REVISTA ELETRÔNICA DA PGE RJ
ISSN 2595-0630
(DOI): 10.46818/ v4i3.269

RESPEITANDO PRINCÍPIOS NO COMPARTILHAMENTO DE DADOS: BASES DE UM RACIOCÍNIO JURÍDICO

RESPECTING PRINCIPLES IN DATA SHARING: BASES FOR LEGAL REASONING

BERNARDO JOSÉ OLIVEIRA ARAUJO[1]

RESUMO: O objetivo do artigo é fornecer recomendações para o desenho de cláusulas contratuais para o compartilhamento de dados pessoais entre um controlador e um operador. Iniciamos o artigo comentando o primeiro guia publicado pela Autoridade Nacional de Proteção de Dados com diretrizes não vinculantes a respeito dos agentes de tratamento e do encarregado. O guia é o primeiro do gênero publicado pela autoridade reguladora brasileira e está estruturado em sete capítulos. Optou-se por dividir este item em oito tópicos relevantes, que são: agentes de tratamento; controlador; controladoria conjunta; controladoria singular; operador; operadores subcontratados; encarregado: o DPO brasileiro; e comentários adicionais. Em seguida, resumimos o sistema de responsabilidade civil estruturado pela Lei Geral de Proteção Dados Pessoais para os agentes de tratamento. A partir deste momento, focamos em recomendações objetivas acerca dos tópicos que merecem especial atenção em negociações de instrumentos contratuais que versem especificamente sobre dados pessoais. Dando prosseguimento às orientações, ampliamos o escopo das recomendações para o plano teórico, de modo a definir bases de um raciocínio jurídico que, pelo uso de princípios, funcione como um guia capaz de conduzir intérpretes em casos de compartilhamento de dados pessoais. Por fim, concluímos com um apanhado geral das ideias apresentadas no artigo.

PALAVRAS-CHAVE: LGPD. Privacidade. Proteção de Dados Pessoais. Segurança da Informação. Contratos.

ABSTRACT: The scope of the article is to provide recommendations on how to structure contractual clauses for the sharing of personally identifiable information between a controller and a processor. We initiate the article by commenting the first guide published by the National Data Protection Authority with non-binding guidelines regarding processing agents and the Brazilian Data Protection Officer. The guide is the first of its kind published by the Brazilian regulatory authority and is divided into seven chapters. We decided to divide this item into eight relevant topics, which are: processing agents; controller; joint controllership; singular controllership; processor; subcontracted processors; encharged: the Brazilian DPO. Additional comments. Later, we summarize the civil liability framework for processing agents designed by the Brazilian General Data Protection Law. From this moment on, we focus on straightforward recommendations regarding issues that deserve special attention in the negotiation of contractual agreements that deal specifically with personally identifiable information. Then, we broaden the scope of the recommendations to the theoretical level, in order to define bases for a legal reasoning that, through the use of principles, works as a guideline capable of directing interpreters in abstract cases of data sharing. Finally, we conclude with an overview of the ideas presented in the article.

[1] Doutorando em Direito Público pela Universidade do Estado do Rio de Janeiro (UERJ). Mestre em Direito da Cidade pela Universidade Estadual do Rio de Janeiro (UERJ). Coordenador da disciplina de Direito Digital do Instituto New Law. Advogado.

KEYWORDS: LGPD. Privacy. Data Protection. Information Security. Contractual agreements.

Introdução.

O objetivo deste ensaio é contribuir com recomendações[2] abstratas que auxiliem na preparação de cláusulas contratuais de proteção de dados para utilização em contratos de serviços que envolvam o processamento de dados pessoais por um operador, em nome e sob as instruções de um controlador. Seguindo esta lógica, as recomendações são elaboradas da perspectiva do controlador.

Em primeiro plano, apresentamos os tópicos do primeiro guia publicado pela Autoridade Nacional de Proteção de Dados (ANPD) a respeito dos agentes de tratamento, notadamente controlador e operador, e do encarregado. Na sequência, resumimos o sistema de responsabilidades traçado pela Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) para os agentes de tratamento. Em seguida, fazemos recomendações de cunho prático, visando contribuir com a construção de instrumentos contratuais que versem sobre o compartilhamento de dados pessoais. Ao fim, ampliamos o escopo das recomendações, condensando as propostas em um "guia de princípios", cujo objetivo é sintetizar as etapas de um raciocínio jurídico a ser seguido para casos de compartilhamento de dados pessoais.

[2] As ideias apresentadas neste artigo são elaboradas com base nas seguintes premissas: (i) o fornecedor de serviços e a organização controladora de dados são entidades corporativas brasileiras e o contrato é regido pela lei brasileira; (ii) o negócio principal não envolve o compartilhamento transfronteiriço de informações pessoais. Se a transação envolver o compartilhamento transfronteiriço de informações pessoais, as leis das jurisdições estrangeiras relevantes deverão ser revisadas quanto à conformidade.

Do ponto de vista metodológico, foi realizado levantamento de publicações nacionais e internacionais, que permitiram análise e reflexão crítica das questões teóricas envolvidas. Substancial parte do trabalho foi desenvolvida com pesquisa na internet, bem como uso de material próprio, a partir da atuação profissional com a temática.

Objetiva-se com essas cláusulas, em síntese, minimizar as responsabilizações de um controlador e mitigar os riscos associados à violação de segurança ou ao uso não autorizado das informações pessoais.

1. Os primeiros passos de uma longa jornada: o primeiro Guia da Autoridade Nacional de Proteção de Dados (ANPD) sobre agentes de tratamento e encarregado.

Em 28 de maio de 2021, a Autoridade Nacional de Proteção de Dados (ANPD)[3] publicou seu primeiro Guia, intitulado "*Guia Orientativo para Definições dos Agentes* de *Tratamento de Dados Pessoais* e *do Encarregado"* (doravante aqui referido simplesmente como Guia),[4] contendo diretrizes não vinculativas sobre como identificar agentes de tratamento e os requisitos gerais do encarregado. O Guia surgiu em um momento adequado, pois entidades públicas e privadas têm experimentado alguma confusão quanto à definição e identificação adequada dos agentes de processamento.[5] O documento também tratava de questões ausentes na LGPD, como o conceito de controladores conjuntos.

O Guia é o primeiro do gênero publicado pela autoridade brasileira e está estruturado em sete capítulos. No entanto, optou-se por dividir este item em oito tópicos

[3] A ANPD é um órgão administrativo que foi criado para fazer valer a LGPD e tem autonomia técnica, apesar de estar ligado ao gabinete da presidência. A ANPD não é apenas responsável pela aplicação da LGPD, mas também pela fiscalização e emissão de diretrizes para quaisquer leis de proteção de dados. A ANPD possui poderes específicos para emitir diretrizes para o cumprimento dos requisitos impostos pela LGPD e aplicar sanções administrativas. Como a ANPD está em funcionamento, passa a ter ações de fiscalização e começou a promulgar regulamentos.

[4] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 29 nov. 2021.

[5] Acerca da atuação da ANPD frente ao poder público: "A simetria da incidência da LGPD sobre setores público e privado depende também da existência de um sistema de fiscalização e imposição de sanções sobre órgãos e entidades públicos e sobre agentes públicos que violarem a norma jurídica. Há que se reconhecer, porém, que o Poder Público já se encontra submetido a mecanismos próprios de controle interno e externo, e que também os agentes públicos possuem regramentos específicos para disciplinar sua atuação. (...) Importa notar que a sanção de multa prevista na LGPD claramente não é aplicável ao Poder Público, mas que multas previstas em outras normas aplicáveis ao Estado poderão incidir sobre órgãos e entidades do setor público, no contexto de ações de controle e fiscalização". – Cf.: WIMMER, Miriam. O regime jurídico de tratamento de dados pessoais pelo poder público. In: DONEDA, Danilo *et al. Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021, p. 271-288.

relevantes, que são: (i) agentes de tratamento, (ii) controlador, (iii) controladoria conjunta, (iv) controladoria singular, (v) operador, (vi) operadores subcontratados, (vii) *encarregado*: o DPO brasileiro, e (viii) comentários adicionais.

