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

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


OBSERVATÓRIO DA
LGPD
UNIVERSIDADE DE BRASÍLIA