Empresas do Facebook, aumentando a transparência do usuário; (iv) inserção na política de privacidade de um novo link que informe "Quais informações o WhatsApp compartilha com as empresas no WhatsApp?"; (v) disponibilização em destaque das informações para que o titular possa exercer seus direitos na própria Política de Privacidade; (vi) inserção de informação sobre o Aviso de Privacidade – Brasil, em seção específica, eliminando uma camada de acesso a informação; (vii) correção dos links disponibilizados no Aviso de Privacidade; (viii) correções quanto a revogação de consentimento ou aceitação; (ix) divulgação pública da identidade do encarregado; (x) acrescentar circunstâncias em que o tratamento de dados sensíveis poderia ocorrer de forma não intencional; (xi) acrescentar operações de tratamento de dados de crianças e adolescentes; (xii) descarte e exclusão seguros de dados; (xiii) implementação de controles administrativos relativos à privacidade da informação; (xiv) implementação *de privacy by design and by default*, para além da criptografia fim-a-fim dos conteúdos das mensagens (ANPD, 2021a).

Considerações Finais

Diante do exposto, restou clara a importância das definições de obrigações dos agentes de tratamento, a fim de balizar a sua conduta e evitar quaisquer tipos de abusos no tratamento de dados. Nesse contexto, com bem aponta o RGPD, "o risco para os direitos e liberdades das pessoas físicas, de probabilidade e gravidade variáveis, pode resultar do processamento de dados pessoais que podem levar a danos físicos, danos materiais ou não materiais, em particular: [...] onde os titulares dos dados possam ser privados dos seus direitos e liberdades ou impedidos de exercer controle sobre seus dados pessoais".

Da análise dos casos concretos, verificou-se que, embora os deveres dos agentes de tratamento já estejam devidamente estipulados na LGPD, parece haver uma falta de familiaridade dos agentes de tratamento com os dispositivos da lei, em contraposição ao regulamento europeu, que já está consolidado a mais tempo. Em que pese a LGPD tenha previsto a obrigatoriedade de determinação da base legal para o tratamento, os direitos dos titulares e a necessidade de transparência acerca do tratamento de dados, com disposições bastante semelhantes às constantes no RGPD, tais obrigações não foram traduzidas na política de privacidade do WhatsApp, diferentemente do que ocorreu na União Europeia.

Referências bibliográficas

ALVES JR., SÉRGIO. Fechando um ciclo: do término do tratamento de dados pessoais (art. 15 e 16 da LGPD). In. BIONI, Bruno et al (Coords.). Tratado de Proteção de Dados Pessoais. Disponível em: Minha Biblioteca, Grupo GEN, 2020.

ANPD, Autoridade Nacional de Proteção de Dados. Nota Técnica nº 02/2021/CGTP/ ANPD. Processo nº 00261.000012/2021-04. Assunto Atualização da Política de Privacidade do WhatsApp. Brasília, 22 de mar. 2021a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NOTATECNICADACGTP.pdf

ANPD, Autoridade Nacional de Proteção de Dados. Guia Orientativo para definições dos agentes de tratamento de dados pessoais e encarregado. Brasília/DF, mai. 2021b.

BBC, British Broadcasting Corporation. WhatsApp issued second largest GDPR fine of 225m. Publicado em 2 set. 2021. Disponível em: https://www.bbc.com/news/technology-58422465

BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. O Legítimo Interesse na

LGPD: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021

BRASIL. Recomendação Conjunta. Colaboração entre Ministério Público Federal, Conselho Administrativo de Defesa Econômica, Autoridade Nacional de Proteção de Dados e Ministério da Justiça e Segurança Pública. Brasília, 7 de mai. 2021a. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/recomendacao_whatsapp_-_assinada.pdf

BRASIL. ANPD divulga orientações aos usuários sobre a nova política de privacidade do WhatsApp. Publicado em 14 de mai. de 2021b. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/a-nova-politica-de-privacidade-do-whatsapp

DPC, Data Protection Commission. Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation. DPC Inquiry Reference: IN-18-12-2, Helen Dixon, Comissioner for Data Protection. Publicado em 20 Ago. 2021. Disponível em: https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf

EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, set. 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

EDPB. Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR. Publicada em 28 jul. 2021. Disponível em https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf

HIGH COURT. European Union. Facebook Ireland Limited v. Data Protection Commission. Judicial Review. 2020 No. 617 Jr; No. 126 COM. Judgement of Mr. Justice David Barniville delivered on the 14th day of May, 2021. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2021-08/Facebook%20v.%20DPC%20Judgment%2014.5.21.pdf

MENEZES, Joyceane Bezerra; COLAÇO, Hian Silva. Capítulo 6: Quando a Lei Geral de Proteção de dados não se aplica? In. TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1. ed. - São Paulo: Thomson Reuters Brasil, 2019.

PECK, Patrícia. Proteção de dados pessoais. Disponível em: Minha Biblioteca, (2nd edição). Editora Saraiva, 2020.

VIOLA, Mario; DE TEFFÊ, Chiara Spadaccini. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11º. In. BIONI, Bruno et al (Coords.). Tratado de Proteção de Dados Pessoais. Disponível em: Minha Biblioteca, Grupo GEN, 2020.

WP29. Opinion 1/2010 on the concepts of "controller" and "processor". Adotado em 16 fev. de 2010. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

SEGURANÇA DA INFORMAÇÃO NO TRATAMENTO DE DADOS PESSOAIS

Paulo Ricardo da Silva Santana [1]

Dispositivo LGPD	Dispositivo RGPD
Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.	**Art. 32.** Segurança do tratamento Levando em consideração o estado da técnica, os custos de implementação e a natureza, escopo, contexto e finalidades do processamento, bem como o risco de probabilidade e severidade variadas para os direitos e liberdades das pessoas físicas, o controlador e o operador devem implementar medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco, incluindo, inter alia, conforme apropriado [...]:

Introdução

É difícil imaginarmos uma esfera da vida humana que não tenha influência da Tecnologia da Informação (TI), tendo em vista a centralidade que os dados exercem na sociedade atual, que é progressivamente sustentada por meios tecnológicos e digitais, orientada pelos dados que produz em volumes e velocidades cada vez maiores.

A segurança da informação, até pouco tempo atrás, estava voltada para a proteção do negócio no âmbito empresarial.[2] Contudo, na sociedade atual, essa disciplina da área de TI tem se direcionado para a proteção de toda e qualquer informação, até mesmo aquelas relativas a informações pessoais.[3] Nesse sentido, conforme as legislações de proteção de dados avançam, a segurança da informação ganha cada vez mais relevância. Se anteriormente as empresas se

[1] Paulo Ricardo da Silva Santana é graduado em Sistemas de Informação pelo Centro Universitário do Distrito Federal (UDF) e em Direito pela Universidade de Brasília (Unb). Coordenador de Pesquisa do Observatório da LGPD/Unb. Membro da comissão de Privacidade e Proteção de Dados da OAB/DF. Advogado e Consultor em Proteção de Dados em FDS Advogados.

[2] A norma internacional ISO 27001:2013, que trata sobre segurança da informação, relaciona incidente de segurança com os riscos às operações de negócio.

[3] A ISO (International Organization for Standardization) acompanhando o cenário internacional com relação à proteção de dados pessoais, atualizou a família de normas ISO 27000 com uma norma específica sobre privacidade, a norma ISO/IEC 27701.

preocupavam apenas em proteger a receita do seu produto comercial, atualmente elas também precisam se atentar para a proteção das informações de seus funcionários, consumidores etc.

No Regulamento Geral sobre a Proteção de Dados (RGPD), a segurança da informação no tratamento de dados pessoais é disciplinada no art. 32, o qual dispõe que os agentes de tratamento devem implementar medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco. Por sua vez, a Lei Geral de Proteção de Dados (LGPD) trata do tema em seu art. 46, segundo o qual os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Ante a breve exposição supra, pretende-se, neste artigo, realizar um exame comparativo entre casos relacionados à segurança da informação em âmbito europeu e brasileiro. O caso europeu é o Knuddels decidido pela autoridade de proteção de dados do estado alemão de Baden-Württemberg. O caso brasileiro é o recente vazamento de dados da Serasa Experian, ainda em fase investigativa no âmbito administrativo e de conhecimento no âmbito judicial. Por fim, pretende-se ainda realizar alguns breves apontamentos doutrinários sobre o conteúdo da segurança da informação no RGPDe na LGPD.

1. Estudo de caso

1.1. Caso Knuddels GmbH & Co. KG – Armazenamento de senhas em texto simples

Em 28 de novembro de 2018, a *Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg*- LfDI Baden-Württemberg, autoridade de proteção de dados do estado alemão de Baden-Württemberg, aplicou penalidade de multa de 20 mil euros à empresa Knudells GmbH & Co. KG, rede social alemã com mais de 1,8 milhão de usuários, por violação da obrigação de garantia da segurança dos dados pessoais com fundamento no art. 32 do GDPR.[4]

Em agosto de 2018, a Knudells sofreu um ataque hacker, ocasionando o vazamento de dados como o apelido dos usuários na rede social (*nickname*), seus verdadeiros nomes, endereço

[4] *LfDI Baden-Württemberg verhängt sein erstes Bußgeld in Deutschland nach der DS-GVO*. *LfDI Baden-Württemberg*. 22 de nov. de 2018. Disponível em: <https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo> . Acesso em 09 de set. de 2021.

de e-mail e até mesmo seus endereços residenciais.[5] Tão logo soube do ataque, a empresa comunicou seus usuários do incidente ocorrido fornecendo instruções para que realizassem a alteração de suas senhas de acesso.

Em comunicado à imprensa, a Knudells tornou pública a ocorrência do ciberataque e, por meio de várias redes sociais, pediu desculpas aos seus usuários pelo incidente. Além dessas medidas, a própria empresa elaborou um relatório acerca do incidente de segurança ocorrido e apresentou à LfDI Baden-Württemberg.[6] Por fim, prosseguiu com investimentos para atualização da infraestrutura com o fim de melhorar a segurança.

Tanto na investigação conduzida pela LfDI Baden-Württemberg, quanto pelas informações fornecidas pela Knudells, verificou-se que as senhas dos usuários eram armazenadas em arquivos de texto simples e sem criptografia.[7] Este foi o ponto central discutido no caso.

Em sua decisão, a LfDI Baden-Württemberg concluiu que, ao armazenar senhas não criptografadas, a Knudells não protegeu estes dados por meio de medidas técnicas e organizacionais adequadas para impedir o acesso de pessoas não autorizadas e, portanto, violou sua obrigação de garantir a segurança dos dados ao processar dados pessoais, em conformidade com o art. 32, 1 do RGPD.

A Knuddels foi poupada de uma penalidade mais severa em decorrência de uma estratégia eficaz de resposta ao incidente de segurança, notificando seus usuários de forma rápida, procurando a autoridade competente e fornecendo as informações necessárias para a condução da investigação, o que foi levado em consideração para o estabelecimento do valor da multa, seguindo o disposto no art. 83, 2 do RGPD.[8] No caso em tela, a boa-fé do infrator, a vantagem auferida, o grau do dano, a não reincidência e a cooperação com as autoridades foram determinantes na aplicação da sanção.

---

[5] Knuddels von Hackern angegriffen. Der Spiegel. 08 de set. de 2018. Disponível em <https://www.spiegel.de/netzwelt/web/knuddels-de-von-hackern-angegriffen-a-1227170.html>, acesso em 31 de ago. de 2021.

[6] Chat-Plattform muss nach Hackerangriff Bußgeld zahlen. Der Spiegel. 21 de nov. de 2018. <https://www.spiegel.de/netzwelt/web/knuddels-chat-plattform-muss-nach-hackerangriff-bussgeld-zahlen-a-1239776.html>, acesso em 31 de ago. de 2021.

[7] Criptografia é comumente utilizada para aumentar a segurança de dados em geral. Por meio da dela um dado é cifrado, de modo que apenas quem possui uma chave, pode decifrá-lo e acessar o seu c conteúdo.

[8] Este mesmo artigo encontra paralelo com o art. 52, §1º da LGPD.

1.2. *Caso Serasa Experian* - Vazamento de dados

Diferente do caso alemão, o caso do suposto vazamento de dados da Serasa Experian ainda está sendo analisado pela ANPD e vem sendo acompanhado pelo Ministério Público e por órgãos de defesa do consumidor sendo também objeto de Ação Civil Pública (ACP nº 5002936-86.2021.4.03.6100) que tramita na 22ª vara cível federal de São Paulo, ajuizada pelo Instituto Brasileiro de Defesa da Proteção de Dados Pessoais, Compliance e Segurança Da Informação – SIGILO.

Tal como o caso Knudells, o presente caso versa sobre o vazamento de dados, supostamente das bases de dados do Serasa Experian, se diferenciando essencialmente daquele pela sua dimensão e pela natureza dos dados vazados, em que se reporta que 223 milhões de brasileiros tiveram expostos dados pessoais como CPF, foto de rosto, salário e score de crédito.[9] O vazamento foi inicialmente reportado pela startup brasileira PSAFE, logo após o lançamento de um produto contra vazamento de dados de empresas.[10] A denúncia da empresa de cibersegurança provocou a reação de diversas entidades e órgãos de defesa do consumidor. Nesse contexto, o Instituto SIGILO, associação voltada a assuntos relacionados ao direito à privacidade, ajuizou uma Ação Civil Pública.

Na ACP, o Instituto SIGILO argumentou na inicial que, muito embora a Serasa Experian negue ser a origem do vazamento, há indícios suficientes de sua responsabilidade em razão de os dados estarem associados a serviços oferecidos exclusivamente pela ré, além do fato de o nome do arquivo de banco de dados vazado ser "JBR - Serasa Experian - Full Service".

Ainda segundo o Instituto SIGILO, a responsabilidade da Serasa Experian decorre do fato da empresa ter se omitido de tomar todas as medidas razoáveis necessárias para prevenir atividades que pudessem resultar na violação da legislação, qual seja, o dever objetivo de cuidar e de aplicar as melhores práticas de segurança da informação aos dados conforme o disposto art. 46 da LGPD.

---

[9] VENTURA, Felipe. Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava. Tecnoblog. Disponível em: <https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/amp/> . Acesso em 1 set. 2021

[10] O CEO da PSAFE, Marco De Mello informou que em outubro de 2020, a empresa lançou o "*Dfndr Enterprise*", solução contra o vazamento de dados de empresas. Ao varrer a dark web, o sistema de inteligência artificial de monitoramento alertou para o vazamento de 40 milhões de CNPJs. Sem dar muitos detalhes, De Mello informou que o primeiro passo foi validar os vazamentos a partir de uma amostra de dados coletada com o criminoso pela dark web. Ver mais em SAMBRANA, Carlos. Uma catástrofe digital se aproxima. E nem as empresas e as pessoas se ligaram. Neofeed. 05 de fev. de 2021. Disponível em <https://neofeed.com.br/blog/home/uma-catastrofe-digital-se-aproxima-e-nem-as-empresas-e-as-pessoas-se-ligaram>, Acesso em 15 de set. de 2021.

Em sede de contestação, a Serasa Experian alegou que no exame de sua infraestrutura, realizado por uma auditoria especializada, não se verificou indícios de vazamento massivo de dados. Além do mais, foi alegado que a Serasa possui os recursos técnicos adequados para prevenir, detectar e conter incidentes de vazamento de dados. A ré argumentou ainda que prestou os esclarecimentos necessários à ANPD, executou todas as rotinas previstas em seus protocolos internos e intensificou todas as medidas de monitoramento, verificação e identificação, previstas em suas diretrizes internas.

Colocando os casos lado a lado, é importante observar a diferença da condução dos incidentes pela Serasa Experian e a Knudells, especialmente com relação a notificação das pessoas afetadas. Justo mencionar que no caso alemão, a responsabilidade da empresa estava clara em razão dos dados vazados, até mesmo pelo reconhecimento da própria Knudells. Por sua vez, no caso da Serasa Experian há a controvérsia em torno da origem do vazamento, isto porque não só pelo fato de a Serasa ter negado ser a fonte do vazamento como também pelo fato de que, conforme apontado pela ANPD em sua contestação, ao analisar amostra do vazamento, o Gabinete de Segurança Institucional da Presidência da República (GSI) indicou que o vazamento seria uma mescla de diversas bases de dados do setor privado.

Ainda que a origem não tenha sido exclusiva da Serasa Experian, se das amostras analisadas se reconheceu dados exclusivamente tratados por ela, conforme aponta o Instituto SIGILO na inicial, a notificação aos titulares afetados deveria ter sido realizada, devendo a responsabilidade individual ser apurada em momento posterior, observando o devido processo legal, tal como impõe o art. 52, §1º da LGPD. A comunicação ao titular de incidente de segurança referente a seus dados pessoais não deve ser interpretada como uma assunção de culpa, mas sim como respeito e cumprimento às disposições da LGPD, além de demonstrar boa-fé do controlador que, enquanto princípio, deve ser observada em todas as atividades de tratamento de dados pessoais.[11] A ausência de notificação dos titulares por parte da Serasa Experian, ainda que em fase investigativa, diante dos fatos já postos, indica, além de violação diretamente ao art. 48, §1º da LGPD, ofensa aos seus princípios, tal como o da transparência e da prestação de contas.

Contudo, o que se verificou foi que a própria ANPD, em detrimento dos titulares afetados, ratificou a argumentação da Serasa Experian quando, ao ser questionada sobre a notificação dos titulares de dados, afirmou que ainda seria preciso aguardar a correta

[11] Art. 6º, caput da LGPD.

identificação dos controladores responsáveis. Decerto que a ANPD não pode exigir o cumprimento de uma obrigação sem que seja apurada, por meio de processo adequado, a devida responsabilidade do controlador. Contudo, seria importante que em sua atuação junto à Serasa Experian, a ANPD orientasse a empresa no sentido de comunicar aos titulares de dados pessoais afetados sobre o vazamento de dados, o que poderia ser feito deixando claro aos titulares que o caso ainda estaria em fase investigativa com relação à origem. Como se verá adiante, a notificação dos titulares é importante não somente por questões de transparência e prestação de contas, mas também porque possibilita que o próprio titular de dados tome medidas de proteção. Diante do papel da agência, da extensão do vazamento, dos riscos envolvidos aos titulares e dos elementos da atuação da ANPD no caso em tela, enseja preocupação quanto aos próximos incidentes de segurança que possam surgir.

2. Doutrina

A segurança da informação é definida como preservação da confidencialidade, integridade e disponibilidade da informação.[12] Importante destacar que não há distinção entre o formato da informação, de modo que ela pode estar em meio digital ou físico. Em uma sociedade altamente informatizada, quando falamos em medidas técnicas e administrativas, imaginamos medidas aplicáveis aos meios digitais como senhas, criptografia, antivírus, firewall, backups etc. No entanto, é preciso observar que quando falamos em segurança no tratamento de dados, também deve-se incluir as informações em meio físico. A título de exemplo, o acesso identificado em sala de arquivos e a correta eliminação de dados em papel também são exemplos de medidas administrativas que aumentam a segurança da informação e diminuem o risco de acesso não autorizado à informação.

Na União Europeia, a segurança da informação é tratada por meio de normas e regulamentos específicos e de uma agência própria, a ENISA.[13] No Brasil, contudo, conforme observa Laura Schertel, a segurança da informação não compõe uma política pública própria, nem é executada por um órgão centralizado, como na Europa, mas sim faz parte da agenda de diversos órgãos e atores, que realizam iniciativas esparsas e independentes.[14] Algumas normas

[12] HINTZBERGEN, Jules. Fundamentos da Segurança da Informação: com base na ISO 27001 e na ISO 27002/Jule Hintzbergen... [et al]; tradução Alan de Sá - Rio de Janeiro: Brasport, 2018. P. 30.
[13] A ENISA é a Agência da União Europeia para Cybersegurança que tem o papel de contribuir para a elaboração da política e da legislação da UE em matéria de segurança das redes e da informação.
[14] MENDES, Laura Schetel. Segurança da Informação, Proteção de Dados Pessoais e Confiança. Revista de Direito do Consumidor, São Paulo, vol. 90, p245-261, nov.-dez.2013. p. 249.

como o Código de Defesa do Consumidor, o Marco Civil da Internet (MCI) e até mesmo o Código Penal trazem disposições importantes sobre segurança da informação, porém, é na LGPD que o tema ganha notável destaque, muito em razão de sua interdependência[15] com a proteção de dados pessoais.

Além de um capítulo dedicado ao tópico (VII), a segurança também é referenciada nos arts. 12, §3º; 13, caput e §2º; 34; 38 parágrafo único; 40; 44; 50; e 55-J. Ademais, assim como o RGPD, a LGPD também reconheceu a segurança como um princípio,[16] segundo o qual o tratamento de dados pessoais deve observar a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.[17]

2.1. Requisitos mínimos de segurança

Da leitura do art. 46, Fabiano Menke e Guilherme Goulart, apontam para o fato de que o referido artigo traz um conceito jurídico indeterminado ao impor a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais. Segundo os autores, diante de múltiplas situações envolvidas nos sistemas utilizados, não parece simples indicar o que é uma medida apta.[18] Esta lacuna poderá ser suprida por meio de regulamentos futuros expedidos pela própria ANPD, seguindo o disposto no §1º do mesmo artigo.

Inicialmente, embora a indeterminação descrita acima possa parecer problemática, a disposição do art. 46, §1º viabiliza a expedição de regulamentos conforme as especificidades de cada setor. Desse modo, setores que tratam dados pessoais com maior potencial de afetar os titulares, como o da saúde e o financeiro, por exemplo, podem receber orientações mais precisas da ANPD quanto aos requisitos mínimos de segurança a serem observados no tratamento de dados pessoais.

[15] Ibid. p. 247. Sobre interdependência entre segurança e proteção de dados pessoais, Laura Schertel afirma que a proteção da privacidade e a política de segurança da informação formam, duas faces da mesma moeda; a efetividade de uma depende da efetividade da outra.
[16] A segurança também tem status de princípio no Marco Civil da Internet em seu art. 3º, inciso V.
[17] Art. 6º, VII da LGPD.
[18] MENKE, Fabiano. GOULART, Guilherme D. Segurança da Informação e vazamento de dados. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 347.