1.1. Agentes de tratamento.

Como mencionado acima, a identificação adequada dos agentes de tratamento em uma atividade de processamento de dados vinha gerando confusão entre as organizações brasileiras, especialmente as entidades públicas. A principal questão em jogo se refere ao status dos subordinados que lidam diretamente com dados pessoais, como funcionários ou servidores públicos, e se eles se encaixariam no conceito legal de controlador e/ou operador. O Guia esclarece que um indivíduo subordinado não se qualifica como agente de tratamento de dados, pois atua apenas sob o poder diretivo do agente de tratamento. Para orientar sobre essas consultas, no início do documento, a ANPD afirma que não devem ser considerados controladores (autônomos ou conjuntos) ou operadores os indivíduos subordinados, como empregados, servidores públicos ou equipes de trabalho de uma organização, que atuem sob o poder diretivo de um agente de tratamento de dados.

A LGPD estabelece que um agente de tratamento é um controlador ou operador de dados pessoais. Assim, o Guia elucida que a qualificação de um agente como um ou outro deve ser baseada na finalidade do processamento específico em análise. Portanto, a definição de controlador e processador é relativa, e uma organização pode assumir tanto as funções de um controlador quanto/ou um operador, dependendo do tratamento específico.

1.2. Controlador.

A LGPD define o controlador como pessoa física ou jurídica, seja pública ou privada, que tem o poder de tomar decisões sobre o tratamento de dados pessoais. O Guia complementa essa definição legal ao esclarecer que o controlador é o agente que define a finalidade e toma as principais decisões relativas ao processamento de dados pessoais, o que a ANPD considera como “elementos essenciais” de uma operação de tratamento.

Embora o Guia reconheça que o papel de um controlador possa ser indicado em um instrumento contratual, o documento enfatiza que o contexto e as circunstâncias relevantes do caso devem ser sempre considerados em uma análise final. Em outras palavras, seguindo o entendimento já adotado pelas autoridades europeias de proteção de dados, a identificação de

um agente como controlador deve decorrer do conceito estabelecido pela Lei, e seguir os parâmetros auxiliares indicados nas diretrizes relevantes dos reguladores, sempre considerando o contexto técnico e as circunstâncias pertinentes do caso.

1.3. Controladoria conjunta.

O conceito de controladoria conjunta não foi originalmente abordado pela LGPD, mas agora foi esclarecido no recente Guia. Refere-se às situações em que dois ou mais controladores decidem os propósitos da operação de tratamento em conjunto.

Embora a definição de uma controladoria conjunta não seja expressamente determinada na Lei, o regulador entende que tal conceito pode ser extraído da própria definição do controlador. Para abordar o tema, a ANPD recorreu ao artigo 26 do General Data Protection Regulation (GDPR) e à orientação do Conselho Europeu de Proteção de Dados (EDPB), contida nas *"Diretrizes 07/2020 sobre os conceitos de controlador e processador no GDPR"* publicadas em setembro de 2020.[5] Adaptando as normas europeias ao cenário da LGPD, a Autoridade definiu o conceito de controladoria conjunta como "a determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD".

Em resumo, a ANPD afirma que uma "Controladoria Conjunta" pode ocorrer quando: (1) mais de um controlador tem poder de decisão sobre o processamento de dados pessoais; (2) há um interesse mútuo de dois ou mais controladores, com base em seus próprios propósitos, na mesma operação de tratamento; (3) dois ou mais controladores tomam decisões comuns sobre os propósitos e elementos essenciais da operação de tratamento.

1.4. Controladoria singular.

Em oposição à controladoria conjunta, o Guia esclarece ainda que haverá uma controladoria singular quando os propósitos do tratamento de dados não forem comuns, convergentes ou complementares. Como exemplo, a ANPD ilustra que vários controladores podem, e muitas vezes o fazem, lidar com dados governamentais abertos, cada um para seus

[5] Cf.: EUROPEAN DATA PROTECTION BOARD (EDPB). *Draft guidelines on the concepts of controller and processor (Guidelines 07/2020).* Disponível em https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_pt. Acesso em: 29 nov. 2021.

próprios propósitos específicos. Se esses propósitos não forem comuns, convergentes ou complementares, todos os agentes de tratamento de dados serão considerados controladores singulares e uma controladoria conjunta não será estabelecida.

1.5. Operador.

De acordo com a LGPD, um operador é a pessoa física ou jurídica, seja pública ou privada, que processa dados pessoais em nome do controlador. O Guia também complementa a definição afirmando que, além de atuar em nome de um controlador e sob suas instruções: o operador é o agente que atua até o limite dos propósitos determinados pelo controlador. Embora a legislação brasileira de proteção de dados não determine expressamente que o controlador e o operador devam firmar um contrato para prosseguir com o processamento de dados, a ANPD indica que o estabelecimento de um acordo entre o controlador e o operador é visto como uma "boa prática". No entanto, o regulador não foi tão minucioso ao abordar os tópicos que deveriam ser incluídos em um contrato que verse sobre proteção dedados, apenas destacando a necessidade de indicar (i) o objeto, (ii) a duração, (iii) a natureza, (iv) a finalidade do processamento dos dados, (v) os tipos de dados pessoais envolvidos, (vi) os direitos, obrigações e responsabilidades das partes visando o cumprimento da LGPD. Além disso, o Guia afirma que é obrigação do processador informar o controlador ao usar subprocessadores – e, na medida do possível, obter sua autorização.

1.6. Operadores subcontratados.

O operador subcontratado, que também poderia ser definido como "suboperador" ou “subprocessador”, é o contratado pelo operador para auxiliá-lo no processamento de dados pessoais em nome do controlador. Embora a figura também não esteja diretamente prevista na LGPD, o regulador considera que o subprocessador pode ser considerado como um operador contratado por outro operador. Dito isso, importa saber que o suboperador é aquele “contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador”.

1.7. Encarregado: o DPO brasileiro.

De acordo com a LGPD, os controladores devem nomear um encarregado para atuar como ponto de contato entre o controlador, os titulares de dados e a ANPD. O encarregado deve receber reclamações e comunicações de titulares de dados; fornecer informações e adotar novas medidas relativas à proteção de dados dentro da entidade; receber comunicações de outros encarregados e tomar medidas para garantir o cumprimento da Lei; aconselhar funcionários e contratados sobre obrigações relativas a dados pessoais; e desempenhar outras funções determinadas pelo controlador ou estabelecidas em regras complementares.

O Guia esclarece que o "encarregado" (pessoa responsável) pode ser tanto um funcionário da instituição ou um agente externo, de natureza física ou jurídica. Quanto ao alcance da exigência de nomeação de pessoa ou entidade específica "responsável" em relação ao escopo do processamento e ao tamanho/capacidade do controlador, a ANPD indicou que, como regra geral, toda organização deve atribuir uma pessoa como encarregado até que as possibilidades de dispensa sejam regulamentadas.

Também é importante mencionar uma questão de natureza altamente sensível: a definição usada pela ANPD para conceituar a figura do encarregado. O documento define o encarregado como "o indivíduo responsável por garantir a conformidade de uma organização, pública ou privada, à LGPD". Essa é provavelmente a principal controvérsia estabelecida pelo Guia, uma vez que, na linguagem original da Lei, o encarregado não é necessariamente o responsável pela garantia do cumprimento; a LGPD diz apenas que o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares de dados e a ANPD.

1.8. Comentários adicionais.

É essencial elogiar a forma como a ANPD está contribuindo para o desenvolvimento do ecossistema de proteção de dados no Brasil. A Autoridade tem sido ágil, responsiva e atenta às principais demandas das empresas e do setor público.

Embora existam uma enorme carga de trabalho, prazos curtos e recursos escassos, as primeiras manifestações já foram suficientes para demonstrar a seriedade e qualidade do trabalho e do pessoal, além de um espírito democrático aguçado, estando o regulador especialmente aberto à participação e contribuições de especialistas e acadêmicos.