Por seu turno, diferente do que faz a LGPD, o RGPD traz, nas alíneas do seu art. 32, os parâmetros mínimos a serem adotados pelos controladores e subcontroladores para assegurar um nível mínimo de segurança adequado ao risco envolvido no tratamento de dados: a) a pseudonimização e a cifragem dos dados pessoais; b) a capacidade de assegurar confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; c) a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais em tempo razoável no caso de um incidente físico ou técnico; e d) um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Paul Voigt e Axel Bussche observam que o RGPD apresenta uma abordagem baseada em risco para determinar quais medidas técnicas e organizacionais são apropriadas em uma determinada situação.[19] O nível necessário de segurança de dados deve ser identificado caso a caso por meio de uma avaliação de risco objetiva. A avaliação do risco é importante na adoção de medidas de segurança, especialmente quando o tratamento abarca dados com potencial de discriminação, como é o caso dos dados pessoais sensíveis.[20] No entanto, o risco não decorre somente do tipo de dados envolvido, como também dos controladores e até mesmo de terceiros. Neste sentido, dispõe o Considerando nº 76 do RGPD que a probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento de dados. Embora de forma mais tímida, o risco também é mencionado pela LGPD ao se considerar as medidas de segurança a serem adotadas.[21]

Quanto aos requisitos mínimos de segurança, enquanto novos regulamentos não são estabelecidos pela ANPD, o Decreto nº 8.771/2016 que regulamenta o MCI pode ser aplicado de forma subsidiária, ao menos nas situações que envolvem o tratamento de dados pessoais no meio digital. O referido decreto possui uma sessão sobre padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas, na qual estabelece em seu art. 13 sobre as seguintes diretrizes de segurança: (I) o estabelecimento de controle estrito sobre o acesso aos dados; (II) a previsão de mecanismos de autenticação de acesso aos registros; III - a criação de

[19] VOIGT, Paul. BUSSCHE, Axel. The EU General Data Protecion Regulation (GDPR): A Practical Guide. Berlim. Springer.2017. p. 40.
[20] Art. 5º, II da LGPD.
[21] o art. 50, §1 da LGPD, impõe que ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado; e (IV) o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

2.2. Privacy by Design e Privacy by default

O §2º do art. 46 da LGPD cita que as medidas de que trata o caput deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Deste dispositivo se observa a positivação do conceito *privacy by design* (privacidade desde a concepção).[22] Bruno Bioni esclarece que o *privacy by design* é a ideia de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviços, devendo eles serem embarcados com tecnologias que facilitem o controle e a proteção das informações pessoais.[23] Nessa perspectiva, muitas são as medidas que podem ser adotadas para elevar a proteção de dados pessoais tais como criptografia, anonimização e pseudonimização dos dados.

Em relação ao *privacy by default* (privacidade por padrão), o *European Data Protecion Board* – EDPB [24] elucida que *by default* refere-se a fazer escolhas em relação aos valores de configuração ou opções de processamento que são definidos ou prescritos em um sistema de processamento, como um aplicativo de software, serviço ou dispositivo.[25] Nesse sentido, a título de exemplo, podemos citar as autorizações que são solicitadas ao usuário para permitir acesso à câmera ou ao microfone durante a utilização de algum aplicativo de celular, o que implica que por padrão, os aplicativos instalados não possuem acesso aos dados pessoais, devendo o usuário escolher se permite acesso ou não.

No RGPD, tanto o *privacy by design* quanto *privacy by default* são tratados no art. 25, 1 e 2, respectivamente. O regulamento europeu é mais detalhado sobre ambos e dispõe,

---

[22] CAVOUKIAN, Ann. Privacy by Design: the 7 fundational Principles. Jan. de 2011. p. 1. O *privacy by design* é um conceito criado pela pesquisadora canadense Ann Cavoukian, para quem a garantia de privacidade deve, idealmente, se tornar o padrão de uma organização modo de operação.

[23] BIONI, Bruno Ricardo. Proteção de Dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 234.

[24] O European Data Protection Board (EDPB) é o Comitê Europeu para a Proteção de Dados (CEPD). É um organismo europeu independente que visa contribuir para a aplicação coerente de regras em matéria de proteção de dados na União Europeia e promove a cooperação entre as autoridades de proteção de dados da UE.

[25] EDPB. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. 20 de out. 2020. Disponível em <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en> . Acesso em: 08 de set. de 2021.

inclusive, sobre a forma como o controlador pode comprovar o cumprimento das obrigações impostas pelos referidos dispositivos. Importante observar que o item 2 do art. 25 do regulamento europeu enuncia que o responsável pelo tratamento deve aplicar medidas técnicas e administrativas para assegurar que, por padrão (*by default*), só sejam tratados os dados pessoais que forem **necessários para cada finalidade** (grifei) específica do tratamento. Da leitura do dispositivo, denota-se, portanto, que o princípio da necessidade é um percurso essencial para a aplicação de medidas de segurança por padrão. Daí a afirmação de Bruno Bioni de que, apesar de a LGPD não dispor expressamente sobre o *privacy by default*, é possível extraí-lo do princípio da necessidade.[26]

Tanto o *privacy by design* quanto o *privacy by default* se relacionam com as chamadas *Privacy Enhancing Technologies* (PETs), que são tecnologias que facilitam e aprimoram a privacidade, resultando em medidas que protegem os dados pessoais e dão mais poder ao titular sobre seus dados pessoais. Neste sentido, Bruno Bioni assevera que as PETs são capazes de empoderar os cidadãos desempenhando um papel emancipatório.[27]

2.3. Comunicação de Incidente de Segurança

Conforme a norma internacional de segurança da informação ISO 27001:2013, incidente de segurança é indicado por um único ou uma série de eventos de segurança da informação, indesejados ou inesperados, que tenham uma probabilidade significativa de comprometer a operação dos negócios e ameacem a segurança da informação.[28] É uma definição ampla que engloba dados de qualquer natureza.

Partindo desse conceito é possível extrair o sentido de incidentes de segurança relativos a dados pessoais na LGPD. Neste sentido, Camila Jimene entende que, por meio de uma interpretação harmônica da LGPD, incidente de segurança relativo a dados pessoais pode ser interpretado como um acontecimento indesejado ou inesperado, que seja hábil a comprometer a segurança dos dados pessoais, de modo a expô-los a acessos não autorizados e a situações

[26] BIONI, Bruno R.; MONTEIRO, Renato Leite. Proteção de Dados Pessoais Como Elemento de Inovação e Fomento à Economia: O impacto econômico de uma lei geral de dados pessoais. In: Proteção de dados: contexto, narrativas e elementos fundantes / [organização Bruno Ricardo Bioni]. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021. p.356.
[27] BIONI, Bruno Ricardo. Op. cit. 2019. p. 234.
[28] HINTZBERGEN, Jules. Op. cit. 2018. P. 29

acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.[29]

O art. 48 da LGPD informa que o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Este artigo encontra dois correspondentes no RGPD. Isto porque o regulamento europeu possui um artigo para a comunicação com a autoridade de proteção de dados e outro para a comunicação com os titulares, respectivamente os arts. 33 e 34.

Segundo o RGPD, o controlador deve notificar a autoridade de controle sobre um incidente, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento sobre o mesmo. Essa notificação deve ocorrer apenas quando houver elevado risco para os direitos dos titulares. Segundo o Considerando nº 75 do GPDR, os riscos devem ser aferidos com base em uma avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado. Como abordado no tópico 2.1, esse risco é determinado pela natureza, âmbito, contexto e finalidade do tratamento de dados.

A LGPD, diferente do regulamento europeu, trata do prazo de notificação por meio de um conceito mais aberto, devendo a comunicação ser feita em prazo razoável.[30] Já para o titular, o art. 34 do RGPD informa que a comunicação deve ocorrer sem demora injustificada, o que parece repetir a abertura que ocorre no art. 48 da LGPD. O EDPB, na tentativa de jogar luz sobre a questão, afirma que o termo "sem demora injustificada" quer dizer o mais rapidamente possível.[31]

Já com relação às situações que obrigam a notificação de incidente, a exemplo do que também ocorre no art. 34 do RGPD, a LGPD dispõe que nem todo incidente acarretará a obrigação de comunicação, mas apenas aqueles aptos a acarretar risco ou dano relevante aos titulares de dados. A LGPD não orienta quanto aos critérios para se determinar quando um incidente acarreta risco ou dano relevante de modo que os critérios estabelecidos pelo RGPD

[29] JIMENE. Camilla do Vale. Capítulo VII: Da Segurança e das Boas Práticas. p.387. in: LGPD: Lei Geral de Proteção de Dados comentada/coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020.

[30] Pela redação do art. 48, §1º depreende se que a ANPD possa emitir regulamento sobre prazo razoável. Segundo a página oficial da ANPD, enquanto pendente a regulamentação, recomenda-se que após a ciência do evento adverso e havendo risco relevante, a ANPD seja comunicada com a maior brevidade possível, sendo tal considerado a título indicativo o **prazo de 2 dias úteis**, contados da data do conhecimento do incidente. Ver mais em "Comunicação de incidentes de segurança". ANPD. 22 de fev. de 2021. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>, acesso em 09 de set. de 2021.

[31] EUROPEAN DATA PROTECTION BOARD. Op. Cit. 2018. p. 21.

podem orientar o intérprete da norma brasileira.[32] Nessa direção, Carlos Affonso de Sousa sugere que para verificar o potencial lesivo de um incidente de segurança aos titulares, alguns fatores devem ser considerados. Em primeiro lugar, o tipo de incidente, a natureza, a sensibilidade e o volume dos dados pessoais comprometidos devem ser sopesados nessa equação.[33] O autor acrescenta ainda que, apesar do §2º do art. 48 da LGPD falar em "ampla divulgação do fato em meios de comunicação", é preciso ressaltar que essa medida não substitui a comunicação individual que deve ser direcionada aos titulares das informações.[34]

A comunicação de ocorrência de incidentes aos titulares é importante, não só por questões de transparência, mas também por dar poder ao titular para que possa tentar se preservar diante de possíveis ameaças. Nessa perspectiva, o EDPB esclarece que o objetivo principal da comunicação de incidentes consiste na prestação de informações específicas acerca das medidas que devem ser tomadas para que os titulares possam se proteger. Como observado acima, dependendo da natureza da violação e do risco que coloca, a comunicação no devido prazo irá ajudar as pessoas a tomarem medidas para se protegerem de quaisquer consequências negativas de uma violação.[35]

Considerações Finais

Diante de todo o exposto supra, é possível concluir que com as novas disposições sobre segurança da informação trazidas pela legislação pátria de proteção de dados, uma política nacional ou regulamento geral de segurança da informação parece ser um caminho coerente a fim de proporcionar aos controladores as diretrizes essenciais para que se garanta o mínimo de segurança exigido ao tratamento de dados que a LGPD preceitua.

É evidente que, em matéria de segurança da informação, muito ainda precisa ser ajustado, especialmente em razão de a LGPD ser menos detalhada em relação ao tema que o RGPD. Além dos requisitos mínimos de segurança, é importante que os regulamentos que

[32] A ANPD já deu início à regulamentação da matéria. Ver mais em "ANPD inicia processo de regulamentação sobre incidentes de segurança com tomada de subsídios." 22 de fev. de 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-inicia-processo-de-regulamentacao-sobre-incidentes-de-seguranca-com-tomada-de-subsidios>. Acesso em 22 de set. de 2021.
[33] SOUSA, Carlos Affonso Pereira de. Capítulo XV. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018 p. 435. In: TEMPEDINO, Gustavo. OLIVA, Milena. Lei Geral de Proteção de Dados e duas repercussões no Direito brasileiro. 2ª Edição. Thomson Reuters, Revista dos Tribunais, 2019.
[34] Ibid. p. 435.
[35] EUROPEAN DATA PROTECTION BOARD. *Guidelines on Personal data breach notification under Regulation* 2016/679. 2018. Disponível em < https://ec.europa.eu/newsroom/article29/items/612052/en >. Acesso em: 09 de set. de 2021. p. 21.

possam ser expedidos pela ANPD estimulem ainda mais a adoção de metodologias que aprimoram a privacidade como o *privacy by design* e *privacy by default*. A comunicação de incidentes de segurança é ponto igualmente importante e tem sua urgência de regulamentação, muito em razão de que se constitui de mecanismo que propicia ao titular de dados pessoais o poder de se auto proteger dos possíveis riscos envolvidos em um incidente, em especial quando se trata de vazamento de dados.

Tendo em vista a sua magnitude e sua extensão, o caso do vazamento de dados do Serasa é simbólico para a proteção de dados brasileira. Espera-se da ANPD uma apuração justa e correta dos fatos privilegiando a cooperação com os controladores envolvidos, mas sempre com enfoque na proteção dos titulares de dados. Nesta mesma linha, o Tribunal de Justiça de São Paulo no julgamento da Ação Civil Pública.

O caso Knudells é um caso interessante e significativo, especialmente quando se observa o nível de cooperação que se estabeleceu entre o controlador e a autoridade de controle. A cooperação é incentivada por vários dispositivos da LGPD, por conseguinte, o que se espera é que os controladores brasileiros ajam conjuntamente com a ANPD, não só para a solução de casos de incidente, mas também no sentido de contribuir para fortalecer a proteção de dados no Brasil.

O Brasil, acompanhando a tendência mundial, avançou na proteção de direitos e liberdades individuais com a LGPD. Todavia, será preciso aguardar para ver quais os contornos aos novos direitos e obrigações serão dados pela ANPD e pelos tribunais por meio de suas decisões.

Referências bibliográficas

ANPD. Comunicação de incidentes de segurança. 22 de fev. de 2021. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>, acesso em 09 de set. de 2021.

BIONI, Bruno Ricardo. Proteção de Dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 234.

BIONI, Bruno R.; MONTEIRO, Renato Leite. Proteção de Dados Pessoais Como Elemento de Inovação e Fomento à Economia: O impacto econômico de uma lei geral de dados pessoais. In: Proteção de dados: contexto, narrativas e elementos fundantes / [organização Bruno Ricardo Bioni]. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021

CAVOUKIAN, Ann. Privacy by Design: the 7 fundational Principles. Jan. de 2011. p. 1.

EUROPEAN DATA PROTECTION BOARD. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. 20 de out. 2020. Disponível em <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en>. Acesso em: 08 de set. de 2021.

EUROPEAN DATA PROTECTION BOARD. Guidelines on Personal data breach notification under Regulation 2016/679. Disponível em < https://ec.europa.eu/newsroom/article29/items/612052/en>. Acesso em: 09 de set. de 2021.

HINTZBERGEN, Jules. Fundamentos da Segurança da Informação: com base na ISO 27001 e na ISO 27002/Jule Hintzbergen... [et al]; tradução Alan de Sá - Rio de Janeiro: Brasport, 2018. P. 30.

JIMENE. Camilla do Vale. Capítulo VII: Da Segurança e das Boas Práticas. p.387. in: LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico] / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020.

MENDES, Laura Schetel. Segurança da Informação, Proteção de Dados Pessoais e Confiança. Revista de Direito do Consumidor, São Paulo, vol. 90, pp. 245-261, nov.-dez.2013.

MENKE, Fabiano. GOULART, Guilherme D. Segurança da Informação e vazamento de dados. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 347.

VENTURA, Felipe. Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava. Tecnoblog. Disponível em: <https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/amp/>. Acesso em 1 set. 2021

SOUSA, Carlos Affonso Pereira de. Capítulo XV. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018 p. 435. In: TEMPEDINO, Gustavo, OLIVA, Milena. Lei Geral de Proteção de Dados e suas repercussões no Direito brasileiro. 2ª Edição. Thomson Reuters, Revista dos Tribunais, 2019.

VOIGT, Paul. BUSSCHE, Axel. The EU General Data Protecion Regulation (GDPR): A Practical Guide. Berlim. Springer.2017. p. 40.

ENCARREGADO DE PROTEÇÃO DE DADOS & DATA PROTECTION OFFICER (DPO): UM ESTUDO À LUZ DAS (PRÉ) CONCEPÇÕES BRASILEIRAS E CONCEPÇÕES EUROPEIAS

Rafael Luís Müller Santos[1]

Dispositivo LGPD	Dispositivo RGPD
Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados	**Art. 37** (Designação do encarregado da proteção de dados). **Art. 37** (Posição do encarregado da proteção de dados). **Art. 37** (Funções do encarregado da proteção de dados).

[1] Graduando em Direito pela Universidade de Brasília (UnB). Assessor no Gabinete da Superintendência-Geral do Conselho Administrativo de Defesa Econômica (Cade). Co-organizador do Grupo de Estudos e Pesquisa em Jurisprudência e Constituição (GEPJuC). Integrante do Grupo de Estudos em Constituição, Empresa e Mercado (GECEM). Foi Editor-Gerente na Revista dos Estudantes de Direito da Universidade de Brasília (RED|UnB) e Gerente de Projetos na Advocatta (Empresa Júnior de Direito da UnB)..

Introdução

O presente artigo visa realizar uma análise geral dos panoramas e diretrizes estabelecidos para a regulamentação e concretização dos cargos relativos ao Encarregado de Proteção de Dados (Brasil) e ao *Data Protection Officer* (EU).

Nesse sentido, serão analisados os dispositivos da Lei Geral de Proteção de Dados (artigo 41) e do *General Data Protection Regulation* (artigos 37, 38 e 40). Diferentemente do cenário europeu, que se encontra com diversas balizas já discutidas e concretizadas, a Autoridade Nacional de Proteção de Dados (ANPD) ainda não estabeleceu diretrizes aprofundadas sobre a figura do encarregado.

Dessa forma, a previsão normativa e discussões travadas na academia em face às dúvidas levantadas pelo mercado ainda se fazem com um dos principais pontos para estudo e aplicação, a qual é necessária de imediato tendo em vista a vigência total da norma já ser uma realidade e a obrigação de as entidades públicas e privadas promoverem adequações.

1. Lei Geral de Proteção de Dados e Autoridade Nacional de Proteção de dados: panorama atual

Em primeira análise, é de extrema relevância mencionar que o artigo 41 da Lei Geral de Proteção de Dados, assim como outros artigos da lei, deixam diversos fatores em aberto, que seriam interpretados nos casos concretos e com base nas diretrizes que serão implementadas pela ANPD.

Como será abordado posteriormente nos termos do recente *paper* "O Papel do(a) Encarregado(a) conforme a Lei Geral de Proteção de Dados", a norma se fez a partir de um caráter consideravelmente lacônico. À primeira vista, o intérprete pode considerar que essa característica implica em grande imprevisibilidade e insegurança jurídica. Entretanto, diante da experiência e estudos europeus, a legislação de proteção de dados estrangeira, como um todo, demonstra um caráter extremamente rígido, que não abre espaço para adaptações concretas que muitas vezes se fazem necessárias.

A lei brasileira, ao deixar lacunas propositais que serão objeto de discussão e regulamentação pela autoridade de proteção de dados, permite uma flexibilidade para adaptação a depender do contexto da organização e uma melhor e mais efetiva proteção de dados no âmbito nacional.

Dessa forma, a norma brasileira é compreendida por cláusulas consideravelmente gerais. Essa criação se deve ao fato de o tema de proteção de dados, na lei, envolver diversas searas com realidades distintas; e, portanto, a necessidade de se postular diretrizes generalistas e permitir, além de análises caso a caso, a possibilidade de a ANPD regular assuntos específicos.

Nesse sentido, o momento inicial de recém-constituição em que a Autoridade se encontra representa alguns desafios para a cultura de proteção de dados no Brasil, tendo em vista que as organizações ainda apresentam muitas dúvidas em como se adequar à lei diante de suas diferentes realidades de aplicação.

Esse entendimento permanece válido quando se pensa no encarregado de proteção de dados. Dessa forma, apesar de as diretrizes e bases estarem bem consolidadas na Europa, esta não é uma realidade no Brasil. Nesse sentido, no presente artigo, serão abordadas as preconcepções que permeiam a figura do encarregado no aspecto nacional e as concepções europeias.

Vale ressaltar que o objetivo deste artigo, não é tão somente estabelecer semelhanças e diferenças entre as diretrizes nacionais e europeias, mas também analisar o contexto e cultura de proteção de dados em que estão inseridas. Dessa forma, convergências e divergências entre os dois dispositivos devem ser analisadas cuidadosamente, a fim de não proporcionar falsas perspectivas em relação à possibilidade de transferência de concepções internacionais ao Brasil, sem o devido olhar para a (consideravelmente diferente) realidade que se apresenta[2].

2. Encarregado de Proteção de Dados

O encarregado, diferentemente do controlador e operador, não é um agente de tratamento. É representado por uma figura responsável, em principal, por garantir a comunicação da organização com os titulares de dados e com a ANPD; e a conformidade dos agentes de tratamento à LGPD (promoção do *compliance*), que consiste na promoção da cultura de proteção de dados na organização.

Em dissonância com legislações internacionais que versam sobre proteção de dados, a LGPD não estabelece regras específicas em relação às circunstâncias necessárias para que o

[2] As balizas normativas devem ser analisadas com cuidado, para que não seja realizada transposição direta dos conceitos de outras jurisdições, o que nada adiantaria diante da realidade brasileira e suas singularidades.

controlador indique o encarregado. Dessa forma, entende-se que esse cargo, diante da falta de balizas de dispensa da ANPD (possibilidade prevista em lei), deve ser ocupado em todas as organizações que realizam tratamento de dados de pessoas físicas[3].

Nessa linha, o § 3º do art. 41, prevê que normativas futuras da ANPD poderão trazer hipóteses de dispensa da necessidade de indicação do encarregado, tendo como critérios objetivos a natureza, o porte da entidade ou o volume de operações de tratamento de dados. Nesse sentido, uma das diretrizes principais da minuta de resolução apresentada pela ANPD, para os agentes de tratamento de pequeno porte, refere-se à possibilidade de dispensa de indicação do Encarregado pelo Tratamento de Dados Pessoais, sendo necessária apenas a disponibilização de um canal de comunicação para uso do titular de dados.

Vale ressaltar que a indicação do DPO não é necessária apenas em entidades privadas, mas também por órgãos e entidades públicas. Não há previsão distintiva no que concerne no DPO ser pessoa jurídica ou física, interna ou externa à organização que realiza o tratamento. Há uma recomendação de contratação a partir de um ato formal, como um contrato de prestação de serviços ou um ato administrativo. Nesse processo de escolha, o controlador deve levar em consideração fatores como conhecimento do tema de proteção de dados e do tema de segurança da informação.

Apesar de a Lei não estabelecer diretrizes concretas mais aprofundadas, é visível que as atribuições exercidas no cargo devem ser realizadas com eficiência. Esse ponto é reforçado pelo Guia Orientativo para Definição dos Agentes de Tratamento de Dados Pessoais e do Encarregado da ANPD, que ressalta o DPO como ponto-chave de comunicação entre a organização e a ANPD e os titulares de dados. Nesse sentido, as entidades devem fomentar o fácil acesso ao contato com o Encarregado.

Na linha do estabelecido em relação ao tratamento de dados por parte de pequenos e médios negócios, será possível que a ANPD determine hipóteses de dispensa da necessidade de indicação do encarregado, considerando não apenas a natureza ou o porte das entidades, mas também o volume das operações de tratamento de dados da organização. Entretanto, reforça a

[3] Esse tema foi objeto de discussão no webinar “O Papel do Encarregado Conforme a LGPD", que será abordado mais à frente neste artigo.

recomendação de que, em termos de estruturação de programas de conformidade, exista um encarregado para a organização mesmo que esse não seja um requisito formal.[4]

3. Data Protection Officer

3.1. Considerações Iniciais

No documento *Guidelines on Data Protection Officers*[5], são apresentados aspectos mais detalhados da atuação do DPO, que irá tratar de diversas questões relacionadas à proteção de dados dos titulares. Nesse sentido, é possível observar a importância desses profissionais no contexto do GDPR, na promoção de políticas de compliance; e, assim, na prevenção de infrações que venham a ferir os direitos dos titulares; e também analisar as 5 principais diretivas que serão abordadas a seguir.

Vale ressaltar que a figura do DPO não é estranha ao cenário de proteção de dados europeu. Isso se deve pelo fato de que mesmo a Diretiva 95/46/EC não prevendo a necessidade de nomeação de um DPO, a prática se tornou comum.

3.2. Designação

A primeira diretiva consiste nos critérios relacionados à designação do DPO. Vale ressaltar, diferentemente do atual cenário brasileiro, que não serão todas as ocasiões em que o controlador deverá designar uma pessoa para o papel. No caso da previsão europeia, essa figura será essencial no cenário de todos órgãos e autoridades públicas, independentemente do processo de tratamento de dados que realizam; e outras organizações, a depender do tipo de tratamento implementado,[6] sendo estimulada a adoção voluntária[7] mesmo quando não há a obrigatoriedade.

---

[4] Nos casos em que não se tem a obrigatoriedade de nomeação do encarregado, seria disponibilizado apenas um meio de comunicação, que o titular possuiria com a entidade.

[5] Esse documento, de caráter instrutivo, tem como objetivo explorar os dispositivos do GDPR e a experiência prática europeia para auxiliar controladores e operadores a estarem em conformidade com a lei e a assistirem o DPO a cumprir seu importante papel.

[6] Caso a organização apresente em sua atividade monitoramento de indivíduos de uma forma sistemática ou em larga escala ou processe categorias especiais de dados pessoais em larga escala, a figura do DPO, em regra, será indispensável.

[7] O incentivo encontra-se no *Article 29 Data Protection Working Party* (‘WP29’), que representa uma entidade independente que abordava questões relacionadas à proteção de dados e da privacidade até a entrada em vigor do GDPR. Nessa linha, foi colocado que a figura do DPO, além de trazer mecanismos facilitadores de práticas de compliance, também representa uma vantagem competitiva em comparação a outras organizações, a partir do seu

O artigo 37 da norma europeia regula esse tema ao postular a necessidade de nomeação do DPO em três casos específicos:

> **(i)** Autoridades públicas[8] que processam dados;
>
> **(ii)** Organizações em que os agentes realizam o tratamento de dados de forma regular[9] e sistemática e em larga escala[10] e
>
> **(iii)** Organizações em que o tratamento é feito a partir de categorias especiais de dados pessoais ou dados relacionados a condenações criminais[11].

Dessa forma, é relevante notar que, como citado anteriormente, há um incentivo para a adoção voluntária[12] nas organizações. Nestas, os artigos aqui citados serão aplicados; e, por conseguinte, os parâmetros de designação, posição e competências serão aplicados da mesma maneira em comparação a casos de designação obrigatória.

3.3. Posição

O WP 29 explicita a previsão legal no que diz respeito à necessidade de o DPO estar a frente, desde os primórdios dos problemas envolvendo privacidade e proteção de dados. Nesse

papel intermediador e promotor de prestação de contas. Vale ressaltar que política de compliance, segundo o GDPR, é uma responsabilidade não do DPO, que apresenta um papel subsidiário, mas sim do controlador de dados.

[8] O GDPR não define com precisão no que consiste "*public authority or body*". Segundo o *Working Party* 29, essa é uma definição de jurisdição nacional.

[9] O GDPR não define esse conceito. Segundo o recital 24, "*regular and systematic monitoring*" consiste em todas as formas de rastreamento e perfilamento nos meios digitais. Em contrapartida, WP 29, expõe que esse conceito não estaria limitado ao ambiente online, além de explicar que a regularidade seria entendida por monitoramentos contínuos, constantes, em intervalos definidos por um período determinado ou recorrentes e repetidos em ocasiões determinadas. Já o entendimento da sistematicidade, estaria compreendido em tratamentos (i) baseados em um sistema; (ii) de realização pré-arranjada, organizada ou metódica; (iii) parte de um plano para coleta de dados ou (iv) que seja realizado como parte de uma estratégia.

[10] O GDPR não traz a definição desse conceito. O *recital 91* prevê, ainda que não de forma consideravelmente específica e não ideal, alguns parâmetros: *"Large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer".* Ademais, o WP 29 cita que a determinação do conceito "em larga escala" depende de 4 fatores principais: (i) *"The number of data subjects concerned - either as a specific number or as a proportion of the relevant population"* (ii) "*The volume of data and/or the range of different data items being processed*" (iii) "*The duration, or permanence, of the data processing activity*" (iv) "*The geographical extent of the processing activity*".

[11] Nesse entendimento, vale ressaltar que há um vício legislativo no que concerne ao fato de não ser necessário que ocorra a concepção de "*special categories of data*" (art. 9 GDPR) de forma conjunta com a concepção de "*data relating to criminal convictions and offences*" (art. 10 GDPR). É possível que se configure uma ou outra para que seja aplicado o critério de designação do DPO.

[12] Esta vai ao encontro, em destaque, do princípio da prestação de contas (*accountability*).

sentido, ele deve estar informado e possuir caráter participativo nos âmbitos da organização que envolvem os temas, de forma a preservar a horizontalidade do cargo.

3.4. Tarefas e Competências

Em primeiro lugar, é válido explicitar que tanto o GDPR quanto o "*Recital* 97" estabelecem o monitoramento[13] em compliance como uma tarefa de extrema relevância no papel de DPO, sendo que na segunda regulação há uma previsão ainda mais específica, no sentido de o DPO ter de auxiliar o controlador e o operador no monitoramento por meio desta.

Nesse sentido, serão tarefas do cargo em relação ao monitoramento:

> **(i)** coletar informações para identificar atividades correspondentes ao processamento de dados;
>
> **(ii)** analisar e checar o nível de conformidade do processamento de dados e
>
> **(iii)** informar, aconselhar e emitir recomendações para o controlador e o operador.

Em segundo lugar, apesar de ser competência privativa do controlador de dados, o DPO tem um relevante papel em auxiliar este na elaboração do relatório de impacto. Esse auxílio segue o ideário postulado no artigo 35 do GDPR, o qual expõe que o controlador deve buscar o aconselhamento do DPO; e no artigo 39, que estabelece, dentre as tarefas do DPO, a obrigação de fornecer recomendações[14] quando requisitadas.

Em terceiro lugar, vale ressaltar que o DPO tem o encargo de cooperar com a autoridade de proteção de dados, na medida em que fica responsável pela ponte de comunicação[15] com esta em casos de questões problemáticas no tratamento de dados ou em casos de necessidade consultiva.

---

[13] Apesar de ser taxado como uma tarefa do DPO, este não tem responsabilidade alguma em caso de verificação de não compliance. A responsabilização recairá apenas ao controlador de dados.

[14] O WP 29 indica que o controlador pode buscá-las nas seguintes situações: (i) avaliação da necessidade ou não da edição de um relatório de impacto; (ii) escolha da metodologia que será utilizada no relatório de impacto; (iii) realização interna ou terceirizada do relatório; (iv) adoção de (quais) medidas de segurança para mitigar riscos e proteger os interesses dos titulares e (v) avaliação dos resultados do relatório de impacto (nível de compliance) e adoção de medidas práticas de mudança ou continuação (meios de processamento de dados e medidas de segurança).

[15] O WP 29 reforça o papel facilitador que o profissional apresenta, tendo em vista que será por meio dele que a autoridade terá acesso com maior facilidade aos documentos e informações necessárias para se compreender o processo de tratamento de dados de determinada organização ou entidade.

Nesse sentido, também é necessário citar a necessidade de o DPO adotar uma abordagem baseada em risco, "levando em consideração a natureza, escopo, contexto e finalidades do tratamento de dados". Essa competência faz referência ao fato de o cargo exigir uma ponderação e priorização[16] entre atividades a depender do nível de risco à proteção de dados.

Por fim, apesar de a manutenção de registros de operações de tratamento ser competência e responsabilidade exclusivas do controlador e do operador de dados, o DPO apresenta relevante papel no aspecto prático desta. Isso se deve ao fato de os DPOs receberem diversos comunicados sobre operações de tratamento de dados, mantendo essas informações documentadas.

4. Convergências, Divergências e Debates Recentes

Faz-se necessário entender que, apesar de na maioria das ocasiões serem tratados como sinônimos, o Encarregado de Proteção de Dados, previsto na Lei Geral de Proteção de Dados, e o Data Protection Officer (DPO), previsto no General Data Protection Regulation (GDPR), são figuras que apresentam diferenças relevantes. Esta diferenciação é de extrema relevância, pois, apesar de representarem cargos equivalentes com algumas funções semelhantes, possuem diretrizes consideravelmente diferentes, que serão abordadas a seguir.

A previsão normativa do art. 41 da LGPD indica competências de caráter reativo por parte do encarregado. Isso se deve, em primeiro lugar, ao fato de o titular de dados ter que realizar a ação em provocação à atividade do encarregado, para que esse reaja (fornecer respostas frente às dúvidas e reclamações em relação ao tratamento de dados). Nesse mesmo sentido, também é posto que o encarregado é responsável por receber as comunicações realizadas por parte da Autoridade Nacional e tomar providências a partir deste fato.

Em contrapartida, os dispositivos do GDPR preveem uma postura proativa e colaborativa do DPO. Este fato pode ser observado nas previsões de necessidade de colaboração com a *Data Protection Authority* (DPA), possibilitando a realização de consultas perante a autoridade.

[16] Dessa forma, o DPO poderá auxiliar o controlador de forma mais eficiente. Em principal, no que concerne a escolha da metodologia que será utilizada no relatório de impacto; análise das áreas que serão objeto de auditoria interna ou externa; análise de treinamentos efetivos para serem fornecidos para funcionários e administração; e análise de quais atividades de processamento demandam mais tempo e atenção do controlador.

Em 14 de Dezembro de 2021, o CEDIS-IDP[1] e CIPL[2] promoveram o webinar[3] sobre "O Papel do Encarregado Conforme a LGPD", no qual lançaram o relatório em conjunto sobre o tema, que possui um caráter orientativo essencial no cenário de diretrizes ainda não desenhadas pela ANPD[4] e promoveram uma interessante discussão com diferentes visões especialistas discutindo as principais questões do tema.

Em primeiro lugar, Bojana Mellany abriu o debate ressaltando que o Encarregado de Proteção de Dados apresenta um papel fundamental na promoção de *accountability* e adequação das organizações, tendo em vista que é a pessoa responsável por elevar o nível de proteção destas. Esse ponto também é exposto nas considerações iniciais do relatório mencionado, no que concerne a menção do papel do encarregado:

> "supervisionar a implementação do programa de governança em privacidade de dados, traduzir as obrigações legais em ações concretas, documentar as atividades e decisões de tratamento de dados e treinar pessoal relevante como parte do programa de governança".

A jurista reforçou que não se trata do mesmo papel positivado pelo GDPR (DPO), já que a LGPD apresenta estruturas normativas consideravelmente mais flexíveis para as futuras orientações suplementares da Autoridade Nacional de Proteção de Dados.

Também foi comentada a atribuição do cargo no que concerne ao fato de ser necessário estar de acordo com a realidade e características de cada entidade (interessante congruência a maior flexibilidade proposta pelo texto legal) e também voltado a resultados, ao garantir a promoção de programas de *compliance*, de gestão e privacidade, ponto de contato e incentivos à proteção de dados. Nesse sentido, também foram expostas as incertezas em relação ao fato de esse papel ser público, externo ou interno e como a lei será aplicada.

Em seguida, a Professora Laura Schertel fez importantes considerações no que tange à preocupação com a efetiva aplicabilidade da LGPD e que na sua vigência faça sentido de

[1] Centro de Direito Internet e Sociedade do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa.
[2] Centre for Information Policy Leadership.
[3] O evento contou com a participação de nomes relevantes na área: Laura Schertel (CEDIS-IDP); Danilo Doneda (CEDIS-IDP); Bojana Bellamy (CIPL); Vivienne Artz Obe (CIPL); Miriam Wimmer (ANPD); Ricardo Dalmaso Marques (Meta); Gabriela Freitas (Sansung); Andrea Mattos (Telefônica Brasil); Flávia Mitri (Uber) e Vanessa Butalla (2TM).
[4] O relatório realiza uma série de recomendações à Autoridade Nacional de Proteção de Dados, a fim de proporcionar um respaldo acadêmico para que esta regulamente de forma complementar os dispositivos legais que dizem respeito ao papel do encarregado.

forma que todos possam entender e seguir o texto normativo. Nessa linha, a jurista cita uma passagem do de *law on the books* para *law on the ground*, a fim de se discutir quais são os desafios concretos[5] para a eficácia da lei. A discussão prática travada depende de forma substancial do encarregado, que apresenta um papel essencial nas questões de *accountability* e adequação, além da criação de uma cultura de proteção de dados[6].

A professora também citou que a lei traz dispositivos e normas importantes (guia para as empresas) com mais flexibilidade que pode ser aproveitada, tendo em vista que o legislador trouxe maior espaço de interpretação e aplicação, em contraponto com o cenário mais rígido da legislação europeia[7]. Dessa forma, há a possibilidade para que empresas adequem o papel do encarregado de uma forma mais conexa com a realidade e a estrutura da entidade.

Ademais, foi levantado que a profissão do encarregado se faz muito interessante e visada, tendo em vista seu caráter horizontal, em que há um contato com todas as áreas da empresa, pois há questões relacionadas à privacidade e proteção de dados em todos os âmbitos da organização[8].

Miriam Wimmer, não por meio de manifestação formal da ANPD[9], mas mediante percepções próprias, afirmou que, ao analisar o contexto em que o legislador configurou o encarregado, este se faz muito presente em questões relacionadas à *accountability*, em que haja um profissional especializado não apenas para a formação de um ponto de contato, mas também para promoção de uma mudança cultural no interior da organização.

A jurista também reforça o caráter lacônico da legislação nas atribuições do encarregado, ao defini-lo como canal de comunicação entre o controlador e o titular de dados e a ANPD. Esta é uma designação consideravelmente mais restrita e simplista, como é possível comparar nas previsões do GDPR, levando a necessidade de sinalização de diretrizes de interpretação, as quais, em suas lacunas atuais, geram certa insegurança para as organizações,

[5] A discussão sobre os impactos práticos para a aplicação da LGPD é uma diretriz para o projeto "LGPD Efetiva", no qual o paper mencionado está inserido.
[6] A LGPD tem sido cada vez mais aplicada pelo judiciário, mas ainda se faz necessária a criação de uma cultura de proteção de dados mais consolidada no Brasil, que deve ser compartilhada entre empresas, poder público e cidadãos.
[7] Apesar da clara inspiração europeia presente na LGPD, em diversos artigos e temas, o legislador optou por uma maior flexibilidade de interpretação, o que leva ao importante papel da ANPD no auxílio para a efetivação da lei.
[8] As organizações devem se preocupar a empresa deve se preocupar tanto com os dados externos (clientes e leads), quanto internos (dos funcionários, RH e afins), isso ajudaria a delinear o porquê de afetar todas as áreas da empresa.
[9] A ANPD não se manifestou formalmente sobre os aspectos pormenorizados do Encarregado de Proteção de Dados. O tema está contido na agenda regulatória do primeiro semestre de 2022, nos termos da Portaria nº 11/2021.

as quais, por outro lado, geram alta capacidade de adaptação e flexibilidade (levar em consideração o contexto da organização) pretendida na redação da norma.

O papel do encarregado está muito associado à visão que se tem da LGPD. É uma lei pró-inovação e pró-crescimento econômico. Em políticas de compliance, se criou programas específicos para a LGPD, que levam em consideração as diferenças entre as competências dos encarregados e as dos DPOs. Dessa forma, desde 2020, foram estabelecidos diversos canais para contato com DPO, para que sejam atendidos os direitos dos titulares de dados.

Disso se depreende que o Encarregado apresenta cinco competências[10] principais:

> **(i)** apresentar e implementar um programa de *compliance* e privacidade (treinamentos, controle e governança[11]);
>
> **(ii)** desenvolver fluxos internos necessários para a possibilitação da redação de documentos de prestações de contas (*accountability documents*);
>
> **(iii)** aconselhar o operador sobre as formas de cumprimento da norma;
>
> **(iv)** atuar como ponto de contato com os reguladores (ANPD) e
>
> **(v)** atuar como ponto de contato com os titulares de dados (não apenas os usuários externos, mas também titulares da empresa).

As competências do Encarregado no contexto brasileiro, ao se observar em um quadro comparativo[12] citado no referido relatório, apresenta uma considerável simplicidade na definição de tarefas. Dessa forma, diferentemente de países como Colômbia, Austrália, Egito e Coreia do Sul, que possuem uma quantidade consideravelmente maior de competências elencadas, o Brasil opta por essa regulação geral.

---

[10] As organizações, a depender do contexto interno e demanda, poderão atribuir outras competências para o encarregado. O relatório cita possibilidades como: "manter registro das operações de tratamento de dados pessoais; realizar ou supervisionar avaliações de risco de privacidade de dados; identificar as bases legais aplicáveis ao tratamento de dados; redigir notificações a titulares sobre o tratamento de dados; participar na resposta e na gestão de incidentes de segurança; realizar ou participar de auditorias; elaborar políticas, processos, controles e modelos internos; redigir/negociar contratos de proteção de dados; oferecer treinamento e planejar atividades de conscientização; atuar como facilitador, ou responsável, do programa de governança em privacidade; supervisionar a implementação de políticas internas e processos relacionados à privacidade de dados; envolver-se nas principais avaliações de risco de privacidade de dados; acompanhar desenvolvimentos nacionais e globais em privacidade de dados e envolver-se externamente em questões de proteção de dados".

[11] Nesse sentido, o relatório expõe: "O encarregado deve ter um papel estratégico como assessor de confiança, trabalhando em parceria com a liderança da organização e cooperando com a empresa na privacidade de dados, mas possivelmente também de forma mais ampla em todos os assuntos relacionados a dados ou ao meio digital." O programa de governança apresenta benefícios internos, no que concerne ao envolvimento dos colaboradores das organizações; e benefícios internos, no que concerne a maior confiabilidade que é repassada para os clientes.

[12] Data Protection Officer Requirements by Country (Requisitos para encarregados por país) da IAPP

Nesse sentido, vale ressaltar que a escolha e implementação do cargo deve levar em consideração fatores como: experiência na área de proteção de dados e experiência no modelo de negócio da organização (possibilitar a efetiva assessoria especializada à empresa); autoridade nos âmbitos gerais da organização (possibilitar a real influência na cultura de proteção de dados); posicionamento na organização (independente ou vinculado à outra área interna); posicionamento geográfico (nacional ou internacional, desde que atenda às demandas e competências da mesma forma e haja a promoção da comunicação em língua portuguesa); envolvimento em questões de privacidade (busca por conhecimento interno da organização e dos estudos relacionados ao tema); habilidades e qualificações (liderança, comunicação, análise e proatividade); recursos ofertados pela organização (possibilitar o trabalho); equipe de suporte (colaboradores devem estar habilitados a exercer as mesmas competências que o encarregado).

A flexibilidade[13] mencionada anteriormente auxilia a adaptação prática dessas atribuições, a depender do contexto e particularidades organizacionais. De modo geral, há uma necessidade de se encontrar um ponto de equilíbrio entre a possibilidade de execução da atividade econômica (propósito) da organização e ao mesmo tempo observar e prezar pelos direitos dos titulares. Portanto, deve-se compreender que é o caso de um cargo que busca equilíbrio entre os interesses da empresa e os direitos dos consumidores, sendo que é importante trazer, para a organização, as perspectivas do indivíduo que é afetado pela atividade.

O cargo descrito possui um papel importante no que concerne a postura de colaboração, incentivando o estímulo para uma maior obtenção informações da organização; e, assim, maior conhecimento dos riscos relevantes e melhores condições de estruturação de soluções e orientações de acordo com as Lei e as melhores práticas (efetiva implementação da proteção dos dados pessoais). Portanto, além da necessidade de o encarregado estar conectado internamente, ele também deve estar atento aos acontecimentos no mercado em que atua, em outros mercados, nas autoridades, discussões, congressos e seminários, além de buscar melhores práticas mencionadas para aprimorar seu programa de forma permanente e eficaz.

Seguindo essa linha, é retomada a importância do papel do encarregado na promoção de uma cultura de proteção de dados e privacidade. Esta se faz de tamanha relevância, tendo

[13] Nos termos do relatório, o encarregado "não desempenha uma função estática e igual em todas as circunstâncias e que as organizações têm flexibilidade para definir as atribuições do encarregado que melhor atendam a seus negócios e atividades de tratamento de dados (desde que estejam em conformidade com as normas da LGPD)".

em vista que, a partir de uma mudança de cultura, há uma perpetuação do tema na companhia e nas ações cotidianas dos colaboradores. Ademais, em relação a *accountability*, é necessário que a cultura inclua os cargos da alta administração da organização, se for o contexto em questão. Faz-se necessário, por exemplo, que sejam levadas questões relacionadas à privacidade para o conselho de administração, na forma de um conselho de auditoria e controle.

Nessa linha, também é válido mencionar a relevância que o encarregado possui para a manutenção e aprimoração da responsabilidade ética organizacional, como abordado no relatório. Essa apresenta um caráter de ação proativo e preventivo por parte do encarregado, o qual deve trabalhar para mitigar riscos nas atividades relacionadas ao tratamento de dados, planejando, implementando e supervisionando o programa de governança em privacidade, além de ser capaz de demonstrar a eficácia desse trabalho.

O relatório, assim como os convidados no webinar, levantam uma série de questões que representam as principais dúvidas e incertezas do mercado, as quais ainda dependem de uma regulamentação da ANPD de forma efetiva:

> **(i)** Possibilidade de isenção de nomeação do encarregado;
>
> **(ii)** Obrigação (ou não) de os operadores designarem um encarregado;
>
> **(iii)** Encarregado é representado por pessoa física ou por departamento com a mesma finalidade;
>
> **(iv)** Cargo pode (ou não) ser desempenhado por pessoa externa à organização;
>
> **(v)** Autonomia e questões relacionadas ao conflito de interesses;
>
> **(vi)** Responsabilidade pessoal (ou não) pelo descumprimenro da lei[14]
>
> **(vii)** Necessidade de divulgação pública da identidade do encarregado e suas informações de contato

Diante desse considerável cenário de dúvidas, vale ressaltar alguns pontos importantes. Em primeiro, nota-se que a indicação do encarregado é mandatória[15] na LGPD. Entretanto, a

[14] Além disso, também há uma discussão muito presente em relação à responsabilização do encarregado perante não à LGPD, mas a outros tipos de normas legais.
[15] Concepçãoque vai de encontro com o GDPR, tendo em vista que, na previsão deste, apenas algumas organizações que essencialmente realizam atividades de maior risco são obrigadas a indicar o encarregado.

norma abre a possibilidade de que a ANPD[16] regule o tópico, de forma a poder autorizar a dispensa da indicação em certos contextos e organizações.