No entanto, para garantir um cenário mais claro e mais coeso em relação à proteção de dados no Brasil, ainda há espaço para contribuir com visões críticas e ideias construtivas, que não devem ser interpretadas como desaprovação. Nesse sentido, nos aventuramos a levantar

algumas questões e fornecer contribuições que possam ser relevantes para novas regulamentações e orientações da ANPD.

Primeiro, o Guia avançou consideravelmente em questões que estavam levantando discordâncias e incertezas entre as partes interessadas, mas pouco se preocupou com dúvidas de alto nível. Por exemplo, considerando a tendência de terceirização de serviços, muito comum em setores de tecnologia, como programadores, designers, serviços de segurança da informação, o que também pode ser caracterizado pelo processo conhecido no Brasil como "pejotização", quais elementos devem ser considerados pelas entidades locais envolvidas no que diz respeito à estipulação de cláusulas de proteção de dados para esses tipos de contratados? Sob o pretexto da lei, eles poderiam ser considerados operadores, mas, diariamente, parecem agir de forma muito semelhante aos empregados ou colaboradores dores internos.

Segundo, o regulador não comentou sobre como as "instruções sobre o processamento de dados" devem ser realizadas e documentadas, por exemplo, instruções de um controlador para um operador. Assim, resta uma questão importante: como devem ser realizadas as instruções do controlador para o processador e como os agentes de tratamento devem documentar esse processo?

Terceiro, a redação escolhida pela ANPD para definir o encarregado como "uma pessoa responsável pelo cumprimento da LGPD" foi infeliz. Como mencionado acima, esta é possivelmente a principal inconsistência do Guia, pois acreditamos que, no sistema LGPD, o encarregado não é necessariamente o indivíduo responsável por garantir o cumprimento, mas sim o responsável pela manutenção de uma articulação de comunicação entre o controlador, os titulares dos dados e a ANPD.

Por fim, vale ressaltar que a ANPD indica que está aberta a receber comentários e propostas para melhorar o Guia, as quais podem ser encaminhadas para o seguinte e-mail: normatizacao@anpd.gov.br.

2. O sistema de responsabilidades da LGPD para agentes de tratamento.

Pensemos numa hipótese em que uma organização controladora[6] de dados contrata um serviço e este serviço envolve o compartilhamento de dados pessoais com um operador.[7]

Considerando que o controlador pode enfrentar significativos danos financeiros e à reputação devido a um incidente de segurança ou ao uso não autorizado das informações compartilhadas, o controlador e o operador devem cumprir uma matriz de obrigações que rege a divulgação de dados pessoais de acordo com leis e regulamentos, princípios de leis gerais e específicas, além das diretrizes e padrões do setor. Em geral, essas regras exigem que os prestadores de serviços concordem contratualmente em tomar medidas razoáveis ou apropriadas para proteger os dados pessoais compartilhados.

Embora a lei de proteção de dados brasileira não delimite expressamente a obrigatoriedade de elaboração de um contrato entre as partes para tratar de questões de proteção de dados pessoais, no sistema desenhado pela LGPD, ao compartilhar dados pessoais com operadores, o controlador é, em regra, solidariamente responsável por qualquer dano causado pelo operador aos titulares dos dados pessoais. Além disso, como vimos, a ANPD já se manifestou no sentido de que é considerada uma boa prática dispor, pelo menos, sobre os elementos essenciais do tratamento. Neste aspecto, é importante conhecer a sistemática legal.

Nos artigos 42 ao 45, a LGPD aborda o regime de responsabilidade civil e ressarcimento de danos que podem ser aplicados aos agentes de tratamento quando alguma prática viole a Lei, resultando em um tratamento irregular de dados pessoais. Com efeito, é bom lembrar que o art. 39 da LGPD prevê que o operador deverá realizar o tratamento de dados segundo as instruções fornecidas pelo controlador. Como vimos anteriormente, a temática das "instruções" não foi abordada de forma expressa pelo primeiro Guia da ANPD, de forma que, por enquanto, nos resta conhecer a letra fria da Lei. [9]

O art. 42 estabelece que a reparação dos danos ocasionados pelo controlador ou operador, em razão do exercício de atividade de tratamento de dados pessoais irregular, viola a LGPD. A definição de "tratamento irregular" de dados está contida no art. 44 da norma, o qual prevê que um tratamento será irregular quando deixar de observar a legislação ou quando não

[6] A LGPD define como Controlador a "*pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais*" (art. 5º, VI).
[7] A LGPD define como Operador a "*pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador*" (art. 5º, VII).
[9] Cf.: Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. (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]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 29 nov. 2021).

fornecer a segurança que o titular de dados dele poderia esperar, considerando circunstâncias específicas.

Sendo assim, o controlador de dados poderá ser responsabilizado em caso de concessão de instruções ilícitas ao operador, ou em caso de prática direta de atos que venham a violar a legislação. O operador, por sua vez, poderá ser responsabilizado pelos seus atos, ou pela desobediência das ordens do controlador.

Vale destacar que todas as instruções realizadas pelo controlador, ou os atos diretamente praticados por este ou pelo operador, serão irregulares quando violarem a legislação de proteção de dados, ou quando deixarem de observar os modos seguros e técnicos pelos quais o tratamento de dados deve ser realizado, as técnicas de tratamento de dados disponíveis à época, além dos riscos e resultados que podem ser esperados. Além disso, o controlador ou operador também respondem pelos prejuízos decorrentes da violação da segurança que derem causa, resultando em danos ao titular dos dados, em razão de não terem adotado as medidas de segurança conforme disciplina o art. 46 da LGPD.

No artigo 42 da Lei, em seu parágrafo primeiro, são contempladas as hipóteses de responsabilidade solidária entre os agentes de tratamento de dados. Os operadores de dados pessoais poderão ser solidariamente responsabilizados entre si, nos casos em que haja mais de um operador e estes venham a descumprir a LGPD. Importante destacar que o direito de regresso entre os agentes é contemplado no §4º do art. 42, sendo este um ponto relevante também para as negociações contratuais.

A respeito das exceções à responsabilização dos agentes de tratamento, temos a primeira hipótese disposta no inciso I do art. 43, qual seja, quando o agente provar que não realizou o tratamento de dados (irregular) que lhe é atribuído. Já a segunda exceção está prevista no inciso II do mesmo artigo, sendo clara ao afirmar que, se não houver violação à legislação de proteção de dados, o tratamento questionado não será irregular, de maneira que não haverá dever de indenizar e sequer ilicitude do ato. O inciso III do art. 43, por sua vez, cuida da exceção de culpa exclusiva do titular de dados pessoais ou de terceiro envolvido. Esta hipótese faz surgir o questionamento de que, mesmo havendo a violação por meio da invasão de um sistema por este terceiro, os agentes de tratamento poderiam ser responsabilizados em razão da não adoção das medidas técnicas de segurança cibernética adequadas.

É bom lembrar que, embora a responsabilidade na LGPD seja, em regra, solidária (art. 42), há discussão sobre se o regime seria de responsabilidade subjetiva, objetiva, proativa ou de outra espécie. Aqueles que argumentam a favor da responsabilidade objetiva o fazem, em geral, com base em analogias ao Código de Defesa do Consumidor (CDC – Lei nº 8.078/1990).

Afirmam que a LGPD possui várias disposições que são inspiradas no CDC, a exemplo da possibilidade de o juiz inverter o ônus da prova (art. 42, § 2º, da LGPD). Soma-se a isso o argumento de que o próprio texto do art. 43 da LGPD se assemelharia à redação do art. 12, § 3º, do CDC, sendo este, por sua vez, muito parecido com a redação do art. 14, § 3º, do CDC. No extremo oposto, estão aqueles que defendem a responsabilidade subjetiva e a culpa como fundamento do regime estabelecido pela LGPD. Os argumentos também são consistentes e se baseiam, via de regra, no fato de a estrutura da LGPD estar pautada na criação de deveres. Dessa forma, não se justificaria – nem do ponto de vista lógico, nem do jurídico –, a criação de uma série de deveres de cuidado se não fosse para implantar um regime de responsabilidade subjetiva. Para este grupo, se o Legislador pretendeu responsabilizar os agentes independentemente da culpa, seria ocioso criar deveres a serem seguidos, tampouco responsabilizá-los quando tiverem cumprido perfeitamente todos esses deveres[10].

Tais questões ainda serão profundamente disputadas pela doutrina no plano teórico e definidas pelo Judiciário em casos práticos. Enquanto isso, para controladores, importa estar atento também às orientações da ANPD, que foram feitas com base em análises breves de casos abstratos como analisamos no tópico anterior. Vejamos alguns trechos de destaque do primeiro Guia publicado pela autoridade brasileira:

> 59. Muito embora o controlador tenha a principal responsabilidade e o operador deva atuar em nome dele, o art. 37 da LGPD determina que ambos partilham obrigações e, consequentemente, a responsabilidade de manter o registro das operações de tratamento. Além disso, nos termos do art. 42 da LGPD, ambos possuem a obrigação de reparação se causarem dano patrimonial, moral, individual ou coletivo a outrem, no âmbito de suas respectivas esferas de atuação.
>
> 60. No entanto, cabe ressaltar que, via de regra, as obrigações e responsabilidades do controlador e do operador são distintas, pois são determinadas de acordo com o papel exercido por cada um no âmbito do tratamento dos dados pessoais. Assim, a responsabilidade solidária estabelecida pelo inciso I, § 1o do art. 42 da LGPD, prevista para os casos de danos causados em razão do tratamento irregular realizado por operador (por descumprir as obrigações da legislação ou por não observar as instruções do controlador), pode ser considerada como uma excepcionalidade, já que em regra a responsabilidade é do controlador. A princípio, essa é a única hipótese em que o operador é equiparado ao controlador.[11]

Como vimos, a ANPD também se pronunciou sobre outras questões aguardadas, a exemplo dos requisitos e características que tornam uma controladoria conjunta ou singular, suas diferenças e elementos essenciais. Vimos que, em resumo, para que haja controladoria

[10] Cf.: TEPEDINO, Gustavo. TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. Capítulo XV: Responsabilidade Civil na Lei Geral de Proteção de Dados. In: _____. *Fundamentos do direito civil: responsabilidade civil – vol. 4.* Rio de Janeiro: Forense, 2020. p. 235-236.
[11] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo*...cit., p. 17.

conjunta, é necessário que três critérios sejam preenchidos ao mesmo tempo: (a) mais de um controlador possuir poder de decisão sobre o tratamento de dados pessoais; (b) haver interesse mútuo de dois ou mais controladores, com base em finalidade próprias, sobre um mesmo tratamento; e (c) dois ou mais controladores tomarem decisões comuns ou convergentes sobre as finalidade e elementos essenciais do tratamento. Vale a pena ter em mente as orientações expressas do regulador:

> 38. A depender do contexto, uma mesma operação de tratamento de dados pessoais pode envolver mais de um controlador. Conforme a LGPD, art. 42, §1º, II, quando mais de um controlador estiver diretamente envolvido no tratamento do qual decorram danos ao titular de dados, estes responderão de forma solidária, à exceção das hipóteses previstas no art. 43.
>
> 39. Assim, embora a LGPD não explicite o conceito de controladoria conjunta, é possível inferir que ele está contemplado no sistema jurídico de proteção de dados. A definição das funções dos controladores conjuntos implica consequências no que diz respeito às funções dos agentes de tratamento e aos direitos dos titulares. (...)
>
> 43. Entretanto, ainda que o mesmo conjunto de dados seja tratado, não haverá controladoria conjunta se os objetivos do tratamento forem distintos. Por exemplo, diversos controladores podem tratar dados abertos do governo, cada um para suas finalidades específicas. Se estas finalidades não forem comuns, convergentes ou complementares, ambos serão controladores singulares em relação ao tratamento de dados e a controladoria conjunta não estará estabelecida, o que afastaria a incidência do art. 42, §1o, II, da LGPD.
>
> 44. Assim como na controladoria singular, os controladores conjuntos são capazes de determinar os elementos essenciais do tratamento. Essa decisão é tomada de maneira coletiva, mas não há a necessidade de que cada controlador determine todos os elementos envolvidos em uma operação de tratamento para que a controladoria conjunta se estabeleça.
>
> 45. Cabe, contudo, frisar, que a identificação da controladoria conjunta será contextual e apenas o caso concreto permitirá identificar em que casos a controladoria conjunta foi estabelecida. Uma vez que se configure, a responsabilidade dos controladores será solidária, nos termos do art. 42, §1o, II, o que reforça a importância de que todos estejam em conformidade com a LGPD.
>
> 46. Assim, ao adaptar a concepção europeia para o cenário da LGPD, pode-se entender o conceito de controladoria conjunta como "a determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD."[8]

Importa saber, então, que os conceitos de controlador e operador são conceitos funcionais: eles visam alocar responsabilidades de acordo com as funções reais e atuais das partes. Isso implica que o status legal de um ator como um "controlador" ou "operador" deve, em princípio, ser determinado por suas atividades reais em uma situação específica, ao invés de ocorrer a partir da designação formal de um ator como sendo um "controlador" ou "operador",

[8]AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo...* cit., p. 12-13.

por exemplo, em um contrato. No contexto europeu e em termos gerais, a cocontroladoria existe para uma atividade de tratamento específica quando diferentes partes determinam em conjunto a finalidade e os meios dessa atividade. Portanto, a avaliação da existência de cocontroladoria requer o exame de se a determinação dos objetivos e dos meios que caracterizam o controlador é decidida por mais de uma parte. A avaliação deve ser feita a partir de uma análise factual, e não apenas formal, da real influência sobre os propósitos, finalidades e meios de processamento.[9]

Portanto, para os fins deste ensaio, importa saber que em muitas situações os agentes de tratamento podem ser controladores e/ou operadores, mas não é incomum que eles figurem como controladores independentes, cocontroladores ou cocontroladores independentes.[10] Descolando-se de uma análise literal da Lei, não é raro que, durante a prestação de um serviço, um agente possa até mesmo estar predominantemente como operador, ou seja, a análise sobre o papel do agente no tratamento incorre em uma zona nebulosa. E aí, o que fazer?

Diante de tais complexidades e do fato de que existem diversas obrigações do controlador – por exemplo, garantir que os titulares exerçam seus direitos, ou notificar a ANPD no caso de incidentes de segurança – que fazem emergir a necessidade de comunicação e assistência entre as partes contratantes (o que envolverá a definição de prazos e medidas de cooperação), é natural que a definição de regras e responsabilidades acerca do tratamento de dados pessoais esteja cada vez mais presente nos negócios. Essas questões serão abordadas nos próximos itens, contudo vale reforçar que, ainda que a autoridade brasileira pareça ter sido minimalista em relação ao que deve restar pactuado, há o entendimento de que um instrumento contratual é uma boa prática:

> 53. O conceito e o escopo de atuação do operador indicam, também, a importância das definições contratuais para a relação entre controlador e operador. Ainda que a LGPD não determine expressamente que o controlador e o operador devam firmar um contrato sobre o tratamento de dados, tal ajuste se mostra como uma boa prática de tratamento de dados, uma vez que as cláusulas contratuais impõem limites à atuação do operador, fixam parâmetros objetivos para a alocação de responsabilidades entre as partes e reduzem os riscos e as incertezas decorrentes da operação.

[9] É essencial avaliar a situação prática para a determinação dos papéis de Controlador e Operador e não apenas contar com a formalidade contratual para avaliação das responsabilidades. Nesse sentido: "*A avaliação para determinação do papel de Controlador deve ser realizada com base na situação fática, na realidade prática da atividade de tratamento em apreço, não com base em formalismos ou por mera discricionariedade dos agentes envolvidos. Assim, ainda que os agentes determinem, através de instrumento formal quais serão os papéis de cada um dos agentes, a realidade prática da atividade de tratamento prevalecerá e o que será analisado é a real atuação do agente de tratamento na situação fática, a fim de determinar se seu papel se enquadra na configuração de um Controlador*". – Cf.: STURARI, Matheus. *Contratos e Proteção de Dados Pessoais*. 2020. Disponível em: https://drive.google.com/drive/u/0/folders/12gKoxQ4ihvrjvLaRBrgbpYfC8vGJKt8Z. Acesso em: 29 nov. 2021.
[10] Cf.: EUROPEAN DATA PROTECCTION BOARD (EDPB). *Draft guidelines*… cit.