Vale mencionar, que em um futuro que haja possibilidades (exceção à regra) de dispensa[17], as competências do encarregado deverão ser exercidas, mesmo que de uma forma geral, para garantir efetiva a proteção do direito dos titulares. A Autoridade deve indicar, nesses casos, quais outros mecanismos efetivos deverão ser implantados para assegurar que, ainda sem a representação do encarregado em si, o titular de dados tenha canais para poder exercer seus direitos e não seja prejudicado.

Há também a dúvida em relação à possibilidade de o encarregado estar em um departamento da organização, em que haveria uma pulverização de responsabilidades. Essa reflexão também leva a questões relativas ao conflito de interesses e acúmulo de obrigações.

É notória também, em relação ao conflito de interesses, a questão da independência do encarregado. A LGPD, diferente do GDPR[18], não requer que o encarregado seja independente, sendo que, dentre as divergências de atribuições, o encarregado é um cargo um pouco mais diluído.

Entretanto, no webinar foi levantada a questão que, diante do contexto de o encarregado ser um fiscal para proteção de dados dentro da empresa, ter um poder efetivo de fiscalização e da necessidade de ter ingerência em relação à liderança da organização, deve-se pensar em conflito de interesses, que pode ocorrer a depender da alocação do encarregado. Portanto, a organização deve trabalhar em formas de como blindar a posição dentro do departamento que ele ocupa.

É possível citar também, que um dos maiores desafios de caráter prático para a implementação do encarregado, é a experiência em casos nos quais os titulares de dados recorrem ao cargo para todo e qualquer assunto. Assim, é gerada uma considerável dificuldade de resposta por parte das empresas.

---

[16] No webinar, foi levantado o importante ponto no que concerne a necessidade, por parte da ANPD, definir critérios para estipular quando há ou não necessidade de indicar um encarregado, quais são as hipóteses de exceção, de que maneira pode-se trabalhar o conceito de risco e não só o conceito de porte econômico da empresa para definir necessidade de designação.

[17] Essa questão começou a ser endereçada na minuta de regulação dos agentes de pequeno porte divulgada pela ANPD. Entretanto, ainda se faz necessário detalhar as situações "*must have*" e "*nice to have*".

[18] Nos termos do WP 29, "given the size and structure of the organization, it may be necessary to set up a DPO team (a DPO and his/her staff). In such cases, the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up. Similarly, when the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the tasks of a DPO as a team, under the responsibility of a designated lead contact for the client."

Considerações finais

Em suma, no futuro próximo, ainda será necessário muito estudo e aprimoramento quando se pensa no encarregado e no seu papel fundamental na proteção de dados nas organizações e na sociedade em um plano geral. Esse deve ser feito com demasiada cautela, a fim de não se incorrer em interpretações ou importações vazias de conceitos e características estrangeiras, sem a devida contextualização do cenário brasileiro que se faz muito peculiar.

A ANPD terá um papel crucial nos próximos meses a definir as diretivas com a finalidade de regulamentar o papel do encarregado, com o cuidado de, ao mesmo tempo, ir ao encontro da flexibilidade e amplitude que a lei tem como finalidade, e também de não proporcionar lacunas excessivas e, portanto, dúvidas, que os mercados não possam solucionar.

Como foi levantado no webinar, ainda é uma área nova e em implementação no Brasil. As organizações, aos poucos, começam a lidar com programas de proteção de dados e privacidade no seu cotidiano e ainda é necessário que as pessoas entendam o assunto e se habituem, fato que leva a importância do papel do encarregado.

Diante da grande dimensão do tema, tendo em vista que um estudo da IAPP (*International Association of Privacy Professionals*) prevê a necessidade de preenchimento de cinquenta mil cargos de encarregados de proteção de dados, espera-se que as discussões envolvendo o tema sejam cada vez mais ricas.

Referências bibliográficas

Centre for Information Policy Leadership (CIPL) e Centro de Direito, Internet e Sociedade do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (CEDIS-IDP). *Artigo 3 do Projeto Conjunto LGPD Efetiva. O Papel do/a Encarregado/a conforme a Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em < https://www.idp.edu.br/o-papel-do-a-encarregado-a-conforme-a-lei-geral-de-protecao-de-dados-pessoais-lgpd/>. Acesso em 14 de dezembro de 2021.

Article 29 Data Protection Working Party ('WP29'): *Guidelines on Data Protection Officers ('DPOs')*. Disponível em: <https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A>. Acesso em 2 de dezembro de 2021.

DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. Disponível em: Minha Biblioteca UnB. Acesso em 20 de novembro de 2021.

Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_at

o2015-2018/2018/lei/l13709.htm>. Acesso em 20 de novembro de 2021.

Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definição dos Agentes de Tratamento de Dados Pessoais e do Encarregado da ANPD. Dispível em <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf>. Acesso em 25 de novembro de 2021.

Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=EN>. Acesso em 30 de Novembro de 2021.

General Data Protection Regulation (GDPR). Disponível em <https://gdpr-info.eu/>. Acesso em 20 de novembro de 2021.

Webinar "O Papel do Encarregado Conforme a LGPD". Disponível em: <https://m.youtube.com/watch?v=sEKBLJp1XYk&utm_campaign=CIPL&utm_medium=email&_hsmi=200280202&_hsenc=p2ANqtz-8ZGQ0bZgQ0z59ZjJYNItj--qVM98UsGmbyQrzCXKqC11ZkcsbYSRN7E82hto_a3PSEE_siEbaJp-WjL8bAiDNneS6F3N5EF7ariwpQ3ZZFxa99E64&utm_content=200280202&utm_source=hs_email>. Acesso em 20 de janeiro de 2022.

Portaria nº 11/2021 da ANPD. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>. Acesso em 20 de dezembro de 2021.

Data Protection Officer Requirements by Country (Requisitos para encarregados por país) da IAPP. Disponível em: <https://iapp.org/resources/article/data-protection-officer-requirements-by-country/>. Acesso em 20 de janeiro de 2022.

International Association of Privacy Professionals (IAPP). *Study: LGPD likely to require at least 50K DPOs in Brazil alone*. Disponível em: <https://iapp.org/news/a/study-lgpd-likely-to-require-at-least-50000-dpos-in-brazil-alone/>. Acesso em 20 de Janeiro de 2022.

International Association of Privacy Professionals (IAPP). Brazil's DPO dilemma: How and who to choose?. Disponível em: <https://iapp.org/news/a/brazils-dpo-dilemma-how-and-who-to-choose/>. Acesso em 20 de janeiro de 2022.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS COMO INSTRUMENTO ÚTIL DE ADEQUAÇÃO E GOVERNANÇA CONFORME A LGPD E O RGPD

Wanessa Larissa Silva de Araújo[1]

Dispositivo LGPD	Dispositivo RGPD
Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: §3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. **Art. 5º** Para os fins desta Lei, considera-se: XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; **Art. 10.** O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: **§ 3º** A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial. **Art. 32**. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público. **Art. 38**. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais,	**Artigo 35** – Avaliação de impacto sobre a proteção de dados 1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação. 2. Ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento solicita o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado. 3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o nº 1 é obrigatória nomeadamente em caso de: [...] 4. A autoridade de controle elabora e torna pública uma lista dos tipos de operações de tratamento sujeitas ao requisito de avaliação de impacto sobre a proteção de dados por força do nº 1. A autoridade de controle comunicou essas listas ao Comitê referido no artigo 68.o. 5. A autoridade de controle pode também elaborar e tornar pública uma lista dos tipos de operações de tratamento em relação aos quais não é obrigatória uma análise de impacto sobre a proteção de dados. A autoridade de controle comunica essas listas ao Comité. 6. Antes de adotar as listas a que se referem os nº 4 e 5, a autoridade de controlo competente aplica o

[1] Bacharela em Direito na Universidade de Brasília (UnB). Integrante do Observatório da LGPD da Universidade de Brasília.

inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. **Parágrafo único.** Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, 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. **Art. 55-J.** Compete à ANPD: XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;	procedimento de controlo da coerência referido no artigo 63. sempre que essas listas enunciem atividades de tratamento relacionadas com a oferta de bens ou serviços a titulares de dados ou com o controlo do seu comportamento em diversos Estados-Membros, ou possam afetar substancialmente a livre circulação de dados pessoais na União. 7. A avaliação inclui, pelo menos [...]: 8. Ao avaliar o impacto das operações de tratamento efetuadas pelos responsáveis pelo tratamento ou pelos subcontratantes, em especial para efeitos de uma avaliação de impacto sobre a proteção de dados, é tido na devida conta o cumprimento dos códigos de conduta aprovados a que se refere o artigo 40 por parte desses responsáveis ou subcontratantes. 9. Se for adequado, o responsável pelo tratamento solicita a opinião dos titulares de dados ou dos seus representantes sobre o tratamento previsto, sem prejuízo da defesa dos interesses comerciais ou públicos ou da segurança das operações de tratamento. 10. Se o tratamento efetuado por força do artigo 6º, nº 1, alínea c) ou e), tiver por fundamento jurídico o direito da União ou do Estado-Membro a que o responsável pelo tratamento está sujeito, e esse direito regular a operação ou as operações de tratamento específicas em questão, e se já tiver sido realizada uma avaliação de impacto sobre a proteção de dados no âmbito de uma avaliação de impacto geral no contexto da adoção desse fundamento jurídico, não são aplicáveis os nº 1 a 7, salvo se os Estados-Membros considerarem necessário proceder a essa avaliação antes das atividades de tratamento. 11. Se necessário, o responsável pelo tratamento procede a um controle para avaliar se o tratamento é realizado em conformidade com a avaliação de impacto sobre a proteção de dados, pelo menos quando haja uma alteração dos riscos que as operações de tratamento representam. **Artigo 36 - Consulta prévia.** **Considerandos** (74) Responsabilidade do Controlador; (75) Riscos para os direitos e liberdades das pessoas singulares;

	(76) Avaliação de Risco; (77) Diretrizes de Avaliação de Risco; (84) Avaliação de Risco e Avaliação de Impacto; (89) Eliminação do Requisito Geral de Relatórios; (90) Avaliação do Impacto à Proteção de Dados; (91) Necessidade de uma Avaliação do Impacto à Proteção de Dados; (92) Avaliação mais ampla do Impacto à Proteção de Dados; (93) Avaliação do Impacto da Proteção de Dados nas Autoridades; (94) Consulta à Autoridade Supervisora; (95) Apoio do Operador; (96) Consulta da Autoridade Supervisora no Curso de um Processo Legislativo.

Introdução

Este artigo, mediante análise comparativa dos arcabouços legais de proteção de dados pessoais brasileiro e europeu, parte de uma investigação bibliográfica acerca do Relatório de Impacto à Proteção de Dados Pessoais. Nesse sentido, o objetivo da pesquisa é evidenciar as correspondências referentes ao Relatório de Impacto, considerando elementos comuns entre tais legislações.

A Lei n° 13.709, de 2018, também conhecida como a Lei Geral de Proteção de Dados (LGPD) é fortemente inspirada na *General Data Protection Regulation*, também conhecida como Regulamento Geral sobre a Proteção de Dados – RGPD. Ambas as legislações preveem a necessidade da elaboração de um Relatório de Impacto à Proteção de Dados (RIPD), no contexto brasileiro; e de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD)[2], no contexto europeu.

O Relatório de Impacto é considerado como uma documentação do controlador[3]. Diante disso, o caráter instrumental dos relatórios de impacto pode ser evidenciado pelos elementos

[2] Traduzido oficialmente do inglês: "*Data Protection Impact Assessment (DPIA)*".

[3] No contexto brasileiro, o controlador é definido como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (art. 5º, inciso VI, LGPD). Já no contexto europeu, o controlador é definido como "responsável pelo tratamento, a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios

comparativos entre a LGPD e o RGPD: competência, definição, contexto e conteúdo. Nesse ínterim, será analisada a decisão do Supremo Tribunal Federal (STF) que suspendeu a MP 954/2020, cuja previsão estabelecia a elaboração e divulgação do Relatório de Impacto à Proteção de Dados, após a realização do compartilhamento dos dados pessoais.

1. Brasil x União Europeia (UE)

1.1. Lei Geral de Proteção de Dados - LGPD

A LGPD prevê que o Relatório de Impacto à Proteção de Dados (RIPD) é a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (art. 5º, XVII).

Vale mencionar que compete à Autoridade Nacional de Proteção de Dados (ANPD) editar regulamentos e procedimentos sobre o Relatório de Impacto, para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD (art. 55-J, XIII). Por isso, no contexto brasileiro, a análise do objeto desse artigo enfatiza os dispositivos da LGPD, uma vez que o processo de regulamentação sobre o tema está sendo desenvolvido.

O art. 5º, XVII, da LGPD, resume três aspectos importantes do RIPD: (i) definição, (ii) contexto e (iii) conteúdo em que se deve produzi-lo. Nesse sentido, o objeto desta pesquisa será analisado por meio desses três aspectos previstos pela LGPD, os quais também serão considerados na comparação com o RGPD, a fim de observar o relatório de impacto como instrumento útil de adequação e governança.

1.2. Regulamento Geral sobre a Proteção de Dados - RGPD

O Relatório de Impacto, Avaliação de Impacto sobre a Proteção de Dados (AIPD), exigido pelo RGPD, procede de outros exemplos europeus de relatórios de impacto, bem como o exemplo previsto na Diretiva nº 95/46/EC, antiga legislação geral de proteção de dados europeu. Diante da inspiração da Diretiva no relatório de impacto previsto na legislação

específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro" (art. 4º, nº 7, RGPD).

ambiental europeia, pode-se considerar que tal instrumento está intimamente associado a uma perspectiva de risco que envolve identificação, mitigação e prevenção de riscos ao meio ambiente e aos indivíduos que possam ser afetados (GOMES, 2019, p.8).

Nesse sentido, o Regulamento Europeu apresenta o Relatório de Impacto como um instrumento de apoio à tomada de decisão em relação ao tratamento de dados suscetível a um elevado risco para os direitos e liberdades dos titulares. É uma ferramenta que visa gerir os riscos para os direitos dos titulares dos dados e, como tal, avaliá-los na perspetiva destes últimos (ARTIGO 29, 2019, p.21).

A legislação de proteção de dados na União Europeia (UE) prevê sobre o Relatório de Impacto nos artigos 35 e 36 e nos Considerandos 75-77, 84, 89-92, 94-95. Conforme a análise comparativa com a legislação brasileira, pode-se considerar que o RGPD, em relação ao Relatório de Impacto, prevê sobre a quem compete procedimentalizar a sua realização (arts. 35, nº 4, 5, 6 e 51); a sua definição (art. 35, nº 1); o contexto geral e específico de situações que obrigam a sua elaboração (art. 35, nº 1, 3-4); o seu conteúdo (art. 35, nº 7), dentre outras previsões exclusivas no regulamento europeu (arts. 35, nº 2, 8, 9, 10, 11 e 36).

2. Elementos comparativos entre LGPD x RGPD

2.1. Competência das Autoridades de Proteção de Dados

2.1.1. Competência da Autoridade Nacional de Proteção de Dados (ANPD)

Em relação ao Relatório de Impacto, à Autoridade Nacional de Proteção de Dados (ANPD) compete solicitar o RIPD ao controlador de dados pessoais (arts. 4º, §3º; 10, §3º; 32, LGPD). Além disso, é expressamente previsto a competência da Autoridade poder editar regulamentos e procedimentos sobre relatórios de impacto (art. 55-J, XI).

Em janeiro de 2021, foi publicada a agenda regulatória da autoridade brasileira para o biênio 2021-2022. Nesse contexto, o início do processo regulatório do RIPD foi previsto para o mês de setembro de 2021. No mês de junho, a ANPD organizou três reuniões técnicas para discutir sobre a matéria, tais reuniões compreendem parte do processo da regulamentação do RIPD a ser produzida pela Autoridade, por meio da realização de consulta e audiência pública (GARROTE; PASCHOALI; MEIRA; BIONI, 2021).

O cronograma[4] das reuniões técnicas foi dividido em três blocos temáticos: (i) metodologias e critérios para elaboração e análise do Relatório de Impacto, discussão entre a possibilidade de disponibilizar *checklist* ou *template*; (ii) situações/circunstâncias que ensejam a necessidade ou dispensa de elaboração de Relatório de Impacto; (iii) transparência e publicidade dos Relatórios de Impacto para o setor público e o setor privado.

Os expositores da reunião técnica convergiram em direção à interpretação de que a LGPD propõe uma abordagem baseada em riscos. Nesse sentido, foi considerado que os relatórios de impacto são ferramentas relacionadas à avaliação e gerenciamento de risco, sendo fundamental dispensar a correlação entre porte do controlador com nível de risco do tratamento, pois a natureza do processo de tratamento de dados em questão deve ser o critério principal a ser observado para definir a necessidade da elaboração do relatório de impacto em cada caso concreto. Evidencia-se, portanto, a possibilidade da regulamentação brasileira seguir os passos europeus (GARROTE; PASCHOALI; MEIRA; BIONI, 2021).

2.1.2. Competência das Autoridades da União Europeia

O RGPD estabelece que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da sua aplicação, a fim de defender os direitos e liberdades fundamentais dos titulares relativamente ao tratamento e facilitar a livre circulação desses dados na União (art. 51).

Em relação ao Relatório de Impacto, vale considerar a importância do Grupo de Trabalho do Artigo 29º (WP29)[5], atual Comitê Europeu para Proteção de Dados (CEPD). O Grupo de Trabalho, em 2017, publicou[6] diretrizes e esclarecimentos sobre o tema por meio da publicação do "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD)

[4] O cronograma oficial pode ser consultado no site da ANPD. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-cronograma-completo-de-reunioes-tecnicas-sobre-relatorio-de-impacto-a-protecao-dos-dados-pessoais>.

[5] Grupo de trabalho formado pelas Autoridades de Proteção de dados na UE (*Data Protection Authorities "DPA"* ou *Supervision Authorities*) e que atuou até 2016, quando o Comitê Europeu para a Proteção de Dados - CEPD (*European Data Protection Board - EDPB*) assumiu essa função.

[6] Tal publicação do WP29 foi incorporada pelo EDPB, em 2018. Disponível em: https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf. Acesso em: 18 out. de 2021.

e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679"[7].

Nesse sentido, convém considerar que o processo de regulamentação europeu apresenta um nível elevado de consistência, tendo em vista que se trata de um regulamento aprovado em 2016 e vigente desde 2018. Nesse sentido, o procedimentalismo estabelecido pelas autoridades, bem como os efeitos de algumas regulamentações sobre o Relatório de Impacto, serão abordadas ao longo dos elementos comparativos apresentados nos tópicos seguintes.

2.2. Definição

2.2.1. Definição pela LGPD

A LGPD define o Relatório de Impacto como uma documentação do agente de tratamento a quem competem as decisões referentes ao tratamento de dados pessoais; isto é, do controlador (art. 5º, XVII).

O RIPD é definido como uma documentação, em virtude do seu caráter instrumental, em que se destaca a forma e condições a serem apresentadas à autoridade competente. Neste sentido, o Relatório deve ser compreendido como resultado de um processo de avaliação de impacto. Por isso, ressalta-se que não se trata apenas de uma documentação do controlador gerada após um processo de conformidade, "mas sim como um instrumento de apoio nas atividades de tratamento de uma organização para que ela possa fazer sua governança de dados e demonstrar conformidade com as obrigações legais previstas" (GOMES, 2019, pp. 8-11).

Embora a previsão da LGPD tenha definido expressamente o Relatório de Impacto como uma documentação do controlador, pode-se interpretar sistematicamente a viabilidade de operadores de dados também terem a necessidade de elaborar relatórios de impacto em benefício de suas atividades de tratamento. Isso é pertinente tendo em vista que o relatório de impacto é útil para garantir o atendimento e a preservação dos direitos dos titulares de dados, sendo uma ferramenta de governança e um documento a ser utilizado durante um processo de adequação regulatória (GOMES, 2019, pp. 6 e 12).

[7] Tradução livre do inglês: *"Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679".*

3.2.2. Definição pelo RGPD

Enquanto a LGPD dispõe expressamente sobre a definição de um Relatório de Impacto, o RGPD não define formalmente o conceito de uma AIPD, mas compreende como uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais (art. 35, nº 1).

Por outro lado, percebe-se a semelhança na definição instrumental brasileira com a compreensão do Relatório de Impacto estabelecida nas orientações europeias. Diante disso, entende-se que a AIPD deve ser encarado como um instrumento de apoio à tomada de decisão em relação ao tratamento de dados pessoais, sendo um processo contínuo e não um exercício que acontece uma única vez (WP29, 2018, p. 17).

É oportuno ressaltar que a LGPD direciona a responsabilidade da elaboração do Relatório ao controlador, assim como previsto no RGPD. Por outro lado, o regulamento europeu prevê expressamente que o controlador deverá solicitar o parecer do encarregado de proteção de dados, nos casos em que este tenha sido designado (art. 35, nº 2). Além disso, é previsto que o operador auxilie o controlador na realização da AIPD (art. 28, nº 3, 'f').

2.3. Contexto

2.3.1. Contexto pela LGPD

Pode-se considerar que a LGPD prevê que o Relatório de Impacto à Proteção de Dados (RIPD) será exigido no contexto em que a ANPD deverá ou poderá solicitar ao controlador. Diante disso, a Lei não definiu muitas diretrizes sobre o tema, porém é possível destacar um contexto geral e contextos específicos, nos quais apresentam situações que ensejam a necessidade de elaboração de Relatório de Impacto.

O contexto geral corresponde à solicitação da ANPD ao controlador para que este produza o Relatório de Impacto, referente aos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e direitos fundamentais do titular (art. 5º, XVII), bem como aos casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na Lei (art. 55-J, XIII).

Destaca-se que a LGPD não definiu de forma extensiva definições de risco e suas gradações, considerando que tal conceito envolve duas dimensões: uma centrada na previsão

de eventos futuros possíveis e outra baseada no processo de tomada de decisão informada pela avaliação de riscos (GOMES, 2019, pp. 174-183). Além disso, a Lei não estabeleceu pontualmente hipóteses que podem apresentar potencial em configurar um tratamento de alto risco, esse cenário evidencia a necessidade da regulamentação de tal tema.

Sobretudo, é possível destacar os contextos específicos previstos pela LGPD. Nesse sentido, a Autoridade poderá solicitar o RIPD ao controlador, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial (art. 10, II e §3º). Além disso, a Lei prevê que a ANPD deverá solicitar o Relatório, quando o tratamento for realizado para fins exclusivos de (i) segurança pública; (ii) defesa nacional, (iii) segurança do Estado e (iv) atividades de investigação e repressão de infrações penais (art. 32, §3º). É oportuno considerar que a publicação de relatórios de impacto poderá ser solicitada pela Autoridade aos agentes do Poder Público (art. 32).

Vale destacar que os tratamentos que envolvem legítimo interesse demandam mais atenção. Nas reuniões técnicas da ANPD, mencionadas no início deste texto, foi destacada a diferença entre o Teste de Proporcionalidade[8] e o Relatório de Impacto. A primeira corresponde a um teste para avaliar o equilíbrio entre os interesses do controlador, ou de terceiros, e os interesses e direitos fundamentais do titular. Por outro lado, o RIPD corresponde à documentação do controlador referente ao tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como altos riscos aos princípios gerais de proteção de dados pessoais previstos nesta Lei (arts. 5º, XVI e 55-J, XIII).

Em virtude dos princípios de transparência e prestação de contas (*accountability)*, por meio de uma interpretação sistemática dos artigos da LGPD, entende-se que a lei condiciona o uso responsável da base legal do legítimo interesse ao Teste de Proporcionalidade, sendo uma possível documentação especial, representada no próprio conteúdo normativo relativo à "licitude da aplicação de tal base legal" (BIONI, 2021, p. 185). Diante disso, entende-se que no contexto brasileiro, enquanto não houver regulamentação e manifestações da ANPD sobre o tema, o Teste de Proporcionalidade deve ser realizado antes do início do tratamento de dados pessoais; enquanto a elaboração do RIPD é obrigatória, quando for requisitado pela Autoridade (MATTIUZZO; PONCE, 2020, pp. 70-71).

[8] Do inglês: *"Legitimate Interests Assessment (LIA)"*.

Destaca-se que a Autoridade do Reino Unido (*Information Commissioner's Office – ICO*)[9] entende que o Teste de Proporcionalidade e a AIPD são documentos que tratam de temas comuns, porém apresentam diferenças. Nos termos da regulação europeia, o Teste de Proporcionalidade é uma avaliação simplificada de mensuração de riscos baixos, sendo necessário para o tratamento cuja base legal seja o legítimo interesse. Por outro lado, a AIPD pode servir como teste de adequação para utilização do legítimo interesse, sendo uma avaliação de riscos mais detalhada, independe de base legal, e necessário para casos que envolvem riscos elevados para os titulares de dados pessoais (MATTIUZZO; PONCE, 2020, pp. 70-71).

Sendo assim, conforme a Autoridade do Reino Unido, quando o Teste de Proporcionalidade identificar risco significativo, cabe ao controlador considerar a necessidade da elaboração de uma AIPD, para avaliar os riscos e a forma de mitigá-los.

2.3.2. Contexto pelo RGPD

Em contexto geral, ressalta-se que o Relatório é obrigatório somente quando o tratamento for "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" assim como previsto pela lei brasileira. Sobretudo, o RGPD se diferencia, pois expressa a previsão temporal de que a avaliação de impacto precisa ser documentada antes de iniciar o tratamento que se planeja realizar (art. 35, nº 1).

Em contrapartida, a AIPD é aplicável aos tratamentos existentes suscetíveis de implicar um elevado risco para os direitos e as liberdades das pessoas singulares e em relação às quais não tenha havido alteração dos riscos, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento (WP29, 2018, p.15).

Nesse sentido, destaca-se que o artigo 35, nº 3, dispõe uma lista com três exemplos relativos aos contextos em que uma operação de tratamento é suscetível de implicar elevados riscos. Diante disso, compreende-se que a AIPD é necessário quando o tratamento de dados pessoais: i) envolve decisões automatizadas relacionadas a perfilamento; (ii) tiver operações em grande escala de categorias especiais de dados a que se refere o artigo art. 9º (1) do RGPD, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o art. 10

[9] Com relação aos detalhes do Teste de Proporcionalidade, conforme diretrizes do ICO e nos termos do regulamento europeu, ver: *Legitimate Interests.* Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/. Acesso em 13 dez. 2021.

da norma europeia; ou (iii) realizar controle sistemático de zonas acessíveis ao público em grande escala (WP29, 2018, pp. 9-10).

A partir disso, destaca-se a diferença entre as técnicas legislativa brasileira e europeia, tendo em vista que o RGPD estabeleceu critérios para definir contextos em que há necessidade de realizar uma AIPD. As diretrizes europeias destacam nove critérios que devem ser considerados para identificar se um tratamento de dados é provável em resultar um alto risco, tendo em conta os elementos específicos do artigo 35, 1, 3, alíneas a) e c); a lista a adotar a nível nacional nos termos do artigo 35, 4, e dos Considerandos 71, 75 e 91 do RGPD (WP29, 2018, pp. 10-12).

Os critérios a serem considerados consistem em: (i) avaliação ou classificação; (ii) decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar; (iii) controle sistemático; (iv) dados sensíveis ou dados de natureza altamente pessoal, como relacionado a condenações penais e infrações; (v) dados tratados em grande escala, considerando quantidade pertinente referente ao número de titulares envolvidos, volume de dados e/ou diversidade de dados, duração da atividade e dimensão geográfica; (vi) estabelecer correspondências ou combinar conjuntos de dados; (vii) dados relativos a titulares vulneráveis; (viii) utilização de soluções inovadoras ou aplicações de novas soluções tecnológicas ou organizacionais; (iv) quando o próprio tratamento impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato (WP29, 2018, pp. 11-12).

O regulamento europeu estabelece a possibilidade de complemento aos contextos específicos pela publicação de lista das autoridades de proteção de dados (art. 35, nº 4). No contexto europeu, há elaboração de *blacklists* e *whitelists*, respectivamente, tratam-se de listas que estabelecem a necessidade ou dispensa da elaboração do Relatório (FAZLIOGLU, 2018). Nesse sentido, vale considerar que, na Reunião Técnica realizada para a regulamentação brasileira, especialistas ressaltaram que listas taxativas, no contexto da LGPD, poderiam prejudicar a aplicação desta, tendo em vista a possibilidade de os avanços tecnológicos tornarem tais listas obsoletas (GARROTE; PASCHOA; MEIRA; BIONI, 2021).

2.4. Conteúdo

2.4.1. Conteúdo Pela LGPD

A LGPD prevê que o conteúdo do Relatório de Impacto consiste na descrição dos (i) processos de tratamento de dados que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como (i) medidas, salvaguardas e mecanismos de mitigação de risco (art. 5º, XVII).

Vale citar que a LGPD também prevê sobre o conteúdo do RIPD em seu art. 38, *caput* e parágrafo único. O *caput* deste artigo dispõe que o Relatório de Impacto se refere às operações de tratamento de dados pessoais, inclusive de dados sensíveis, nos termos de regulamento, observados os segredos comercial e industrial.

O parágrafo único do mesmo artigo da LGPD versa sobre o conteúdo mínimo do Relatório, conforme a descrição dos seguintes aspectos: (i) tipos de dados coletados, (ii) metodologia utilizada para a coleta e para a garantia da segurança das informações e (iii) a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. Nesse sentido, diante da avaliação dos riscos, torna-se possível definir quais medidas, salvaguardas e mecanismos serão adotados para que tais riscos sejam mitigados.

Convém ressaltar as diferenças entre medidas, salvaguardas e mecanismos. Medidas são compreendidas como ações afirmativas do controlador que visem a redução ou gerenciamento de riscos, como a decisão de não coletar dados pessoais sensíveis, por exemplo. Salvaguardas são medidas preventivas que potencializam a mitigação dos riscos, ou a redução dos danos causados por esses, como a contratação de um seguro contra incidentes de segurança. Por fim, mecanismos são conjuntos de ações positivas ou negativas (fazer ou deixar de fazer) que contribuem com a mitigação dos riscos envolvidos em uma operação de tratamento de dados pessoais, como projetar um novo produto conforme um desenho baseado em uma infraestrutura que garanta os direitos relacionados à privacidade e à proteção de dados (*privacy by design*), por exemplo (GOMES, 2019, p. 11).

2.4.2. Conteúdo pelo RGPD

O RGPD também prevê conteúdo mínimo a ser apresentado em um Relatório de Impacto. Referente ao tratamento de dados, a AIPD deve apresentar, pelo menos (i) uma

descrição sistemática do tratamento; (ii) uma avaliação da necessidade e proporcionalidade em relação aos objetivos; (iii) uma avaliação dos riscos para os direitos e liberdades dos titulares; (iv) as medidas de mitigação de riscos (art. 35, nº 7).

A Autoridade do Reino Unido (*Information Commissioner's Office – ICO*) estabelece etapas para a produção de uma AIPD. Dentre essas etapas consta a necessidade de descrever sistematicamente o tratamento. Considera-se (i) a natureza: o que se pretende fazer com os dados; (ii) o âmbito referente à natureza, volume, variedade, sensibilidade, extensão, frequência, duração, número de titulares envolvidos, área geográfica; (iii) o contexto e propósitos referentes a aspectos mais gerais, bem como à fonte dos dados, ao relacionamento entre controlador e titular, ao controle e expectativas deste último, ao envolvimento com dados de pessoas vulneráveis; (iv) o objetivo do processamento em razão pela qual o controlador deseja tratar os dados pessoais, considerando, interesses legítimos, resultado pretendido para os indivíduos e benefícios esperados como um todo (ICO, 2021).

Destaca-se aqui, a ênfase semelhante dada tanto pelo RGPD, quanto pela LGPD, referente a consideração do legítimo interesse para avaliar a necessidade de Relatório de Impacto.

Além disso, as diretrizes europeias também destacam medidas que precisam ser consideradas para demonstração de conformidade incluindo detalhes como a base legal para o tratamento; e medidas que contribuam para os direitos dos titulares com detalhes sobre o fornecimento de informações prestadas ao titular (ARTIGO 29, 2018, p. 26).

Referente à avaliação de riscos, são considerados o impacto potencial sobre os indivíduos e a probabilidade e a gravidade do possível dano. Assim, em relação ao titular, deve ser considerado o potencial de o tratamento contribuir para incapacidade de exercer direitos, por exemplo. Esta avaliação, compreende também mapeamento de riscos de segurança, incluindo fonte de risco ou impacto potencial de um incidente de segurança (ICO, 2021).

A identificação de medidas de mitigação precisa corresponder a cada risco documentado, considerando a capacidade de tal medida reduzir ou evitar os riscos. Nesse contexto, as medidas previstas para fazer face a esses riscos são determinadas (art. 35, (7), 'd', e Considerando 90). Os exemplos de medidas são variados, diante disso pode-se considerar desde decisões para não coletar certos tipos de dados, como também implementação de novos sistemas para ajudar as pessoas a exercerem seus direitos (ICO, 2021).

Ressalta-se que algumas Autoridades de Proteção de Dados[10] disponibilizam templates que demonstram como o Relatório de Impacto deve ser e o que ele deve conter, conforme as disposições da legislação de proteção de dados pessoais (GOMES, 2019, p. 9).

Convém considerar que, pelo fato da LGPD ter importado a definição do Relatório de Impacto do RGPD, a metodologia para elaboração do RIPD tende a ser baseada em riscos, assim como ocorre na Europa (GARROTE; PASCHOALI; MEIRA; BIONI, 2021). Tal tendência pode ser evidenciada pelo *template* disponibilizado no site do Governo Digital, no qual estabelece orientação para que órgãos e entidades federais possam elaborar "documento de comunicação e transparência que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos, bem como propõe medidas, salvaguardas e mecanismos de mitigação" (BRASIL, 2021a).

Ressalta-se que a ANPD permanece com autonomia para proceder com a regulamentação e estabelecer a escolha metodológica para elaboração do Relatório de Impacto, considerando os interesses da realidade brasileira.

2.5. Diferenciais do RGPD

Vale destacar que a consulta prévia à Autoridade de Proteção de Dados é um dos diferenciais previstos no RGPD. O artigo 36 do Regulamento prevê que a consulta prévia ocorre quando a AIPD apresenta elevados riscos residuais. Ou seja, o controlador poderá consultar a própria Autoridade competente sobre a viabilidade de determinado tratamento, a partir da apresentação dos riscos da atividade através da AIPD.

Além disso, outros diferenciais podem ser considerados em relação ao contexto brasileiro, uma vez que, em relação ao Relatório de Impacto, o RGPD dispõe especificidades sobre (i) solicitação ao encarregado; (ii) conformidade; (iii) solicitação ao titular; (iv) exceções

[10] Cabe citar exemplos europeus, como (i) Alemanha: *Standard Data Protection Model* [Modelo normalizado de proteção de dados], V.1.0 – versão experimental, 201631; https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf ; (ii) Espanha: *Guía para una Evaluación de Impacto en la Protección de Datos Personales* (EIPD), Agencia española de protección de datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Gui a_EIPD.pdf ; (iii) França: *Privacy Impact Assessment* (PIA), Commission nationale de l'informatique et des libertés (CNIL), 2015. https://www.cnil.fr/fr/node/15798 ; (iv) Reino Unido: *Conducting privacy impact assessments code of practice, Information Commissioner's Office* (ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf .

por direito da União ou do Estado-Membro; (v) controle da conformidade (art. 35, (2), (8), (9), (10), (11)).

3. Estudo de Caso: Decisão do STF sobre Relatório de Impacto de Proteção de Dados Pessoais

Em maio de 2020, o Supremo Tribunal Federal (STF) referendou medidas cautelares deferidas pela ministra Rosa Weber em cinco Ações Diretas de Inconstitucionalidade (ADIs) contra a eficácia da Medida Provisória nº 954/2020. A MP em seu art. 2º, *caput*, determinava que as empresas de telecomunicações compartilhassem dados pessoais (como nome, número de telefone e endereço) de seus consumidores de telefonia móvel e fixa com o Instituto Brasileiro de Geografia e Estatística (IBGE) para produção de estatística oficial durante a pandemia do novo coronavírus.

O STF suspendeu a eficácia da MP 954/2020 por meio da decisão que estabeleceu o reconhecimento de um direito fundamental à proteção de dados como direito autônomo, extraído a partir de interpretação sistemática do texto constitucional brasileiro. Nesse sentido, esse relevante marco jurisprudencial abordou sobre o Relatório de Impacto à Proteção de Dados Pessoais (RPID).

A MP 954/2020 suspensa pelo STF previa a elaboração e divulgação de um RIPD a ser realizado posteriormente ao compartilhamento dos dados de milhões de clientes das operadoras de telecomunicações. Esse caso apresenta um conflito temporal uma vez que a MP estabeleceu que o RIPD fosse elaborado após o tratamento de dados pretendido pelo IBGE, o qual não serviria para apresentar os procedimentos possivelmente adotados para prevenir ou mitigar os riscos previamente identificados e envolvidos no tratamento (MENDES; RODRIGUES JÚNIOR; FONSECA, 2021, p. 81).

Vale ressaltar que a LGPD não prevê expressamente o contexto temporal em que o Relatório de Impacto deverá ser elaborado. Em contrapartida, o RGPD estabelece que o Relatório deve ser realizado antes de se iniciar o tratamento, exceto quando se refere a um tratamento já existente e que foi previamente controlado pela Autoridade de Proteção de Dados (art. 35, nº 1 e 10, e Considerandos 90 e 93).

Nesta decisão, frisa-se o seguinte entendimento do Ministro Ricardo Lewandowski:

> "o relatório de impacto à proteção das informações pessoais dos consumidores não poderia ser feito a destempo, depois de já compartilhados e ocorridos eventuais abusos, pois assim, ao menos em um juízo de cognição sumária, será tarde demais para que seja apurado se houve ou não adequação à legislação e como foi impactado o regime de proteção de dados" (ADI n. 6387. Rel. Min. Rosa Weber, Plenário, DJe. 06 e 07.05.2020).

Nesse contexto, a Ministra Relatora Rosa Weber considerou que "a elaboração de relatório de impacto após o uso dos dados, e não previamente ao compartilhamento, impede a efetiva avaliação dos riscos". Nesse sentido, considerou-se a necessidade da elaboração de relatório de impacto anterior à coleta e uso dos dados, uma vez que a realização após o compartilhamento agravaria os riscos à segurança e proteção dos dados.

Vale considerar a complexidade deste caso, uma vez que, em julho de 2019, pela Lei nº 13.853/19, foi criada a Autoridade Nacional de Proteção de Dados (ANPD) a quem compete fiscalizar, solicitar e regulamentar sobre o Relatório de Impacto à Proteção de Dados Pessoais. Apenas em outubro de 2020, foi iniciado o processo de estruturação da Autoridade, com a nomeação para o Conselho Diretor. Diante disso, à época da MP 954/2020, em maio de 2020, não havia uma Autoridade estruturada para avaliar as conclusões, metodologia e parâmetros normativos aplicados ao Relatório de Impacto a ser realizado pelo IBGE (MENDES; RODRIGUES JÚNIOR; FONSECA, 2021, p. 82).

Considerando como exemplo os critérios estabelecidos pelas diretrizes europeias, a necessidade em realizar um relatório de impacto era evidenciada pelo potencial de alto risco sobre o tratamento pretendido, seja pelo tratamento em grande escala ou pela quantidade de titulares afetados.

Fica evidente, portanto, que o STF interpretou adequadamente a necessidade da realização do Relatório de Impacto, anterior ao tratamento, a fim de garantir a transparência pública e medir os riscos do compartilhamento.

Considerações Finais

Diante o exposto, percebe-se que em relação ao Relatório de Impacto de Proteção de Dados Pessoais, a LGPD possui uma abordagem menos específica em comparação ao RGPD. Contudo, ambas legislações tendem a apresentar regulamentações semelhantes, tendo em vista

a identificação da instrumentalização dos relatórios de impacto, tanto para a conformidade regulatória, quanto para a realização de boa prática de proteção de dados pessoais.

Torna-se evidente as correspondências da legislação europeia na legislação brasileira, referente aos aspectos do Relatório de Impacto em relação (i) à competência das autoridades de proteção de dados pessoais, (ii) à definição; (iii) ao contexto de exigibilidade e (iv) conteúdo dos relatórios de impacto.

A importância da correspondência entre a LGPD e o RGPD foi evidenciada na decisão do STF, na qual suspendeu a MP 954/2020. Conforme a decisão em que foi compreendido o direito fundamental à proteção de dados pessoais, entende-se que os critérios utilizados no julgado provêm das repercussões legislativas e regulamentares europeias. Diante disso, foi possível identificar a real necessidade do relatório, bem como o contexto a ser produzido; isto é, antes do tratamento suscetível a um elevado risco à liberdade e direitos do titular.

Evidencia-se, portanto, que a definição do Relatório de Impacto prevista na LGPD não objetiva indicar todas as especificidades que envolvem a elaboração deste instrumento de adequação e de governança. Nesse sentido, pode-se considerar a crescente tendência entre as semelhanças da LGPD e DO RGPD, conforme atuação regulamentar da ANPD sobre a definição, contexto e conteúdo dos relatórios de impacto.

Referências bibliográficas

ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, WP248. Disponível em: <https:// ec.europa.eu/newsroom/article29/item-detail. cfm?item_id=611236>. Acesso em: 20 ago. 2021.

BIONI, Bruno Ricardo. Legítimo interesse: aspectos gerais a partir de uma visão obrigacional. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021, p. 163-176.

BRASIL. Lei nº 13.709/2018, de 14 de agosto de 208. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União.* Brasília, DF, 15, Ago. de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 27 ago. 2021.

BRASIL. Medida Provisória n. 954, de 17 de abril de 2020. *Diário Oficial da União.* Brasília, DF, 18, Abr. de 2020. Disponível em: <https://www.in.gov.br/web/dou/-/medida-provisoria-n-954-de-17-de-abril-

de-2020-253004955>. Acesso em: 17 ago. 2021.

BRASIL. Portaria nº 11, de 27 de Janeiro de 2021. Diário Oficial da União. Brasília, DF, 28, Jan. de 2021. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>. Acesso em: 17 ago. 2021.

BRASIL, Supremo Tribunal Federal. ADI n. 6.387. Rel. Min. Rosa Weber, Decisão Monocrática, j. 24.04.2020, DJe 28.04.2020. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>. Acesso em: 27 ago. 2021.

BRASIL. GOVERNO DIGITAL. Guia de Boas Práticas LGPD. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia-boas-praticas-lgpd>. Acesso em: 17 jul. 2021a.

FAZLIOGLU, Müge. *What's subject to a DPIA under the GDPR?* EDPB on draft lists of 22 supervisory au-thorities. IAPP. 30 de outubro de 2018. Disponível em <https://iapp.org/news/a/whats-subject-to-a-dpia-under-the-gdpr-edpb-on-draft-lists-of-22-supervisory-authorities/?mkt_tok=eyJpIjoiTjJNMFpEY-zJNR05rTUROb SIsInQiOiJKclk5WjkrYW51UVI4cmZGcXUrZDFjRVhtVzNcL2pqMnppT-FwvZ3BHY21oY0VTQnRCeEdYMWMwVFZ5azJnUnNSRU0zMXd6aWt4RlZnclBUbGNmTTBqNE-xoVnV6VFBzQjRFM3hWRFBrc3VSWFdxXC9tSWoyYzlqWThkRzFCaHpqNitUeiJ9>. Acesso em: 17 ago. 2021.

GARROTE, Marina Gonçalves; PASCHOALI, Nathan; MEIRA, Marina; BIONI, Bruno R. ANPD na regulamentação do Relatório de Impacto à Proteção de Dados Pessoais. Portal JOTA, Brasília, 13.07.2021. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/anpd-relatorio-impacto-protecao-dados-pessoais-13072021>. Acesso: 17 agosto 2021.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados: uma breve análise da sua definição e papel na LGPD. Revista do Advogado, São Paulo, n. 144, nov. 2019.

GOMES, Maria Cecília O. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. In Direito Digital: Debates Contemporâneos. LIMA, Ana Paula. HISSA, Carmina. SALDANHA, Paloma Mendes (org.). São Paulo: Revista dos Tribunais, 2019, pp. 141-153.

ICO. Legitimate Interest. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>. Acesso em: 26 out. de 2021;

MATTIUZZO, Marcela; PONCE, Paula Pedigoni. O Legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa. Internet&Sociedade. V.1. n.2. Dezembro de 2020. Páginas 54 a 76. Disponível em: <https://revista.internetlab.org.br/wp-content/uploads/2020/12/O-legi%CC%81timo-interesse-e-o-teste-da-proporcionalidade.pdf>. Acesso em: 24 out. de 2021.

MENDES; Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz; FONSECA, Gabriel Campos Soares. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). Tratado de Proteção de Dados

Pessoais. Rio de Janeiro: Forense, 2021, pp. 61-71.

UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 17 jul. 2021.