> 54. Os pontos que podem ser definidos contratualmente são o objeto, a duração, a natureza e a finalidade do tratamento dos dados, os tipos de dados pessoais envolvidos e os direitos e obrigações e responsabilidades relacionados ao cumprimento da LGPD.
>
> 55. Por fim, dentro do escopo de atuação do operador, importa dizer que ele pode definir elementos não essenciais do tratamento, como medidas técnicas.[11]

Como conclusão parcial, temos que, a partir da chegada da LGPD e do amadurecimento do ecossistema nacional de regulação da proteção de dados, a tendência é que cada vez mais os contratos tradicionais possuam uma seção específica, ou ao menos cláusulas gerais que regulem como se dará o tratamento de dados pessoais. Outra possibilidade é que tais contratos sejam acompanhados de anexos ou de declarações prevendo acordos sobre o tratamento de dados. Em muitas hipóteses, pode ser preferível utilizar anexos para restringir os pontos de (re)negociação.

3. Considerações práticas.

Em termos práticos, um controlador de dados deverá estabelecer proteções contratuais apropriadas com cada um de seus operadores para especificar o padrão de atendimento do prestador de serviços e suas obrigações com relação ao tratamento de dados pessoais. Pode ser recomendável ampliar os elementos trazidos pela ANPD de modo que o controlador formalize um instrumento contratual que o resguarde em relação a pelo menos os seguintes pontos:

1. Definição de quem é o controlador e quem é o operador;[16]

[11] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia Orientativo*... cit., p. 16.

[16] A cláusula relativa ao papel dos agentes de tratamento deve ser avaliada com base no caso específico. Não basta apenas reconhecer, em relação ao tratamento de dados pessoais em um contrato, que a contratante é o controlador de dados e que a contratada é um operador de dados. Há uma série de particularidades a respeito da definição e da negociação. Por exemplo, pode ocorrer de a parte contratante não possuir capacidade técnica e conhecimento sobre o serviço, de modo que não seja possível, de fato, realizar instruções adequadas a respeito do tratamento de dados, tampouco definir as categorias de dados a serem utilizadas. Por outro lado, podem ocorrer ocasiões em que o prestador de serviços não possui capacidade decisória relevante e executará o tratamento em estrito cumprimento às instruções da parte contratante. Ademais, uma organização pode possuir diversos contratos com um mesmo parceiro e, para cada contrato, assumir a posição de controlador ou de operador. Há hipóteses também, sobretudo para a realidade de empresas globais e/ou organizações com vultuoso número de contratos, em que definir o papel dos agentes de tratamento em cada contrato se torna tarefa inviável ou de extrema dificuldade, de modo que a organização poderia optar por utilizar modelos de cláusulas que não dispõem expressamente sobre o papel de cada parte como agente de tratamento, ou até mesmo indicando que atuam como controlador e operador.

2. Garantir que o operador esteja adequado às obrigações da LGPD (e de outras normas eventualmente aplicáveis), incluindo boas práticas, governança corporativa e medidas de segurança da informação;[12]
3. Obrigação expressa de manter registro do tratamento e de cumprir com normas e parâmetros de segurança da informação do controlador;[13]
4. Garantir que o controlador possa realizar auditorias para verificar se a declaração de adequação à LGPD e as políticas são verdadeiras, se aplicável para a natureza do serviço;[14]
5. Especificar claramente a finalidade do tratamento, sendo possível incluir vedação de tratamento pelo operador para qualquer outra finalidade de forma expressa;[15]

[12] Pode ser recomendável submeter expressamente a contratada ao cumprimento dos deveres e obrigações referentes à proteção de toda e qualquer informação relacionada a uma pessoa natural que possa de alguma forma identificá-la ou torná-la identificável (os dados pessoais) e obrigá-la contratualmente a tratar tais dados, se houver, de acordo com as legislações aplicáveis, incluindo, mas não se limitando à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – "LGPD"), à Lei nº 12.965, de 23 de abril de 2014 e ao Decreto nº 8.771, de 11 de maio de 2016 ("Marco Civil da Internet"), no que couberem e conforme aplicáveis. Neste aspecto, sugere-se que, caso ocorra modificação nos textos legais indicados, bem como expedição de recomendação/orientação de reguladores/fiscalizadores ou modificação de qualquer outro regulamento, de forma que se exija alterações no contrato ou na execução das atividades ligadas ao tratamento de dados pessoais realizado no âmbito do contrato, que as partes se adequem às condições supervenientes, hipótese em que poderiam, por exemplo, celebrar aditivo contratual formalizando as modificações acordadas.

[13] Sendo o dever de manter registro das operações de tratamento de dados uma obrigação legal, especialmente quando a atividade de tratamento está baseada no legítimo interesse (art. 37 da LGPD), pode ser recomendável dispor sobre a necessidade da prestadora de serviços manter registro das operações de tratamento de dados pessoais que realizar, bem como implementar medidas técnicas e organizacionais adequadas (incluindo as medidas estabelecidas nas políticas da contratante) para proteger os dados pessoais e informações contra destruição, acidental ou ilícita, perda, alteração, comunicação, difusão ou acesso não autorizado ou ilegal, além de garantir que o ambiente utilizado por ela para o tratamento seja estruturado de forma a atender os requisitos de segurança, os padrões de boas práticas de governança e os princípios gerais previstos nas legislações e demais normas aplicáveis. A depender do serviço e da natureza do compartilhamento, pode ser desejável dispor também sobre a atualização dos registros e seu conteúdo mínimo. Um sugestão é que cada documento de registro detenha, pelo menos: (i) a categoria dos dados tratados; (ii) os sujeitos envolvidos na atividade; (iii) a finalidade das atividades de tratamento realizadas; (iv) por quanto tempo os dados pessoais serão processados e armazenados após o cumprimento de sua finalidade originária; (v) a base legal utilizada, inclusive nos casos de legítimo interesse; (vi) a ocorrência de compartilhamento com quaisquer terceiros ou suboperadores; (vii) a transferência internacional de dados; (viii) a existência ou inclusão de dados pessoais sensíveis ; e (ix) formas e prazos de descarte físico e digital adotados.

[14] De acordo com a natureza do contrato e com os programas de conformidade da parte contratante, pode ser recomendável estabelecer o direito de monitorar, fiscalizar, solicitar evidências e/ou auditar as operações de tratamento, mediante a contratação de terceiro (ou não), em período previamente combinado entre as partes, a fim de verificar o cumprimento dos controles de segurança, decisões, finalidades e instruções determinadas pelo controlador, bem como as demais obrigações de privacidade e proteção de dados pessoais, e sem que isso implique em qualquer redução da responsabilidade desta perante a contratante, a legislação e/ou o contrato. Indo além, é possível pactuar acerca da necessidade de a contratada disponibilizar toda documentação necessária para demonstrar cumprimento às obrigações, resultando, por exemplo, na elaboração de um relatório de auditoria.

[15] Em relação ao tema da finalidade, é natural que o contratante instrua a prestadora de serviços, a partir do início da relação contratual, a processar dados pessoais de acordo com o contrato, sem prejuízo de fornecer instruções adicionais (preferencialmente por escrito) à contratada a respeito do tratamento de dados. Sugere-se que a parte contratada seja obrigada a observar prontamente, e dentro do prazo solicitado pela contratante, todas as instruções fornecidas na medida necessária para que a contratada (i) cumpra com suas obrigações de operador e (ii) auxilie a contratante a cumprir com as obrigações de Controlador. Na hipótese de a contratada entender que qualquer instrução contraria a legislação, importaria informar imediatamente para eventuais esclarecimentos. Por fim, pode ser recomendável dispor expressamente a respeito das consequências, caso a contratada utilize dados para

6. Definir termos de indenização e direito de regresso do controlador;[16]
7. Criar obrigação de o operador colaborar com o controlador para o cumprimento das obrigações deste, tais como: exercício dos direitos dos titulares, notificação e informação, no caso de ocorrência de incidentes ou violações de dados pessoais. Neste aspecto, estabelecer regras, prazos e um fluxo claro para comunicações de incidentes, confirmados ou suspeitos, ou de quaisquer outras demandas de titulares ou autoridades relacionadas ao tratamento objeto do contrato;[17]
8. Incluir regras sobre exclusão dos dados pessoais após a extinção do contrato;[18]
9. Regras de subcontratação pelo operador;[19]

---

finalidades alheias ao contrato e ao determinado pela contratante. Por exemplo, essas atividades de tratamento alheias poderiam ser consideradas fora de contexto, sendo a contratada a única responsável, assumindo para si todos os eventuais ônus decorrentes do tratamento em desconformidade.

[16] Sugere-se que o descumprimento pela contratada e/ou suas subcontratadas de qualquer legislação de proteção de dados pessoais aplicável ou das provisões contidas no contrato, a respeito dos dados, gere a obrigação de indenizar integralmente, de defender e manter integralmente isentos a contratante e as partes interessadas de e contra todas as responsabilidades, perdas e danos, lucros cessantes, prejuízos, custos, despesas, ações, processos, demandas, multas e penalidades, entre outros, independentemente de serem provenientes de demandas de titulares, medidas de órgão e/ou entidade(s) governamental(ais). Além disso, na hipótese de a contratante ou quaisquer partes relacionadas serem condenadas por responsabilidade solidária ou subsidiária, seja nas esferas administrativa ou judicial, em decorrência do descumprimento pela contratada das obrigações de proteção de dados avençadas, a contratada poderia vir a ser obrigada a reembolsar todos os valores estipulados em condenação, bem como as custas e despesas do processo, independentemente da propositura de ação judicial para o que seja devido ao referido reembolso.

[17] Este tema é de suma importância. A prestadora de serviços deve ser obrigada a notificar a contratante, no prazo máximo acordado pelas partes, por escrito, sobre: (i) quaisquer pedidos de titular em relação aos seus dados pessoais, incluindo, pedidos de acesso e/ou retificação, solicitações de exclusão, e outros pedidos semelhantes, sendo vedado à contratada a responder a tais pedidos, a menos que expressamente autorizado a fazê-lo pela contratante; (ii) qualquer reclamação relacionada ao tratamento, incluindo alegações de que a atividade viola direitos de titular; (iii) qualquer incidente e/ou violação; (iv) qualquer ordem, emitida por autoridade judicial ou administrativa (incluindo, mas não se limitando à ANPD), que tenha por objetivo obter quaisquer informações relativas ao tratamento; (v) qualquer citação/intimação em procedimento/processo, administrativo ou judicial, proposta por titular ou parte interessada no escopo do contrato, e que tenham as partes legitimidade e interesse para intervir ou figurar no polo passivo da mencionada demanda. Indo além, na hipótese de a contratada tomar conhecimento, de maneira inequívoca, de acesso não autorizado, divulgação indevida e/ou de situação acidental ou intencional de destruição, perda, alteração, comunicação que afete os dados pessoais tratados em decorrência do contrato, que envie comunicação à contratante por escrito, em até 24 (vinte e quatro) horas, observadas eventuais disposições legais aplicáveis. A comunicação referente a incidentes de segurança poderia incluir no mínimo as seguintes informações: (i) a descrição da natureza dos dados pessoais afetados; (ii) as informações sobre os titulares envolvidos; (iii) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; (iv) os riscos relacionados ao incidente; (v) os motivos da demora, no caso de a comunicação não ter sido imediata; e (vi) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. Por fim, a contratada poderia ser obrigada também a se abster de realizar qualquer comunicação à ANPD, às autoridades governamentais e aos titulares ou terceiros, sem a prévia e expressa concordância da contratante, que poderá controlar a redação final dessas comunicações e quem deverá realizá-las, observadas as disposições das legislações aplicáveis.

[18] Ao término do contrato, a prestadora de serviços pode ser obrigada, a critério da contratante e conforme seu pedido escrito, a excluir permanentemente ou a devolver integralmente os dados tratados no âmbito do contrato, salvo se o armazenamento for de outra forma licitamente pactuado entre as partes ou se aplicáveis obrigações legais e/ou regulatórias que demandem o armazenamento por tempo adicional.

[19] Em determinadas hipóteses, é comum que as organizações autorizem, por padrão, a contratação de terceiros necessários ao cumprimento do objeto do contrato. Nesse aspecto, caso a contratada subcontrate quaisquer terceiros para realizar uma ou mais operações de tratamento, ela poderia ser obrigada a assinar, antes de qualquer

10. Regras para transferência internacional,[20] se aplicável.
11. Obrigações de confidencialidade, inclusive para empregados, colaboradores e terceirizados que tratem dos dados. Pode haver, também, obrigação de treinar essas pessoas em relação à confidencialidade e proteção dos dados.[21]

Para o dia a dia, mas ainda em termos abstratos, o esboço do instrumento contratual poderá conter – dividido em tópicos, seções cláusulas, aditivos e/ou anexos - tendendo a fazer uma exposição clara sobre os seguintes aspectos:

1. Partes: agentes de tratamento envolvidos e seus papéis;
2. Considerandos;
3. Definições;
4. Âmbito de aplicabilidade;
5. Legislações aplicáveis;
6. Finalidade e escopo;
7. Definições sobre o tratamento de dados em nome do controlador (instruções);
8. Duração do tratamento (e/ou validade do contrato);

compartilhamento de dados, instrumento contratual por escrito com a referida subcontratada, que seria considerada como suboperadora, devendo o acordo conter as mesmas obrigações de proteção de dados previstas no contrato principal, sendo a contratada considerada como responsável solidária juntamente com a suboperadora. Se necessário, o controlador na posição de contratante poderia estipular, ainda, que os dados pessoais somente pudessem ser compartilhados, transferidos ou disponibilizados a terceiros mediante anuência prévia, expressa e por escrito do controlador, e desde que tal tratamento fosse necessário para a execução do contrato, e limitado, sempre, às finalidades estabelecidas para o cumprimento do contrato.

[20] A transferência internacional de dados pessoais é uma situação muito comum, por exemplo, em casos de compartilhamento de dados de colaboradores entre empresas do mesmo grupo econômico (dados que ficam armazenados na sede da matriz no exterior), há a contratação de servidores de nuvem que utilizam *data centers* localizados em outros países, a terceirização de SAC, dentre outras. De acordo com a LGPD, a transferência internacional de dados pessoais somente poderá ocorrer nas seguintes hipóteses: (i) transferência para países/organizações internacionais que assegurem grau de proteção adequado; (ii) comprovação, pelo controlador, de que certas garantias foram atendidas (cláusulas contratuais, normas corporativas globais, selos, certificados, etc.); (iii) transferências em casos de cooperação internacional entre órgãos públicos de inteligência, investigação ou persecução; (iv) quando necessária para a proteção da vida do titular; (v) autorizada pela ANPD; (vi) em caso de compromisso assumido em acordo internacional; (vii) quando necessária para a execução de política pública; (viii) quando o titular tiver fornecido o seu consentimento específico; ou (ix) quando necessário, para atender cumprimento de obrigação legal ou regulatória pelo controlador, para a execução de contrato ou de procedimentos preliminar relacionados a contrato do qual seja parte o titular, ou para o exercício regular de direitos em processo judicial, administrativo ou de arbitragem. Assim, caso o tratamento de dados pessoais realizado no contexto ou em decorrência do contrato envolver ou requerer a realização de uma transferência internacional, a prestadora de serviços poderia ser obrigada a concordar que esta transferência estivesse sujeita aos requisitos de segurança, privacidade e proteção de dados consistentes com os termos e condições da norma brasileira, do contrato e também das leis de proteção de dados pessoais aplicáveis à jurisdição para a qual os dados pessoais seriam transferidos.