UNIÃO EUROPEIA. Diretiva 95/46/EC.

Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how9>. Acesso em: 17 jul. 2021.

LIMITES AO COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE OS ENTES DO PODER PÚBLICO

Júlia Carvalho Soub[1]

Introdução

A distopia literária 1984 de George Orwell demonstra um dos maiores medos da atualidade, isto é, a constante sensação de vigilância pelo governo para com seus cidadãos. Com o advento e avanço da tecnologia esse medo demonstra-se ainda mais palpável, sendo amplamente demonstrado pela arte, a exemplo das séries "Pessoa de interesse" e "Bull".

Diante desse cenário, a fim de que a vida não volte a copiar a arte, o presente artigo busca compreender os limites à possibilidade de o Estado compartilhar dados pessoais de seus cidadãos entre os entes do Poder Público. Isso porque o compartilhamento público-público é fundamental para a maior eficiência e desenvolvimento das atividades administrativas do governo. Todavia, sem as devidas limitações, poderia resultar em cenários indesejados de vigilância (WIMMER, 2021- b), a exemplo dos referenciados como o do *Big Brother*.

Por conseguinte, o presente artigo tem como objetivo identificar quais os limites ao compartilhamento público-público, excluindo-se da presente análise o compartilhamento de dados entre o Estado e entes privados. Para tanto, no tópico 1 - comentários - será feita uma revisão bibliográfica, com o intuito de assimilar as considerações doutrinárias sobre o tema. Ademais, serão analisados, enquanto parâmetros de limitação do referido compartilhamento, os dispositivos do *General Data Protection Regulation* (GDPR), relativos ao art. 5º, 1, b e o art. 6º, 4, a, b, c, d, e.

Posteriormente, examinar-se-á no tópico 2 - estudo de caso - a decisão proferida na Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6529 (MC-ADI 6529), caso no qual se questiona o compartilhamento de dados entre o DETRAN e a ABIN. Será, então, exposta uma breve síntese da referida decisão no subtópico 2.1. O subtópico 2.2, por sua vez, destinar-se-á ao exame da rejeição ao isolamento do interesse público no tratamento de dados

[1] Graduanda no Curso de Direito da Universidade de Brasília. Pesquisadora do Observatório da LGPD da Universidade de Brasília 2020-2021.

pessoais pelo Poder Público, haja vista decisões proferidas pelo Supremo Tribunal Federal. Para além, no subtópico 2.3 será examinada a deliberação da Corte Europeia de Direitos Humanos (CEDH) no caso paradigma *Big Brother and Others vs. The United Kingdom,* a fim de se explorar o cenário que o presente artigo pretende evitar ao sugerir limitações ao tratamento de dados pessoais dos cidadãos brasileiros pelos entes públicos.

Por fim, observar-se-á que a visão dicotômica entre interesse público e privado não se faz adequada para a proteção dos dados pessoais dos cidadãos em relação ao Estado. Isso porque, a relevância, proporcionalidade e razoabilidade do compartilhamento de dados pessoais para a realização do tratamento secundário desses pela Administração Pública apenas poderá ser observada *in concreto*, a partir de uma análise de observância dos princípios constitucionalmente impostos, conforme fora feito na MC-ADI 6529, ora analisada. Para além, verificar-se-á que o conhecimento europeu em muito pode acrescentar nas possibilidades de limitação do poder estatal no que diz respeito ao tratamento das informações dos indivíduos.

1. Comentários

O tratamento de dados pessoais dos cidadãos pelo Estado não é um tema recente, apesar de ter se intensificado e de ter ganhado destaque com a revolução tecnológica. Nesse cenário, sem pretensões de usufruir desse termo de maneira anacrônica, porém a fim de exemplificar a situação apresentada, é possível verificar que o ente estatal a muito concentra a tutela de documentos essenciais, como certidões de nascimento, de casamento e de óbito, que geram dados pessoais. Ou seja, informações pessoais individualizadas/individualizáveis (MENDES, 2021), que, a depender da forma de utilização e interpretação, poderão gerar consequências positivas e/ou negativas aos titulares desses dados (MENDES; MATTIUZZO; FUJIMOTO, 2021).

Dessa maneira, faz-se imprescindível compreender que na atual sociedade da informação, os indivíduos estão a todo momento a produzir dados pessoais, seja com o intuito de desenvolver relações sociais, por intermédio de redes sociais como o *instagram* e o *tik tok*, seja com a compra de medicamentos em farmácias - que não raro solicitam o CPF do cliente. No caso específico de coleta de dados pelo Poder Público, verifica-se que inúmeras são as fontes de coletas de dados, dentre as quais destaca-se o cadastro em sites ou enquanto requisito para obtenção de serviços públicos (CELLA; COPETTI, 2017).

Diante dessa perspectiva, a utilização crescente dos dados pessoais (*input*) para o tratamento de dados, fenômeno também denominado como *big data*, exige a existência de uma assídua preocupação com as consequências que o processamento desses poderá trazer aos indivíduos e os riscos aos quais esses estarão expostos. Nesse sentido, tem-se que as consequências geradas poderão ser drásticas para a vida dos cidadãos, na hipótese de produção de resultados discriminatórios, ilícitos ou abusivos (MENDES; MATTIUZZO; FUJIMOTO, 2021).

A conjuntura apresentada torna-se ainda mais complexa na hipótese de tratamento de dados pessoais pelo Poder Público, haja vista a relação verticalizada entre Estado e cidadão. Essa evidente desigualdade entre titular e controlador de dados é envolta por uma situação de dependência, na qual o cidadão depende do Estado para usufruir de serviços públicos, a exemplo da saúde pública (BLACK; STEVENS, 2013).

Contudo, a tecnologia possui papel fundamental na performance estatal e viabiliza que, a partir do tratamento de dados pessoais, os órgãos e entidades públicas desempenhem seu papel da forma mais eficiente possível e, para além, que as próprias políticas públicas sejam melhor desenhadas e executadas (MENDES; MACHADO; GASIOLA, 2021).

Logo, o compartilhamento dos referidos dados entre os entes que compõem o Poder Público apresenta-se enquanto importante ferramenta no contexto governamental. Tanto é, que o art. 26 da Lei Geral de Proteção de Dados Pessoais (LGPD) autoriza o referido compartilhamento para "execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas", sendo, portanto, a base legal para o denominado tratamento secundário diante da lógica *ex ante* proposta pela LGPD (WIMMER, 2021-a).

Esse dispositivo, apesar de reforçar a necessidade de observância aos princípios de proteção de dados pessoais discriminados no art. 6º da LGPD, autoriza o compartilhamento de forma ampla e, portanto, faz-se fundamental compreender quais os limites para a realização desse (WIMMER, 2021-a). A necessidade de limitações impostas ao tratamento efetuado pelo Poder Público é proveniente da própria noção de respeito aos direitos fundamentais dos indivíduos pelo Estado, dando-se enfoque no presente artigo à proteção da privacidade.

Entende-se, nesse sentido, a privacidade como um direito abrangente, no qual o indivíduo poderá desenvolver sua personalidade, independente de constrangimentos sociais para adotar determinados comportamentos. Assim, este deverá ser "deixado em paz" para que

tenha espaço suficiente para refletir sobre quem pretende ser (SARLET *apud* ARIENTE *et al.*, 2020), todavia, isso não significa dizer que possuirá total controle sobre o tratamento de seus dados pessoais, a fim de, por exemplo, impedir que a Receita Federal processe sua declaração de imposto de renda (WIMMER, 2021- b).

Diante desse cenário, é extremamente importante compreender que a Administração Pública, enquanto concretizadora da previsão abstrata da lei, necessita avaliar o contexto fático, a fim de optar e executar as Políticas Públicas. Dentro dessa lógica estatal, os dados pessoais dos cidadãos apresentam grande relevância, haja vista a atual sociedade da informação (MENDES; MACHADO; GASIOLA, 2021).

O art. 26 da LGPD, por conseguinte, foi promulgado com o intuito primordial de viabilizar o compartilhamento de dados entre os órgãos e entidades do Poder Público - compartilhamento Público-Público (WIMMER, 2021-a) -, concretizando, portanto, o princípio da eficiência, previsto no art. 37, *caput*, da Constituição Federal.

No entanto, ainda que vise promover maior agilidade à Administração, conforme fora anteriormente destacado, sua natureza principiológica e harmônica para com os ideais trazidos na LGPD deixa evidente a necessidade de observância aos princípios previstos no art. 6º desta lei (WIMMER, 2021-a). Desta feita, destacam-se aqueles presentes nos incisos I, II e III. Vejamos:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - **finalidade:** realização do tratamento para **propósitos legítimos, específicos, explícitos e informados ao titular**, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - **adequação:** compatibilidade do tratamento com as **finalidades informadas** ao titular, de acordo com o contexto do tratamento;
> III - **necessidade**: limitação do **tratamento ao mínimo necessário para a realização de suas finalidades**, com abrangência dos **dados pertinentes, proporcionais e não excessivos** em relação às finalidades do tratamento de dados; **(GRIFOS NOSSOS)**

Mediante a leitura dos referidos incisos, é possível aferir que os dados compartilhados entre os entes do Poder público apenas poderão dar ensejo a um tratamento secundário que tenha finalidade compatível com o tratamento que possibilitou a coleta dessas informações individualizadas, sendo, portanto, uma das mais relevantes limitações ao compartilhamento público-público (WIMMER, 2021-a).

Essa adequação às finalidades informadas ao titular deverá estar sempre combinada ao mínimo tratamento necessário, uma vez que deverão os dados serem sempre pertinentes, proporcionais e não excessivos, para que não se tenha um resultado viciado, com correlações abusivas ou ilícitas (MENDES; MATTIUZZO; FUJIMOTO, 2021).

Apesar de serem balizas de extrema relevância, a finalidade, adequação e necessidade não são suficientes para limitar o poder estatal, a fim de que o tratamento secundário de dados não origine um verdadeiro cenário de vigilância. Assim, a título de aplicar a experiência internacional no contexto brasileiro, entende-se que os artigos 5, 1, b, e 6, 4, da GDPR poderão ser entendidos enquanto excelentes balizas limitadoras para o referido compartilhamento de dados. Verifiquemos, portanto, sua redação em português:

> **Artigo 5. Princípios relativos ao tratamento de dados pessoais**
>
> 1. Os dados pessoais são:
>
> b) Recolhidos para finalidades determinadas, explícitas e legítimas e **não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades**; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89. , n. 1 («l**imitação das finalidades**»);
>
> **Art. 6. Licitude do tratamento**
>
> 4. Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23. o , n. o 1, o responsável pelo tratamento , a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta:
>
> a) Qualquer **ligação entre a finalidade** para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
>
> b) O **contexto em que os dados pessoais foram recolhidos**, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;
>
> c) A **natureza dos dados pessoais**, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9., ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.;
>
> d) As **eventuais consequências** do tratamento posterior pretendido para os titulares dos dados;

> e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a **anonimização**. (**GRIFOS NOSSOS)**

Cabe destacar que o art. 5, 1, b, fora de certa forma reproduzido na própria redação do art. 26 da LGPD, uma vez que estabelece a compatibilidade entre finalidades enquanto requisito essencial para o tratamento secundário de dados pessoais pelo Poder Público. Esse juízo de finalidade, adequação e necessidade deverá ser feito dentro dos parâmetros do caso concreto, conforme evidenciado nos dispositivos analisados. Essa perspectiva também se encontra englobada no art. 6, 4, a e b.

No que diz respeito ao art. 6, 4, c, é interessante notar que a natureza dos dados pessoais foi levada em consideração para a possibilidade de compartilhamento. Nesse sentido, cabe destacar que dados sensíveis dizem respeito a futuras informações que são potencialmente discriminatórias. Diante dessa conjuntura, os titulares adquirem direitos subjetivos em face dos controladores, sendo um grande exemplo dessa situação a possibilidade de revogação sem justificativa do consentimento para usufruto desses dados, na hipótese de essa ser a base legal que justifica o tratamento. Ademais, destaca-se que dados podem aparentar ser insignificantes, porém, a depender do tratamento realizado, podem tornar-se sensíveis (MENDES, 2014). Haja vista relativo consenso de que o tratamento de dados sensíveis provoca riscos maiores à personalidade individual, seria de extrema relevância a adoção desse critério enquanto limitação para o compartilhamento público-público.

Quanto a necessidade de levar em consideração as eventuais consequências do tratamento posterior, conforme descrito na alínea d do referido artigo 6, cabe destacar que no contexto brasileiro a LGPD foi a primeira legislação que previu o relatório de impacto, instrumento que possibilita a verificação da aderência das condutas do controlador à lei. Observa-se que na legislação europeia o *Data Protection Impact Assessment* (DPIA), que serviu de inspiração ao relatório de impacto, encontra-se diretamente ligado à noção de prevenção e mitigação de riscos aos titulares de dados (GOMES, 2019).

Nesse sentido, o risco pode ser entendido enquanto uma visão subjetiva na qual o controlador, a partir do conhecimento de eventos futuros, deverá tomar uma decisão de assumir ou não a possibilidade de sofrer eventual sanção (GOMES, 2019). Logo, entende-se que poderá a Autoridade Nacional de Proteção de Dados (ANPD) indicar modelos de relatórios de impactos, com o intuito de possibilitar que os entes da Administração Pública verifiquem as consequências de eventual tratamento secundário, podendo, dessa forma, mitigar e,

principalmente, prevenir eventuais riscos aos direitos dos titulares, em especial os direitos fundamentais previstos no art. 5º da Constituição Federal, a exemplo das liberdades civis.

Por fim, no que diz respeito à anonimização prevista no art. 6º, 4, e da GDPR, é necessário, antes de tudo, compreender a definição de dados pessoais. Assim, toda informação que possibilitar a identificação de uma pessoa natural, a exemplo de seu nome, endereço, endereço eletrônico, entre outros, será considerado um dado pessoal (FINKELSTEIN; FINKELSTEIN, 2019) que, eventualmente, a depender da forma com a qual for tratado, poderá gerar riscos a esse indivíduo (MENDES; MATTIUZZO; FUJIMOTO, 2021).

Dados "anonimizados", por outrora, ao não possibilitarem a identificação dos titulares, não encontram-se resguardados pelo escopo da LGPD. Essa anonimização advém da impossibilidade de rastrear os titulares, levando-se em consideração meios técnicos razoáveis e disponíveis em seu tratamento (FINKELSTEIN; FINKELSTEIN, 2019). Por óbvio existe uma evidente zona de penumbra que fora melhor desenvolvida pela pesquisadora Ana Júlia Prezotti no presente anuário. Porém, para os fins deste artigo, entende-se que a anonimização, sempre que possível, de dados compartilhados entre os entes do Poder Público poderá ser uma excelente baliza de limitação do poder estatal.

Levando-se em consideração todo o exposto, o presente artigo irá se dedicar no tópico seguinte à análise da MC-ADI 6.529/DF e das demais decisões - ADI 6529 MC-Ref, ADI 6387 MC-Ref. SL 1103 e MS 36150 MC -, a fim de compreender como a Suprema Corte brasileira vem se posicionando sobre o tema ora debatido. Por fim, serão feitas considerações sobre o posicionamento da CEDH no caso *Big Brother and Others vs. United Kingdom* com o propósito de demonstrar que eventual tratamento secundário deverá sofrer limitações, para que esse não proporcione a vigilância de cidadãos sob um falso pretexto.

2. Estudos de Caso

2.1. Síntese geral da MC-ADI 6.529/DF

Trata-se de Ação Direta de Inconstitucionalidade (ADI), com pedido de medida cautelar, proposta pelo Partido Socialista Brasileiro e pela Rede de Sustentabilidade, a fim de declarar parcialmente a inconstitucionalidade do §1º, art. 2º, parágrafo único, art. 4º e do art. 9º-A da Lei nº 9.883/1999:

> **Art. 2º. § 1º** O Sistema Brasileiro de Inteligência é responsável pelo processo de obtenção, análise e disseminação da informação necessária ao processo decisório do Poder Executivo, bem como pela salvaguarda da informação contra o acesso de pessoas ou órgãos não autorizados.
>
> **Art. 4º** À ABIN, além do que lhe prescreve o artigo anterior, compete:
>
> **Parágrafo único**. Os órgãos componentes do Sistema Brasileiro de Inteligência fornecerão à ABIN, nos termos e condições a serem aprovados mediante ato presidencial, para fins de integração, dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais.
>
> **Art. 9º A -** Quaisquer informações ou documentos sobre as atividades e assuntos de inteligência produzidos, em curso ou sob a custódia da ABIN somente poderão ser fornecidos, às autoridades que tenham competência legal para solicitá-los, pelo Chefe do Gabinete de Segurança Institucional da Presidência da República, observado o respectivo grau de sigilo conferido com base na legislação em vigor, excluídos aqueles cujo sigilo seja imprescindível à segurança da sociedade e do Estado. (Vide Medida Provisória nº 2.123-30, de 2001) (Incluído pela Medida Provisória nº 2.216-37, de 2001)

Outrossim, a referida ADI pretende a declaração da inconstitucionalidade por arrastamento do art.1º, §3º, da Estrutura Regimental da Agência Brasileira de Inteligência (ABIN), aprovada pelo Decreto nº 10.445/2020. *Vide*:

> **Art. 1º** A Agência Brasileira de Inteligência - Abin, órgão integrante do Gabinete de Segurança Institucional da Presidência da República, criada pela Lei nº 9.883, de 7 de dezembro de 1999, é órgão central do Sistema Brasileiro de Inteligência e tem por competência planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País, obedecidas a política e as diretrizes estabelecidas em legislação específica.
>
> **§ 3º** Os órgãos componentes do Sistema Brasileiro de Inteligência fornecerão à Abin, sempre que solicitados, nos termos do disposto no Decreto nº 4.376, de 13 de setembro de 2002, e na legislação correlata, para fins de integração, dados e conhecimentos específicos relacionados à defesa das instituições e dos interesses nacionais.

Em suma, intenta-se que o Sistema Brasileiro de Inteligência (Sisbin) apenas possa compartilhar dados pessoais à Agência Brasileira de Inteligência (Abin) quando for de interesse público, não sendo possibilitado o compartilhamento na hipótese de interesse privado/pessoal. Diante do referido pedido, a decisão majoritária usufruiu da técnica relativa à interpretação conforme à constituição, estabelecendo a necessidade de motivação do ato de solicitar os dados a serem compartilhados, para além da necessidade de instauração de procedimento formal, a

fim de que se possa sofrer eventual controle de legalidade pelo judiciário, ocorrendo, inclusive responsabilização nos casos de omissões, desvios e abusos (SUPREMO TRIBUNAL FEDERAL, 2020).

Ademais, foi firmado o entendimento de que existem hipóteses específicas as quais se reservam à jurisdição, sendo apenas possível com prévia análise e autorização judicial, como, por exemplo, as interceptações telefônicas. Por sua vez, a divergência compreendeu que estando a referida legislação em vigor há 21 anos, não haveria riscos em se aguardar a manifestação do Congresso Nacional, autoridade competente (SUPREMO TRIBUNAL FEDERAL, 2020). A Ementa da referida Medida Cautelar foi pronunciada nos seguintes termos:

> DIREITO CONSTITUCIONAL. AÇÃO DIRETA DE INCONSTITUCIONALIDADE. PARÁGRAFO ÚNICO DO ART. 4o DA LEI N. 9.883/99. INTERESSE PÚBLICO FORMALMENTE DEMONSTRADO COMO ÚNICO ELEMENTO LEGITIMADOR DO DESEMPENHO ADMINISTRATIVO. VEDAÇÃO AO ABUSO DE DIREITO E AO DESVIO DE FINALIDADE. OBRIGATORIEDADE DE MOTIVAÇÃO DO ATO ADMINISTRATIVO QUE SOLICITA DADOS DE INTELIGÊNCIA AOS ÓRGÃOS DO SISTEMA BRASILEIRO DE INTELIGÊNCIA. NECESSÁRIA OBSERVÂNCIA DA CLÁUSULA DE RESERVA DE JURISDIÇÃO. DEFERIMENTO PARCIAL DA MEDIDA CAUTELAR PARA DAR INTERPRETAÇÃO CONFORME AO PARÁGRAFO ÚNICO DO ART. 4o DA LEI N. 9.883/99.
>
> **1.** Para se concluir válido o texto legal e dar-se integral cumprimento ao comando normativo infralegal pelo Poder Executivo há de adotar-se como única interpretação e aplicação juridicamente legítima – como é óbvio – aquela que conforma a norma à Constituição da República. **É imprescindível vinculem-se os dados a serem fornecidos ao interesse público objetivamente comprovado e com motivação específica.**
>
> **2. Todo fornecimento de informação entre órgãos que não cumpra os rigores formais do direito nem atenda estritamente ao interesse público, rotulado legalmente como defesa das instituições e do interesse nacional, configura abuso do direito, contrariando a finalidade legítima posta na norma legal.**
>
> **3. Práticas de atos à margem ou diversos do interesse público, especificado em cada categoria jurídica, devem ser afastadas pelo Poder Judiciário, quando comprovado o desvio de finalidade no cometimento.**
>
> **4.** A ausência de motivação expressa impede o exame da legitimidade de atos da Administração Pública, incluídos aqueles relativos às atividades de inteligência, pelo que a motivação é imprescindível.

> **5.** Mesmo nos casos de prática de atos motivados pelo interesse público, não é possível que os órgãos componentes do Sistema Brasileiro de Inteligência forneçam à ABIN dados que importem em quebra do sigilo telefônico ou de dados, por ser essa competência conferida ao Poder Judiciário, nos termos constitucionalmente previstos. **6.** Medida cautelar parcialmente deferida para dar interpretação conforme ao parágrafo único do art. 4o da Lei no 9.883/99 estabelecendo-se que: *a)* **os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida, afastada qualquer possibilidade desses dados atenderem interesses pessoais ou privados**; *b)* toda e qualquer solicitação de dados deverá ser devidamente motivada para eventual controle de legalidade pelo Poder Judiciário; *c)* mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo legal, em razão daquela limitação, decorrente do necessário respeito aos direitos fundamentais; *d)* **nas hipóteses cabíveis de fornecimento de informações e dados à ABIN é imprescindível procedimento formalmente instaurado e a existência de sistemas eletrônico de segurança e registro de acesso, inclusive para efeito de responsabilização, em caso de eventual omissão desvio ou abuso. (GRIFOS NOSSOS)**

Com a devida vênia à divergência, compreende-se que a prevalência da decisão majoritária era necessária, pois, ainda que a legislação questionada tenha sido editada há 21 anos, inegável o avanço tecnológico durante esse período, sendo que o compartilhamento de dados atualmente poderá trazer inúmeras consequências que seriam inimagináveis durante a década de 90.

Haja vista o cenário apresentado, passar-se-á às considerações sobre o posicionamento do Supremo Tribunal Federal em decisões cujo teor diz respeito às limitações impostas ao compartilhamento público-público.