[21] É recomendável determinar como informação confidencial e/ou sigilosa todo dado pessoal tratado no âmbito do contrato. Nesse sentido, seria possível obrigar o prestador de serviço a fornecer aos empregados e/ou colaboradores treinamentos periódicos e adequados sobre segurança da informação, privacidade e proteção de dados pessoais, garantindo também que a contratante possa, a qualquer momento, requerer a comprovação do cumprimento das premissas estabelecidas pela LGPD, como políticas, comprovante de demonstração de realização de treinamentos e a existência, por exemplo, de procedimento de gerenciamento de riscos e de resposta a incidentes, dentre outros que se façam necessários.

9. Obrigações do controlador;
10. Obrigações do operador;
11. Confidencialidade;
12. Direito dos titulares de dados, formas de cumprimento e comunicação entre as partes;
13. Medidas técnicas e organizacionais;
14. Notificações (endereços, formas e prazos);
15. Comunicação em casos de incidentes de segurança;
16. Assistência (custos e medidas a serem adotadas; *e.g. call center*);
17. Cooperação;
18. Subcontratação (subprocessadores/suboperadores);
19. Transferências internacionais;
20. Prestação de contas;
21. Direitos de auditoria;
22. Execução (*enforcement*);
23. Disposições gerais.

Nunca é demais lembrar que, ao redigir ou negociar cláusulas de proteção de dados pessoais, é importante entender o contexto. As sugestões neste artigo são apenas exemplificativas, pensadas para hipóteses abstratas e para fins elucidativos. Em particular, as cláusulas devem ser modificadas ou suplementadas conforme necessário para refletir:

(1) Os fatos e circunstâncias específicos da transação relevante: nem todas as recomendações podem ser relevantes ou apropriadas para uma transação específica. Por exemplo, as partes precisam levar em consideração: (i) a sensibilidade das informações pessoais em questão, como o volume e as características dos dados; (ii) os resultados da devida diligência do controlador quanto à capacidade do provedor de serviços de cumprir com os requisitos de segurança de dados do cliente; (iii) as políticas de segurança da informação das partes e outras políticas e procedimentos internos; (iv) entre outras questões relacionadas à natureza do negócio e do tipo de serviço contratado. O contexto é extremamente relevante ao avaliar o risco e a exposição.

(2) Quaisquer requisitos legais específicos aplicáveis: (i) às leis específicas (setoriais) - determinados setores (como os prestadores de serviços médicos, serviços financeiros e serviços para crianças) devem atender a requisitos especiais de conformidade estatutária e regulamentar (regulamentos específicos para o setor) - ; e (ii) as empresas sujeitas a essas leis devem revisar os requisitos de privacidade e segurança dessas normas para garantir que os contratos de prestadores de serviços estejam em total conformidade e que cumpram com quaisquer obrigações adicionais relacionadas à divulgação de dados pessoais a terceiros.

4. Bases de um raciocínio jurídico.

São muitas as situações em que a organização, enquanto controladora, deverá se preocupar com o compartilhamento de dados. Por isso, é produtivo construir orientações gerais que funcionem como um guia para hipóteses abstratas em que a contratação de determinado serviço, ou a realização de um negócio jurídico, envolva o compartilhamento de dados pessoais. Inspirando-se na *"The Black Letter of The Ali Principles of Law, Data Protection"*,[22] na qual Daniel Solove e Paul Schwartz fornecem uma visão geral dos princípios aplicáveis à privacidade e à proteção de dados pessoais entre diferentes sistemas legais, buscamos concatenar uma lógica em que os princípios funcionem como um guia para o raciocínio jurídico.[23]

Sem atribuir opiniões aos autores, é possível adaptar o raciocínio utilizado em volta dos princípios e construir recomendações genéricas e abrangentes para o caso de transferências de dados. A avaliação seria feita com base no seguinte raciocínio:

(a) **Limites para transferências posteriores**. Um controlador de dados ou operador de dados que possui dados pessoais, pode transferir posteriormente essas informações para um operador de dados para atividades de dados pessoais apenas se:

(1) o titular dos dados recebeu um aviso das atividades;

(2) a transferência é exigida por lei; ou

(3) a transferência é para usos secundários limitados (exceções à limitação de uso) e os requisitos de transparência e aviso são atendidos.

(b) **Exceções ao requisito de consentimento**.[24] As atividades de dados pessoais podem ser conduzidas sem consentimento se:

---

[22] SOLOVOVE, Daniel J.; SCHWARTZ, Paul M. ALI data privacy overview and black letter text. *UCLA Law Review*, v. 68, 2020. Disponível em: https://ssrn.com/abstract=3457563. Acesso em: Acesso em: 29 nov. 2021.

[23] Os autores têm como objetivo fornecer um plano para que os formuladores de políticas regulem a privacidade de forma abrangente e eficaz. Os princípios escolhidos pelos autores não são uma tentativa de redigir uma "lei global ideal", como se ela estivesse sendo escrita em uma folha em branco. Também não representam uma tentativa de reformular leis existentes. Em vez disso, com base nas regras existentes em diversos sistemas, Solove e Schwartz buscam uma saída intermediária. Tentam demonstrar, de modo geral, como as legislações podem manter seus compromissos essenciais (construídos sobre as bases jurídicas internas), ao mesmo tempo em que aterrissam em um lugar próximo ao GDPR – norma que atualmente é a mais importante referência global na proteção de dados. Em termos práticos, os princípios também podem ajudar advogados envolvidos em operações de transferência de dados.

[24] Importante frisar que o raciocínio proposto não leva exclusivamente em consideração a LGPD e, portanto, não retratou especificamente as bases legais para o tratamento de dados no Brasil. O objetivo é justamente que o

(1) a atividade de dados pessoais é exigida por lei;

(2) obter consentimento seria inadmissível por lei; ou

(3) obter o consentimento seria impraticável, muito caro ou difícil, e o uso satisfaz um ou mais dos seguintes critérios:

(A) a atividade de dados pessoais é necessária na execução de um contrato no qual o titular dos dados é parte;

(B) a atividade de dados pessoais avança significativamente a proteção da saúde ou segurança do titular dos dados ou de outras pessoas;

(C) a atividade de dados pessoais avança significativamente na proteção contra atividades criminosas ou tortuosas por um titular de dados;

(D) a atividade de dados pessoais promove significativamente o interesse público e não representaria um risco significativo de dano material suficiente para desencadear um aumento de notificação (transparência); ou

(E) a atividade de dados pessoais serve a um interesse legítimo significativo e não representa um risco significativo de danos materiais ao titular dos dados ou a outros, nem é significativamente inesperada.

(c) **Revisão da devida diligência dos destinatários dos dados pessoais**. Antes de fazer uma transferência subsequente, um controlador ou operador de dados deve exercer a devida diligência para garantir que o destinatário proteja os dados pessoais.

(d) **Contratos com operadores de dados**. Antes de efetuar uma transferência para um operador de dados, um controlador ou operador de dados deve firmar um contrato vinculativo com o destinatário dos dados pessoais. O contrato deve incluir recursos a serem invocados em caso de descumprimento de seus termos, como rescisão do contrato e exigências, no sentido de que o destinatário de dados pessoais:

(1) proteja os dados pessoais de acordo com os princípios;

(2) proteja os dados pessoais de acordo com a declaração de transparência e aviso individual;

(3) realize apenas as atividades de dados pessoais necessárias para cumprir o contrato ou que sejam expressamente autorizadas pelo controlador ou processador de dados que transferiu os dados; e

(4) execute as seguintes etapas ao transferir dados para outro destinatário:

(A) exerça a devida diligência;

(B) transfira dados apenas para um destinatário que fornecerá a proteção adequada;

raciocínio seja adequado para situações abstratas, as quais potencialmente envolvem outras legislações que versem sobre proteção de dados pessoais.