2.2. Tratamento de dados pessoais pelo Poder Público: princípios constitucionais aplicáveis e rejeição ao isolamento do interesse público

Inicialmente ressalta-se que a discussão jurídica travada nesta ADI assume contornos bem particulares em relação ao debate enfrentado pelo Supremo Tribunal Federal na análise da ADI 6.389 MC-Ref (Caso IBGE), acórdão paradigma no contexto da proteção de dados

pessoais. Isso se deve principalmente às complexidades que permeiam o tratamento de dados no âmbito do Poder Público.

Considerando o interesse público envolvido nas atividades de proteção de dados pessoais pela Administração e o próprio caráter compulsório do relacionamento entre os particulares e o Estado (BLACK; STEVENS, 2013), é possível aferir a essencialidade do tratamento de dados pessoais pelo Estado, a fim de que esse possa executar o que lhe fora constitucionalmente imposto (WIMMER, 2021-b). Ademais, conforme ressaltado pela autora Miriam Wimmer (2021-b), seria inimaginável, por exemplo, que os indivíduos possuíssem o direito subjetivo de requerer à Administração Pública a portabilidade de seus dados pessoais, exigindo sua eliminação.

A discussão sobre a privacidade nas relações com a Administração Estatal, todavia, não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais. Como bem destacado por Gillian Black e Leslie Stevens (2013), se a privacidade fosse compreendida apenas enquanto um interesse particular do titular dos dados pessoais, sempre haveria a possibilidade do tratamento desses pela Administração Pública, uma vez que as finalidades públicas que o justificam sempre seriam consideradas necessárias e proporcionais.

Convém destacar que essa visão de compatibilização dos interesses da Administração Pública com a defesa de garantias individuais na temática da proteção de dados pessoais no Poder Público não é de todo estranha à jurisprudência do STF. Em pelo menos duas ocasiões o Tribunal impôs limitações a um modelo de fluxo multidirecional e irrestrito do compartilhamento de dados entre órgãos e instituições públicas.

Na primeira ocasião, tem-se a Suspensão de Liminar 1.103 MC, julgada monocraticamente pelo então Ministro Presidente - Min. Dias Toffoli - em 30 de maio de 2019. A referida decisão determinou que o IBGE se abstivesse de fornecer ao Ministério Público Federal dados reputados necessários à identificação de 45 (quarenta e cinco) crianças, na área urbana do município de Bauru/SP, desprovidas de registro de nascimento e, por conseguinte, da proteção do Estado e da sociedade.

Nessa decisão, destacou-se a necessidade de conciliação dos valores constitucionais em jogo ao pontuar que manter em sigilo as informações fornecidas é fundamental para que haja confiança nas pesquisas a serem efetuadas pelo IBGE. Observa-se, nesse sentido:

> "**O dever de sigilo proporciona segurança a quem presta as informações e contribui para a confiabilidade das pesquisas efetuadas. Recepção das normas que estabelecem o sigilo das informações colhidas pelo IBGE (art. 2º, § 2º, do Decreto-lei n. 16111967 e parágrafo único, do art. 1–, da Lei no 5.534/1968) pela Constituição Federal de 1988**. IV. Quando princípios fundamentais da Constituição conflitam entre si, a questão deve ser analisada tendo em vista o caso concreto, respeitados os valores supremos consagrados na ordem constitucional. Com base no juízo de ponderação, busca-se identificar em qual dimensão deve um direito fundamental preponderar quando contraposto a outro direito também fundamental. Para isso, deve-se recorrer aos princípios instrumentais da razoabilidade e da proporcionalidade, implícitos na Constituição, e sopesar os valores protegidos pelas normas em conflito. Não se trata de eliminar um direito para fazer predominar exclusivamente outro, mas sim de conciliar os bens jurídicos em conflito e harmonizá-los com os princípios consagrados no sistema jurídico constitucional". (SSL 1.103 MC, Rel. Min. Cármen Lúcia, julgado em 5.2.2017, DJe 8.5.2017).

Na segunda ocasião, cumpre citar ainda a Medida Cautelar nos autos do Mandado de Segurança 36.150. Diante das circunstâncias do caso concreto, o Relator deferiu a cautelar para cassar determinação do Tribunal de Contas da União (TCU), que ordenara ao Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP a entrega de dados individualizados do Censo Escolar e do ENEM para auditoria do Programa Bolsa Família.

Destaca-se que, nessa decisão, apontou-se o risco de o tratamento dos dados compartilhados pelo INEP ser submetido a uma finalidade diversa daquela originalmente declarada no ato da coleta, uma vez que ocorreria a subversão da autorização que possibilitou a coleta desses. Desse modo, dialoga profundamente com a noção do princípio da finalidade ao compreender que eventual tratamento secundário que desvirtue a autorização inicialmente concedida viola o dever de sigilo e, para além, fere a própria intimidade do titular. Nesse sentido:

> "7. É certo que o art. 71, IV, da Constituição confiou ao TCU a competência para a realização de inspeções e auditorias de natureza contábil, financeira, orçamentária, operacional e patrimonial nos órgãos e entidades da Administração. A atribuição dessa competência, por óbvio, supõe o reconhecimento dos meios necessários ao cumprimento desse encargo. Isso inclui a prerrogativa de requerer aos responsáveis pelos órgãos e entidades as informações necessárias à instrução de processos de auditoria e inspeção. No caso, no entanto, as informações que se quer acessar foram prestadas para uma finalidade declarada no ato da coleta dos dados e sob a garantia de sigilo do INEP quanto às informações pessoais. 8. **Nesse aspecto, a transmissão**

> **a outro órgão do Estado dessas informações e para uma finalidade diversa daquela inicialmente declarada subverte a autorização daqueles que forneceram seus dados pessoais, em aparente violação do dever de sigilo e da garantia de inviolabilidade da intimidade**. De igual modo, é plausível a alegação de que a franquia desses dados quebra a confiança no órgão responsável pela pesquisa por violação do sigilo estatístico. Há, pois, risco à própria continuidade das atividades desempenhadas pelo INEP, com efetivo prejuízo ao monitoramento das políticas públicas de educação". (MS 36.150 MC, Rel. Min. Roberto Barroso, julgado em 10.12.2018, DJe 13.12.2018, grifo nosso)

Assim, fica evidente que o Supremo Tribunal Federal está a ponderar os valores constitucionais da eficiência da Administração Pública com o regime constitucional de proteção aos direitos individuais, notadamente com a garantia de autodeterminação informativa espalhada no art. 5º, *caput* e incisos X, e LXXII, da Constituição Federal.

A postura de limitar o poder governamental no compartilhamento de dados pessoais de seus cidadãos, por outro lado, não foi igualmente observada pela CDHU, originando verdadeiro cenário de vigilância que se pretende evitar, conforme será demonstrado a seguir.

2.3. Da decisão da Corte Europeia de Direitos Humanos no caso Big Brother Watch *and Others vs. The United Kingdom: o que se pretende evitar*

Voltando à introdução do presente artigo, o leitor atento percebeu que a expressão "a fim de que vida não VOLTE a copiar a arte" foi utilizada ao versar sobre o Big Brother enquanto referência cultural. Isso porque, diversos movimentos de espionagem e vigilância muito semelhantes a esse ocorreram e são de conhecimento geral.

Nesse cenário, cita-se o denominado Sistema de Vigilância Global "Echelon", que diz respeito a um sistema de espionagem que captura informações e comunicações efetuadas pelos mais diversos meios, a exemplo da fibra óptica e da internet. Desenvolvido no contexto da 2ª Guerra mundial, seu principal objetivo em 1940 era o de espionar militares, porém, na década de 1960 passou a possibilitar a espionagem comercial e industrial e em 1990 foi utilizado enquanto meio de combate ao terrorismo e tráfico de drogas (OLIVEIRA; PESSOA, 2019). Para além, um caso de conhecimento mundial que é referência quando se trata de vigilância governamental foi a denúncia efetuada por Edward Snowden, que expôs o tratamento abusivo

de dados e verdadeira espionagem efetuada pelo governo estadunidense (GREENWALD, 2014).

Compreendendo, por conseguinte, que a vigilância não representa uma temática nova, analisar-se-á o caso paradigma europeu relativo ao *Big Brother Watch and Others vs. The United Kingdom* que fora julgado definitivamente em 25 de maio de 2021, apresentando, também, deliberações privadas entre 11 de julho de 2019, 4 e 6 de setembro de 2019 e 17 de fevereiro de 2021 (GRAND CHAMBER, 2021). Relativo ao primeiro julgamento em massa após o caso Snowden, foi resultado do questionamento das organizações não governamentais *Big Brother Watch, English PEN* e *Open Rights Group* perante a Corte Europeia de Direitos Humanos (CEDH) acerca do regime jurídico de vigilância resguardado sobre o *Regulation of Investigatory Powers*. Argumentou-se, nesse sentido, que a conduta de vigilância em massa do Governo inglês feriria o artigo 8º e 10º da Convenção Europeia de Direitos Humanos (SHARMA, 2018).

A partir da pequena introdução do caso apresentado, já é possível compreender que dele emanam nuances não abordadas no presente artigo a exemplo da interceptação em massa, que fora considerada possível pela CEDH, desde que autorizada por um órgão independente do executivo, o que não ocorrera no caso concreto (ZALNIERIUTE, 2021). No entanto, ele se mostra um excelente paradigma para demonstrar aquilo que o presente artigo visa evitar a partir de limitações à possibilidade de compartilhamento de dados, isto é, um cenário de vigilância e desconfiança da população para com o seu governo.

Ademais, verifica-se ponto de grande valia à discussão relativa aos limites ao compartilhamento de dados entre os entes estatais para que se evite um cenário de vigilância, uma vez que a CEDH entendeu pela possibilidade de compartilhamento de informações (dados pessoais) entre as autoridades do Reino Unido e o serviço de inteligência estadunidense, desde que presentes medidas contra eventuais abusos, para além de sujeição a revisão posterior (ZALNIERIUTE, 2021). Nesse cenário, a Corte Europeia compreendeu que a legislação interna seria clara sobre a possibilidade de intercâmbio de informações entre as agências de inteligência dos Estados Unidos e do Reino Unido, sendo recomendado que o material fosse apenas analisado e investigado caso todas as exigências para uma interceptação nacional fossem supridas. Em outros termos, os dados compartilhados apenas deveriam sofrer eventual tratamento se houvesse autorização e existisse um cenário que exigisse essa intervenção (OLIVEIRA; PESSOA, 2019).

No Brasil, a hipótese de interceptação em massa não seria viável, pois não há legislação que autorize essa conduta. Entretanto, o que mais chama atenção na situação retratada foi se considerar possível e não afrontoso aos direitos humanos a possibilidade de compartilhamento de dados pessoais entre os governos em questão, desde que só fosse realizado um tratamento posterior caso houvesse um cenário propício para tanto.

Essa visão não poderia ser importada para o cenário brasileiro, pois conforme fora amplamente desenvolvido nos tópicos anteriores, o tratamento secundário que justifica o compartilhamento de dados não poderá subverter o tratamento inicial que possibilitou a coleta desses. Essas limitações demonstram-se imprescindíveis em qualquer contexto, pois o Estado, seja qual for, sempre deverá garantir a segurança de seus cidadãos e um cenário de vigilância igual o retratado nunca será a solução.

Considerações Finais

Ante todo o exposto, é possível afirmar que o tratamento de dados pessoais é extremamente relevante para o desempenho estatal, sendo o compartilhamento desses essencial para a dinâmica governamental. No entanto, a relação verticalizada entre Estado e cidadão torna imprescindível a adoção de limites a eventual compartilhamento público-público, para que não ocorra um cenário de vigilância tal qual o denunciado por Edward Snowden e questionado em juízo europeu pela organização não governamental *Big Brother* e outros.

Dessa maneira, a LGPD em seu artigo 26 traz a finalidade específica do tratamento secundário a ser realizado enquanto importantíssima baliza a referida limitação. Contudo, também ficou evidente que a experiência internacional pode ser de grande valia ao tema. Nesse sentido, os art. 6, 4, c, d, e da GDPR demonstram que a natureza dos dados que serão compartilhados, eventuais consequências que o tratamento secundário poderá trazer ao particular e a anonimização dessas informações também poderão influenciar na possibilidade do compartilhamento pretendido.

Por fim, a análise das decisões do Supremo Tribunal Federal - em específico: ADI 6529 MC-Ref, ADI 6387 MC-Ref, SL 1103 e MS 36150 MC - ainda possibilitou a conclusão de que a corte brasileira tende a ponderar a eficiência da Administração Pública em relação a proteção dos direitos individuais dos indivíduos, de modo a não prevalecer a supremacia do interesse

público no que diz respeito ao tratamento de dados pessoais. Pode-se, assim, concluir que a possibilidade de compartilhamento de dados entre os entes que compõem o Poder Público dependerá da análise concreta da situação, devendo-se levar em consideração as limitações acima descritas, para além dos princípios constitucionais da proporcionalidade e razoabilidade.

Referências bibliográficas

ARIENTE, Eduardo Altomare; SANTOS, Alessandro Santiago; PALHARES, Gabriela Capobianco; GOMES, Jefferson de Oliveira. A privacidade em tempos de pandemia e a escada de monitoramento e rastreio. *Estudos avançados* 34 (99), 2020.

BLACK, Gillian e STEVENS, Leslie. Enhancing Data Protection And Data Processing In The Public Sector: The Critical Role Of Proportionality And The Public Interest. *Scripted*. Vol. 10, n. 1, 2013, p. 95

BRASIL. *Lei Geral de Proteção de Dados Pessoais* (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 12 de novembro de 2021.

BRASIL. Supremo Tribunal Federal. ADI 6529 MC-Ref, Relator(a): CÁRMEN LÚCIA, Tribunal Pleno, julgado em 11/10/2021, processo eletrônico DJe-210. Divulgado em 21-10-202. Publicado em 22-10-2021. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur454781/false>. Acesso em: 12 de novembro de 2021.

BRASIL. Supremo Tribunal Federal. ADI 6387 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, Processo Eletrônico DJe-270 Divulgado 11-11-2020 Publicado 12-11-2020. Disponível em:<https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false>.Acesso em: 12 de novembro de 2021.

BRASIL. Supremo Tribunal Federal. SL 1103. Relator: Min. Presidente. Decisão proferida pelo Min. DIAS TOFFOLI. Julgamento: 30/05/2019. Publicação: 04/06/2019. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/despacho986145/false>.Acesso em: 12 de novembro de 2021.

BRASIL. Supremo Tribunal Federal. MS 36150 MC. Relator: Min. Roberto Barroso. Julgamento: 10/12/2018. Publicação: 13/12/2018. Disponível em: < https://jurisprudencia.stf.jus.br/pages/search/despacho937080/false>. Acesso em: 12 de novembro de 2021.

CELLA, J. R. G.; COPETTI, R. Compartilhamento de Dados Pessoais e a Administração Pública Brasileira. *Revista de Direito, Governança e Novas Tecnologias*, Maranhão, v. 3, p. 39-58, jul./dez. 2017.

FINKELSTEIN, Cláudio; FINKELSTEIN, Maria Eugênia. Privacidade e Lei Geral de Proteção de Dados Pessoais. *Revista de Direito Brasileira*. Florianópolis, SC. v. 23 | n. 9. p. 284-301. Mai./ago. 2019

GENERAL DATA PROTECTION REGULATION. Disponível em: <https://gdpr.algolia.com>. Acesso em: 12 de novembro de 2021.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados: uma breve análise da sua definição e papel na LGPD. *Revista do Advogado*, São Paulo, n. 144, nov. 2019.

GRAND CHAMBER. *Case of Big Brother Watch and Others v. United Kingdom.* STRASBOURG, 2021. Disponível em: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]}> . Acesso em 12 de novembro de 2021.

GREENWALD, Gleen. S*em lugar para se esconder: Edward Snowden, a NSA e a espionagem do governo americano*. Rio de Janeiro: Sextante, 2014

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. *In*: SOUZA, Carlos Affonso (coord.); MAGRANI, Eduardo (coord.); SILVA, Priscilla (coord.). *Tratado de Proteção de Dados Pessoais.* Rio de Janeiro: Forense, 2021

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014, cap. 1

MENDES, Laura Schertel; MACHADO, Diego; GASIOLA, Gustavo Gil. A Administração Pública entre transparência e proteção de dados. *Revista de Direito do Consumidor. vol*. 135/2021. p. 179 - 201. Maio - Junho, 2021.

MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz(coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

OLIVEIRA, Rafael dos Santos. PESSOA, João Pedro Seefeldt. Big Brother Watch and Others v. The United Kingdom": el régimen de vigilancia social y el derecho al respecto a la vida privada y familiar y a la libertad de expresión frente a la Corte Europea de Derechos Humanos. *Pensar: revista de ciências jurídicas.* Fortaleza, v. 24, n. 3, p. 1-12, jul./set. 2019.

SHARMA, Chinmayi. Summary: Big Brother Watch and Others v. The United Kingdom. *Lawfareblog*, 2018. Disponível em:<https://www.lawfareblog.com/summary-big-brother-watch-and-others-v-united-kingdom> Acesso em: 12 de novembro de 2021.

SUPREMO TRIBUNAL FEDERAL. STF impõe limites ao compartilhamento de dados do Sistema Brasileiro de inteligência (Sisbin). *Portal STF*, 2020. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=449549&ori=1>. Acesso em: 12 de novembro de 2021.

WIMMER, Miriam. Limites e possibilidades para o uso secundário de dados pessoais no Poder Público: lições da Pandemia. *Revista Brasileira de Políticas Públicas*. Uniceub, volume 11, nº 1. Brasília, abril de 2021 a.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz(coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais.* Rio de Janeiro: Forense, 2021b.

ZALNIERIUTE, Monika. Procedural Fetishism and Mass Surveillance under the ECHR. *Verfassungsblog on Matters Constitucional*, 2021. Disponível em: <https://verfassungsblog.de/big-b-v-uk/>. Acesso em: 12 de novembro de 2021.

A PROTEÇÃO DE DADOS NO BRASIL E NA UNIÃO EUROPEIA: PERSPECTIVA COMPARADA ENTRE A INDEPENDÊNCIA E AUTONOMIA DAS AUTORIDADES DE FISCALIZAÇÃO

Andressa Carvalho Pereira[1]

Dispositivo LGPD	Dispositivo RGPD
Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. §1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. §2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. §3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias. **Art. 55-J**. Compete à ANPD: I - zelar pela proteção dos dados pessoais, nos termos da legislação; II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;	**Art. 51.** 1. Os Estados-Membros estabelecem que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do presente regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União («autoridade de controlo»). 2. As autoridades de controle contribuem para a aplicação coerente do presente regulamento em toda a União. Para esse efeito, as autoridades de controle cooperam entre si e com a Comissão, nos termos do capítulo VII. 3. Quando estiverem estabelecidas mais do que uma autoridade de controle num Estado-Membro, este determina qual a autoridade de controle que deve representar essas autoridades no Comité e estabelece disposições para assegurar que as regras relativas ao procedimento de controle da coerência referido no artigo 63.o, sejam cumpridas pelas autoridades. 4. Os Estados-Membros notificam a Comissão das disposições do direito nacional que adotarem nos termos do presente capítulo, até 25 de maio de 2018 e, sem demora, de qualquer alteração posterior a essas mesmas disposições. [...]

[1] Advogada da área de Resolução de Conflitos, com atuação especialmente em contencioso cível perante Tribunais de Justiça Estaduais e Superiores. Formada em Direito pela Universidade de Brasília. Integrante do grupo de pesquisa Observatório da LPGD.

Introdução

Influenciado pelo debate acerca da proteção de dados pessoais, em âmbito nacional e internacional, amplamente inspirado pela Europa, que elaborou o Regulamento Geral sobre a Proteção de Dados (RGPD), o Brasil notou cada vez mais a importância de criar a própria lei de proteção dos dados pessoais e como regular essa proteção no país. Avançando nessa matéria, foi aprovada a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em agosto de 2021. Posteriormente, através da Lei n. 13.853/2019, que alterou a LGDP, foi criada a Autoridade Nacional de Proteção de Dados – ANPD, o seu contexto e as implicações da sua criação serão expostos mais a frente deste artigo.

Na Europa, inicialmente, o que regulamentou a proteção dos dados dos cidadãos foi a Diretiva 95/46/CE, posteriormente substituída pelo atual regulamento, que entrou em vigor em maio de 2016 e é aplicável desde maio de 2018, influenciando não somente a comunidade europeia, mas todos os países, empresas ou pessoas que queiram prestar serviços aos cidadãos de qualquer um dos países do bloco. Para eles a proteção cabe a cada um dos 27 (vinte e sete) países integrantes do bloco, já que estes devem instituir as suas autoridades nacionais.

Além delas há a Autoridade Europeia para a Proteção de Dados (AEPD). A ela cabe a função de assegurar que as instituições e órgãos da UE respeitem o direito das pessoas ao processamento de seus dados pessoais. Em síntese, cabe à autoridade as funções de supervisionar o processamento de dados, aconselhamento das instituições e órgãos da UE, lidar com reclamações e conduzir investigações, lidar com as autoridades nacionais de cada Estado-Membro e monitorar novas tecnologias que possam impactar a proteção de dados. [2]

Nessa perspectiva, este artigo visa analisar a questão da independência das autoridades de proteção de dados, no Brasil e na Europa, em uma perspectiva comparada à luz do Projeto de Lei (PL) 5276/2016 e os debates que envolveram a criação da autoridade brasileiro e casos europeus que expressam o tratamento que é dado a esses órgãos de supervisão.

[2] Sobre o funcionamento da Autoridade de Proteção de Dados da UE, com sede em Bruxelas, na Bélgica, verificar: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_en.

1. Estudo comparativo entre as Autoridades de Proteção de Dados no Brasil e na União Europeia

As autoridades de proteção de dados constituem um dos principais atores para a execução das políticas de privacidade e proteção das informações pessoais e, do mesmo modo, conscientização da população e sanção no caso de descumprimentos. Nos últimos anos, à medida que a internet evoluiu, também se tornou mais necessário aprimorar as regulamentações de dados existentes, de forma a permitir que a relação com os usuários (detentores dos dados) se tornasse mais simétrica. Com isso, é possível que estes indivíduos tenham maior controle sobre os próprios dados pessoais e compreendam melhor a importância que eles possuem. Além disso, as pessoas podem dimensionar o perigo que se apresenta na ausência de regulamentação e fiscalização apropriada para salvaguardar as informações pessoais (LORENZON, 2021).

Nesse papel institucional desempenhado pelas autoridades, a autonomia administrativa, decisória e financeira são atributos fundamentais, juntamente com a participação social. Em outros exemplos fora do país, como no caso da antiga autoridade Argentina, a falta de autonomia administrativa reduziu o *enforcement* da autoridade, com o exemplo podemos depreender que tal aspecto é fulcral para o seu pleno funcionamento (BEZERRA, 2019).

Para além da autonomia, outro requisito desejável e recomendável para autoridades de proteção é a independência. Apesar desse conceito não ter sido cunhado no Brasil, Danilo Doneda afirma que "o recurso a uma autoridade administrativa independente para a proteção de dados pessoais é uma tendência fortemente enraizada em alguns ordenamentos", sobretudo no modelo europeu de proteção de dados (DONEDA, 2006, p. 385). "Por isso, a existência de uma autoridade nacional forte, independente e eficiente é a regra em países europeus" (BEZERRA, 2019, p. 56), visando o pleno funcionamento do seu *enforcement.*

Na realidade brasileira, a autonomia da autoridade de dados foi restringida, pois esta foi criada vinculada à Presidência da República. Nesse sentido, o modelo que conferiria autonomia seria aquele de agência reguladora, que tem como conceito, em sentido amplo, "qualquer órgão da Administração Direta ou entidade da Administração Indireta com função de regular a matéria específica que lhe está afeta" (DI PIETRO, 2021, p. 618). A gestão, organização e o controle social dessas agências são regulados pela Lei n. 13.848/2019. Apesar de existirem outras entidades com função reguladora, como o Banco Central, a Comissão de Valores Mobiliários e o Conselho Monetário Nacional, para os fins da Lei n. 13.848/2019 e da Lei nº 9.986, de 18-7-00 (que dispõe sobre a gestão de recursos humanos das agências reguladoras), somente são

consideradas as previstas no art. 2º da Lei n. 13.848/2019, além das autarquias especiais, integrantes da administração indireta estão sujeitas ao princípio da especialidade, ou seja, operam na matéria atribuída a elas por Lei (DI PIETRO, 2021).

Adentrando no contexto dessas agências, apesar da regulação não ser exercida somente por elas, como mencionado no parágrafo anterior, tal papel é mais concentrado nesse modelo institucional, muito inspirado no modelo regulatório norte-americano que deposita confiança nas agências. Nesse espectro, o regime jurídico desse modelo reforça a autonomia e possibilita uma certa blindagem contra influências políticas no seu processo decisório. Nesse sentido, a principal vantagem seria a imparcialidade técnica (ARAUJO, 2017).

No Brasil, o modelo adotado não foi o de agência reguladora, mas sim um modelo vinculado à presidência. Um estudo realizado pelo Instituto Brasileiro de Defesa do Consumidor- (Idec) - em que foi analisado de forma comparativa a autonomia das autoridades de proteção de dados na América Latina, em específico na Argentina, Colômbia e Uruguai, as experiências revelaram que o desenho institucional de vinculação da autoridade à presidência da república tende a mitigar a independência decisória. A experiência argentina, por exemplo, demonstrou que nesse mesmo arranjo, após 7 (sete) anos da sua criação, foi necessário passar por um rearranjo institucional. Nesse ínterim, o modelo mais recomendável seria aquele que atribui personalidade jurídica própria à autoridade, desvinculada da administração direta (SIMÃO; OMS; TORRES, 2019).

Apesar de não ser possível afirmar que todas as agências reguladoras possuem independência, a ascensão desse modelo institucional foi pensada como um elemento para garantir legitimidade, especificidade técnica dos funcionários e o comprometimento das políticas nos setores regulados (SIMÃO; OMS; TORRES, 2019).

Sobre a autoridade brasileira, antes da entrada em vigor da LGPD, tramitavam no Congresso propostas que visavam regulamentar o uso dos dados pessoais no Brasil. O Projeto de Lei nº 5276/2016 constitui-se como a LPGD em fase embrionária e o seu debate foi iniciado em 2010 e teve como relator o Deputado Orlando Silva (PC do B-SP). Esse projeto teve como objetivo "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa individual". [3] Ademais, com os avanços das

[3]CÂMARA DOS DEPUTADOS, *PL 5276/2016.* Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 14 de setembro de 2021.

consultas públicas e debate em vários setores da sociedade, uma preocupação que passou a nortear a problemática foi: qual órgão seria responsável por fiscalizar o cumprimento da legislação de proteção de dados no país?

Em um breve contexto histórico da discussão sobre a ANPD, um dos últimos atos da gestão da presidenta Dilma Rousseff foi o encaminhamento do PL 5276/2016 à Câmara. A nova versão do anteprojeto trouxe como principal novidade, após a consulta pública que contou com cerca de 1,3 mil contribuições, a criação de um órgão competente para fiscalizar o governo e as empresas. A ideia seria que esse órgão possuísse recursos próprios, sem vinculação ao Ministério. O texto atribuía a essa autoridade as tarefas de fiscalização, estabelecimento de medidas de proteção aos dados sensíveis, cobrança de relatórios de impacto de privacidade, entre outras tarefas. Além do órgão competente, criava o Conselho Nacional de Proteção de Dados e da Privacidade, com o objetivo de sugerir ações, disseminar o estudo de proteção de dados e tarefas correlatas. O projeto também previa sanções, caso houvesse descumprimento, sendo multas, publicização da infração, anonimização dos dados pessoais, bloqueio dos dados, suspensão da operação de tratamento dos dados, cancelamento dos dados e suspensão do funcionamento do banco de dados. Avançando na sua tramitação, o PL foi apensado ao PL 4060/2012. [4]

Adiante, em outubro de 2016, foi criada a Comissão Especial para a análise de ambos os projetos, tendo como relator Orlando Silva e como presidente Bruna Furlan. Com a entrada em vigor do Regulamento sobre a Proteção de Dados da União Europeia, cresceu o apoio para a aprovação da LGPD. Porém, mesmo após a aprovação do projeto no Senado sem grandes vetos, o projeto foi sancionado pelo Presidente Michel Temer com vetos importantes, dentre eles a criação da ANPD.

Nos últimos dias do seu governo, o presidente publicou a Medida Provisória nº 869, com uma configuração diferente daquela aprovada no Congresso, diminuindo a autonomia da autoridade, por estar subordinada à Presidência da República. Após o importante veto, foi criada uma comissão mista para emitir Parecer sobre a MP. O Parecer final incluiu sugestão para a revisão, que deveria ocorrer em 2 (dois) anos, a partir da data da entrada em vigor, conforme art. 55-A, §2º, da Lei n. 13.709/2018, do modelo da autoridade nacional, com a possibilidade de transferi-la para a administração indireta, o que a tornaria muito mais independente em

[4] INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. Idec. Linha do tempo. Disponível em: <https://idec.org.br/dadospessoais/linha-do-tempo>. Acesso em 14 de setembro de 2021.

âmbito político, financeiro e administrativo. Com a aprovação do relatório pelo Senado, ele foi encaminhado ao presidente Jair Bolsonaro para sanção. Com novos vetos, o presidente aprovou a criação da autoridade.

Contudo, mesmo diante da necessidade de criação da autoridade, influenciado ainda pela pandemia que dificultou ainda mais a capacidade das empresas e do poder público de se adequarem à LGPD, foi editada a Medida Provisória nº 959, postergando a entrada em vigor da lei para 3 de maio de 2021 e as sanções para valer a partir de janeiro de 2022, por meio do PL 1.179/2020. Porém, o artigo da MP, que postergava a entrada em vigor da lei, foi vetado posteriormente e, por isso, a sua validade ficou sendo a data de conversão em lei da MP 959, e a entrada em vigor das sanções se manteve para agosto de 2021, como previsto inicialmente. Após esse longo período, temos em 2020, a nomeação do Conselho Diretor da ANPD, com isso entrou em vigor o Decreto nº 10.474/2020, que estruturou o funcionamento da autoridade. [5]

Comentando mais detidamente sobre o modelo institucional da ANPD, no Brasil muito se falou sobre o veto, do então Presidente Michel Temer na criação da autoridade, pois à época a justificativa para tal decisão foi a inconstitucionalidade formal[6] por vício de origem, uma vez que a autoridade estivesse relacionada ao Poder Executivo, caberia a este legislar sobre o tema, conforme embasamento trazido no art. 61, §1º, inciso II, alíneas *a* e *c* da Constituição Federal (TORRES, 2021):

> Art. 61. A iniciativa das leis complementares e ordinárias cabe a qualquer membro ou Comissão da Câmara dos Deputados, do Senado Federal ou do Congresso Nacional, ao Presidente da República, ao Supremo Tribunal Federal, aos Tribunais Superiores, ao Procurador-Geral da República e aos cidadãos, na forma e nos casos previstos nesta Constituição.
> §1º São de iniciativa privativa do Presidente da República as leis que:
> a) criação de cargos, funções ou empregos públicos na administração direta e autárquica ou aumento de sua remuneração;
> [...]
> e) criação e extinção de Ministérios e órgãos da administração pública, observado o disposto no art. 84, VI;

[5] Idem.
[6] Esse vício, segundo a doutrina, seria aquele em que são praticados atos por órgãos que não possuem competência para tanto.

Entretanto, a decisão foi vista como uma atitude estratégica, pois uma vez independente a autoridade também regularia atos do Poder Executivo. Nessa perspectiva, nota-se que no Brasil, a ANPD necessita de mais independência na sua atuação, uma vez que a prática internacional demonstra que modelos dessa natureza se mostram mais eficientes, uma vez que a autoridade poderá decidir de forma autônoma, com poderes de regular até mesmo ações e comportamentos do próprio Poder Executivo. Nessa senda, se mostra imperioso que haja uma mudança em sua natureza jurídica, pois interferências futuras e presentes podem mitigar a sua força de atuação, impedindo, inclusive, que a LGPD não seja colocada em prática da forma devida.

À vista de todo o exposto, que envolve o complexo assunto do modelo institucional a ser adotado por uma autoridade de proteção de dados, é importante analisar em casos práticos como se dão as suas decisões, sob a ótica da independência, para isso será analisado o contexto da União Europeia.

1.1. O contexto europeu de proteção de dados: uma análise a partir dos casos Comisão Europeia v. Hungria, Comissão Europeia v. República da Áustria e Maximilliam Schrems v. Comissário de Proteção de Dados.

Adentrando no contexto europeu, a supervisão independente é um aspecto importante, por isso as autoridades devem ser indispensavelmente assim, para que possam garantir de forma efetiva os direitos dos indivíduos e o uso de seus dados. Na UE cada Estado-Membro deve criar a sua autoridade local. Como em muitos casos o tratamento dos dados pessoais envolve diversos atores, que se encontram em distintos países e, até mesmo fora da UE, as autoridades devem cooperar entre si para garantir a proteção eficaz dos indivíduos em toda a Europa. Além das autoridades, há o Comitê Europeu de Proteção de Dados (EDPB), o papel do Comitê é a emissão de pareceres, mas além disso monitora a correta aplicação do regulamento aconselhando sempre a tomada de decisão que visem as melhores práticas sobre o assunto. [7]

[7] Handbook on European data protection law - 2018 edition, European Union Agency for Fundamental Rights and Council of Europe, 2018. Disponivel em: <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition>. Acesso em 12 de setembro de 2021.

Para entender melhor a atuação das autoridades na UE há excelentes casos práticos que exemplificam o assunto, como o caso da Comissão Europeia v. Hungria[8]. Nesse caso, o Tribunal entendeu que a competência conferida à autoridade deve ser exercida por ela de forma plena sem que as autoridades públicas precisem disponibilizar mão de obra para o trabalho. O caso versa sobre interferência da Hungria no mandato do supervisor responsável pela autoridade local, frente ao art. 28 da Diretiva 95/46/CE que incumbe a cada estado-membro a criação de uma ou mais autoridades públicas para aplicação do previsto na diretiva. O argumento da Hungria é no sentido de que, com a ausência de previsão na diretiva da duração do mandato das pessoas encarregadas e a organização estrutural, os estados membros seriam livres para determinar a estrutura institucional da sua respectiva autoridade, o que envolve a escolha da pessoa que estará à frente da autoridade e a duração do seu mandato, incluindo a possibilidade de destituir o encarregado antes do tempo. Por isso, a única exigência contida no art., segundo argumentam, seria a atuação livre de interferências à autoridade. No entanto, ao contrário do argumentado, o Tribunal decidiu favoravelmente à independência total da autoridade à medida que os membros não estão vinculados a qualquer ordem externa. Desse modo, o sinal de risco de qualquer interferência política na atuação dos membros deve ser mitigado, mas isso não significa que todas as decisões serão completamente imparciais, mas devem ser dadas condições para que assim o sejam. Nesse caso específico, a Hungria teria obrigado o supervisor a ceder o cargo, com base em seus próprios critérios, o que é incompatível com o requisito da independência.

Ademais, jurisprudência muito similar é o caso Comissão Europeia v. República da Áustria[9]. Nesse caso, o Tribunal decidiu, assim como para a Hungria, que a indicação de membros para a autoridade de proteção da Áustria prejudicou a sua independência, uma vez que era necessário prestar esclarecimentos sobre o trabalho desenvolvido.

Por último, o caso Maximilliam Schrems v. Comissário de Proteção de Dados [10] versa, além da transferência de dados transfronteiriços, da questão da independência das autoridades na UE. A situação fática versa sobre um pedido apresentado pelo Sr. Schrems para uma

[8] InfoCuria Jurisprudência. Disponível: <em:https://curia.europa.eu/juris/document/document.jsf?text=&docid=150641&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=604422>. Acesso em 15 de setembro de 2021.

[9] InfoCuria Jurisprudência. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=604242>. Acesso em 15 de setembro de 2021.

[10] EUR, LEX. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362. Acesso em 13 de setembro de 2021.

investigação de compartilhamento de dados pelo Facebook aos Estados Unidos, que ficavam mantidos em servidores localizados no país. O problema se deu a partir do pedido do requerente para investigação da transferência, no que diz respeito à sua legalidade, porém a autoridade irlandesa rejeitou a queixa, alegando que a decisão da Comissão sobre a adequação do regime de proteção de dados dos EUA impedia a análise. Não obstante essa decisão, a Corte de Justiça da UE decidiu que a decisão não reduziria os poderes de monitoramento e garantia de conformidade com as suas regras, pois derivava de um direito primário, previsto no art. 16 do Tratado sobre o Funcionamento da União Europeia "o estabelecimento de autoridades de supervisão independentes é, portanto, [...] um componente essencial da proteção dos indivíduos no que diz respeito ao tratamento de dados pessoais". Portanto, decidiu-se nesse caso pela "supremacia" da autoridade nacional para contestar nos tribunais nacionais quando a autoridade supervisora considerar a reclamação bem fundamentada. [11]

Nessa seara, nota-se que a independência faz parte do modelo regulatório adotado pelos países integrantes do bloco, mas até que ponto se daria essa independência? Tal questionamento foi levantado quando da discussão do caso Comissão Europeia v. República Federal da Alemanha[12]. Neste caso, a Comissão Europeia solicitou ao Tribunal de Justiça da UE que declarasse como incorreta a atitude do Estado Alemão ao transpor incorretamente o requisito de independência das autoridades de supervisão, nos termos do art. 28 (1) da Diretiva de Proteção de Dados. Na ocasião, o Tribunal decidiu que as autoridades são as "guardiãs" do tratamento de dados, logo o estabelecimento delas em cada estado-membro é imperativo para garantir a eficiência do monitoramento do uso de dados. Dessa forma, a atuação delas deve estar livre de qualquer interferência externa, o que inclui as autoridades públicas. A conclusão obtida pelo Tribunal ao analisar o caso foi a de que as autoridades na Alemanha não eram totalmente independentes, já que supervisionadas por autoridades públicas e, por isso, não estavam conforme a independência conferida pela lei da UE. [13]

Diante das jurisprudências formadas sobre o assunto da "independência total", este requisito foi expressamente incorporado pelo RGPD, de acordo com o regulamento exercer as atividades com total independência implica que os membros não recebam influência de atores externos à autoridade; para além, os membros que atuam na autoridade devem evitar o conflito

[11] Handbook on European data protection law - 2018 edition.
[12] InfoCuria Jurisprudência. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=79752&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=604128>. Acesso em 15 de setembro de 2021.
[13] Handbook on European data protection law - 2018 edition.

de interesses, para isso não devem praticar ações contrárias ao que preceitua a lei; os estados-membros devem garantir que elas conseguirão operar de forma satisfatória, sendo assim devem disponibilizar recursos, mas ao mesmo tempo deixar livre para que componham o seu quadro de pessoal e devem possuir orçamento próprio para desempenhar as suas funções. [14]

Além do mencionado anteriormente, o RGPD prevê que cada autoridade deve, como órgão principal de supervisão da legislação de proteção de dados, possuir catálogo abrangente de tarefas e poderes.Além da função de monitoramento, devem ter poder de supervisão, investigação, correção e ação consultiva, conforme enumerado no art. 58 do regramento. [15]

Diante dos pontos supramencionados, no contexto da União Europeia é perceptível um apego com a independência total das autoridades de proteção de dados, instituídas por cada estado-membro. Tal entendimento se torna perceptível diante de decisões do Tribunal de Justiça Europeu e do próprio do Regulamento sobre a Proteção de Dados. Para reforçar o exposto, na UE, desde a década de 70, já havia órgãos independentes e a Diretiva 46/95/CE estava em linha com esse entendimento, como no caso da Alemanha, a *Datenschutzbeauftrager*, data da década de 70. Atualmente com o RGPD, as Autoridades de Proteção de Dados, em inglês conhecidas como *Data Protection Authorities* - DPA's, funcionam de forma independente, inclusive no art. 8º da Carta de Direitos Fundamentais da UE, ao ser previsto o direito à proteção de dados como autônomo, é assinalada a independência funcional.

2. Considerações finais

Em conclusão, o artigo buscou trazer de forma mais objetiva aspectos comparativos entre os contextos de independência e autonomia das autoridades de proteção de dados no Brasil e na União Europeia, por meio de casos práticos no caso europeu e do caminho legislativo de criação da ANPD, já que ainda é bastante recente a sua criação. O intuito desse formato de exposição é possibilitar ao leitor uma leitura breve sobre o assunto, mas consistente e que dê insumos para pesquisas posteriores em âmbito nacional e internacional.

Com base no exposto ao longo do artigo, nota-se que há diferenças consideráveis entre os modelos aqui comparados, na Europa podemos concluir que a legislação de proteção de dados vem se desenvolvendo de forma diferenciada em relação a outros países, pois já era possível encontrar legislações próprias para regular o assunto desde a década de 70. Com o

[14] Idem.
[15] Idem.

tempo, essas legislações foram unificadas, gerando a Diretiva 95/46/CE e, posteriormente, foi criado o Regulamento Geral sobre a Proteção de Dados em 2016.

Já no Brasil o país avança consideravelmente no assunto. A ANPD completou 1 (um) ano de atuação em novembro de 2021 e segundo dados do sítio eletrônico da autoridade foram realizados e concluídos 15 (quinze) circuitos deliberativos, publicadas 17 (dezessete) portarias, celebrados 4 (quatro) acordos de cooperação técnica, concluída 100% (cem por cento) da agenda regulatória e publicados 6 (seis) materiais, com parceiros, como cartilhas e artigos. Outro dado importante foi o recebimento de mais de 3.100 (três mil e cem) demandas de dúvidas sobre implementação da LGPD. Tais dados demonstram como a autoridade vem ganhando cada vez mais notoriedade no tema da proteção de dados.

Referências bibliográficas

ARAÚJO, Valter. Os quatro pilares para a imparcialidade técnica das agências reguladoras. Revista Jurídica da Presidência Brasília v. 20 n. 120 Fev./Maio, 2017, p. 64-91

http://dx.doi.org/10.20499/2236-3645.RJP2018v20e120-1659. Disponível em: https://revistajuridica.presidencia.gov.br/index.php/saj/article/view/1659/1231. Acesso em 13 de nov. de 2021.

BEZERRA, Maria. Autoridade Nacional de Proteção de Dados Pessoais: a importância do modelo institucional independente para a efetividade da lei. Caderno Virtual, IDP, v. 2, n. 44, abr/jun. 2019. Disponível em: <file:///C:/Users/Sara/Downloads/3828-13366-1-SM.pdf>. Acesso em 14 de nov. de 2021.

CÂMARA DOS DEPUTADOS, Projeto de Lei n. 5276/2016. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 14 de setembro de 2021.

DI PIETRO, Maria Sylvia Zanella. Direito Administrativo. Grupo GEN, 2021. 9788530993351. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530993351/>. Acesso em 02 novembro de 2021.

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

EUR,LEX. Maximilliam Schrems v. Data Protection Commissioner. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362. Acesso em 13 de setembro de 2021.

European Union Agency for Fundamental Rights and Council of Europe. Handbook on European data protection law - 2018 edition. Disponivel em: <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition>. Acesso em 12 de setembro de 2021.

GOVERNO DO BRASIL, Sítio eletrônico da Autoridade Nacional de Proteção de Dados. ANPD completa 1 ano. Disponível em: <https://www.gov.br/anpd/pt-br/ANPD%20completa%201%20ano/>. Acesso em 12 de dezembro de 2021.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia

(LGPD E GDPR) e seus respectivos instrumentos de enforcement. Revista do Centro de Excelência Jean Monnet da FGV Direito Rio. Organizadora Paula Wojcikiewicz Almeida, — Rio de Janeiro: FGV Direito Rio, 2021, p 39-52. Disponível em: <https://bibliotecadigital.fgv.br/ojs/index.php/rpdue/issue/view/4599>. Acesso em 02 de novembro de 2021.

LGPD, Lei Geral de Proteção de Dados. Lei nº 13.709 de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 15 de outubro de 2021.

SIMÃO, B; OMS, J; TORRES, L. Autoridades de Proteção de Dados na América Latina. Um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. Instituto Brasileiro de Defesa do Consumidor. Disponível em:<https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina>. Acesso em 12 de setembro de 2021.

TORRES, Isabela Macedo. A importância da implementação da Autoridade Nacional de Proteção de Dados. Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro - PGE-RJ, Rio de Janeiro, Edição Especial N.1. Disponível em: <https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/160>. Acesso em 10 de setembro de 2021.

InfoCuria Jurisprudência. Comissão Europeia v. República Federal da Alemanha. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=79752&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=604128>. Acesso em 15 de setembro de 2021.

InfoCuria Jurisprudência, Comissão Europeia v. República da Áustria. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=604242>. Acesso em 15 de setembro de 2021.

InfoCuria Jurisprudência, Comissão Europeia v. Hungria. Disponível: <em:https://curia.europa.eu/juris/document/document.jsf?text=&docid=150641&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=604422>. Acesso em 15 de setembro de 2021.

UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados. Disponível em: https://gdpr-info.eu/. Acesso em 10 de outubro de 2021.

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de out de 1995, relativa à protecção das pessoas singulares não que diz respeito ao tratamento de dados pessoais e à livre circulação de dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em 14 de novembro de 2021.


OBSERVATÓRIO DA
LGPD
UNIVERSIDADE DE BRASÍLIA