(C) celebre contratos que incluam as mesmas ou maiores proteções que em seu contrato com o controlador de dados e que exija que o outro destinatário cumpra com as mesmas obrigações de um operador de dados dispostas neste guia;

(D) exija que qualquer destinatário de dados subsequente faça o mesmo se transferir os dados pessoais para outros destinatários em diante;

(5) notifique o controlador de dados sobre qualquer transferência subsequente, antes que ela seja feita, permitindo que o controlador de dados aprove ou rejeite a transferência;

(6) retorne ou destrua os dados a pedido do controlador de dados, quando o destinatário não tiver mais a necessidade legal ou contratual de retê-los;

(7) treine seus funcionários que têm acesso aos dados pessoais sobre suas obrigações sob os princípios e seus requisitos nas declarações de transparência e aviso individual do controlador ou processador de dados;

(8) dedique recursos adequados, incluindo pessoal suficiente, à proteção dos dados pessoais;

(9) facilite a conformidade do controlador de dados com os princípios, cooperando com as atividades de supervisão do controlador de dados - os meios de cooperação devem incluir o fornecimento de informações ao destinatário necessárias para a conformidade e a assistência ao controlador de dados ao responder o exercício de direitos de um titular de dados de acordo com os princípios. Quando necessária para a conformidade do controlador de dados com os princípios, a cooperação será estendida, mesmo após o término ou rescisão do contrato;

(10) desenvolva e mantenha um programa abrangente e razoável de privacidade;

(11) disponibilize as informações necessárias para que o controlador ou operador de dados avalie a conformidade do destinatário (de forma razoável);

(12) notifique o controlador de dados imediatamente após a descoberta de uma violação de dados pessoais ou qualquer descumprimento do contrato, ou dos princípios, e coopere totalmente com os esforços do controlador de dados para resolver o problema.

(e) **Supervisão razoável**. Um controlador de dados ou operador de dados que transfere dados pessoais deve se comprometer com uma supervisão razoável do destinatário. Se considerar que o destinatário dos dados pessoais é deficiente no desempenho de qualquer uma de suas obrigações contratuais relacionadas, o controlador ou operador de dados deve invocar as medidas apropriadas no contrato para resolver prontamente a deficiência, além de exigir garantias razoáveis do destinatário de dados pessoais para que a deficiência não se repita no futuro.

(f) **Transferências posteriores**. Um destinatário de dados que transfira dados pessoais em diante para um outro destinatário de dados, deve seguir os requisitos de compartilhamento

apresentados. A menos que proibido por lei, todos os destinatários de dados pessoais são cobertos pelos princípios mencionados.

5. Considerações finais.

Neste artigo, buscou-se analisar, sob as perspectivas teórica e prática, os agentes de tratamento e o compartilhamento de dados pessoais entre eles. Para tal, abordamos, primeiro, um guia com orientações não vinculantes publicado pela Autoridade Nacional de Proteção de Dados, em oito tópicos, quais sejam: agentes de tratamento, controlador, controladoria conjunta, controladoria singular, operador, operadores subcontratados, encarregado, o DPO brasileiro, e comentários adicionais. Aproveitamos a oportunidade para comentar o documento de forma prospectiva, destacando trechos relevantes do material produzido pelo regulador. Notou-se a opção da ANPD de focar nos temas que vêm sendo alvo de maiores dúvidas no ecossistema brasileiro, a exemplo da definição de subordinados como agentes de tratamento. Se, por um lado, a ANPD foi assertiva em relação a esses aspectos, por outro, economizou em assuntos de maior complexidade, como o que deveria constar em instrumentos contratuais que regem o compartilhamento de dados entre os agentes de tratamento.

Diante desse cenário de incertezas, buscamos realizar recomendações práticas e teóricas para aqueles que precisam negociar cláusulas contratuais entre uma entidade controladora de dados e um operador. Sob a perspectiva do controlador, trouxemos os pontos que merecem especial atenção, destacando nove pontos de maior relevância no quinto tópico do artigo. Ainda no plano prático, apontamos também outros tópicos usualmente abarcados nos instrumentos contratuais que versem especificamente sobre o compartilhamento de informações pessoais.

Por fim, ampliamos o escopo das recomendações para construir, no plano teórico, um guia por meio do qual seja possível seguir um raciocínio jurídico para realizar validações técnicas ao proceder a um compartilhamento de dados. Este guia buscou fornecer, em cinco tópicos, as bases para um raciocínio jurídico que possa ser validado nas hipóteses de transferência. São eles: os limites para transferências posteriores, a revisão da devida diligência dos destinatários dos dados pessoais, os contratos com operadores de dados, a supervisão razoável e as transferências posteriores. Seguindo uma lógica principiológica, ao realizar conferências sobre esses tópicos, o intérprete será capaz de validar se em uma hipótese de compartilhamento de dados são adotadas práticas razoáveis.

Importa frisar que, considerando que o regulador brasileiro tende a abordar a temática dos contratos em matéria de proteção de dados de forma específica, as recomendações neste ensaio não são "à prova do tempo", devido à possibilidade de superveniência de orientações regulatórias. Por fim, cumpre enfatizar que as informações e opiniões apresentadas neste artigo não refletem necessariamente a opinião oficial de autoridades de proteção de dados, do Brasil ou estrangeiras. Nem reflete a opinião das instituições e órgãos do Brasil ou dos autores citados. As informações são apenas para fins acadêmicos e educacionais e não constituem aconselhamento jurídico. Recomenda-se que, ao negociar contratos em matérias de proteção de dados, se busque aconselhamento profissional específico antes de agir de acordo com qualquer uma das informações fornecidas.

Referências.

ARAUJO, Bernardo José Oliveira; BECKER, Daniel. Comentários ao capítulo VIII. In: FEIGELSON, Bruno; BECKER, Daniel; CAMARINHA, Sylvia (Coord.). *Comentários à lei geral de proteção de dados: lei 13.709/2018*. São Paulo: Thomson Reuters Brasil, 2020.

ARAUJO, Bernardo José Oliveira; BECKER, Daniel. Comentários ao capítulo IX. In: FEIGELSON, Bruno; BECKER, Daniel; CAMARINHA, Sylvia (Coord.). *Comentários à lei geral de proteção de dados: lei 13.709/2018*.São Paulo: Thomson Reuters Brasil, 2020.

ARAUJO, Bernardo José Oliveira. *LGPD* Flash: agilidade em privacidade e proteção de dados. In: BECKER, Daniel; FERRARI, Isabela (Coord.). *Regulação 4.0: vol. II: desafios da regulação diante de um novo paradigma científico*. São Paulo: Thomson Reuters Brasil, 2020, p. 323-358.

ARAUJO, Bernardo José Oliveira; FERRARI, Isabela. Relatório de impacto à proteção de dados pessoais: Parte I: contexto, abrangência e escalabilidade. In: VAUGHN, Gustavo Favero; BERGSTRÖM, Gustavo Tank; FABER, Bárbara Breda (Org.). *Primeiras Impressões sobre a Lei Geral de Proteção de Dados - LGPD*. 1 ed. Ribeirão Preto: Migalhas, 2021. p.335-363.

ARAUJO, Bernardo José Oliveira; FERRARI, Isabela. Relatório de impacto à proteção de dados pessoais. Parte II: documentação e etapas de seu desenvolvimento. In: VAUGHN, Gustavo Favero; BERGSTRÖM, Gustavo Tank; FABER, Bárbara Breda (Org.). *Primeiras Impressões sobre a Lei Geral de Proteção de Dados - LGPD*. 1 ed. Ribeirão Preto: Migalhas, 2021. p. 365-396.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 29 nov. 2021.

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

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a lei geral de proteção de dados pessoais e o código de defesa do consumidor. *civilistica.com*, v. 9, n. 3, p. 1-23, 2020.

BODIN DE MORAES, Maria Celina. QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. In: THEMOTEO, Reinaldo José (Coord.). Proteção de dados pessoais: privacidade versus avanço tecnológico. *Cadernos Adenauer xx*, n. 3, Rio de Janeiro: Fundação Konrad Adenauer, 2019. p. 113-135.

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]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 29 nov. 2021.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados*. 2 ed. São Paulo: Thomson Reuters Brasil, 2019.

EUROPEAN DATA PROTECTION BOARD (EDPB). *Draft guidelines on the concepts of controller and processor (Guidelines 07/2020)*. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_pt. Acesso em: 29 nov. 2021

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

SOLOVOVE, Daniel J.; SCHWARTZ, Paul M. ALI data privacy overview and black letter text. *UCLA Law Review*, v. 68, 2020. Disponível em: https://ssrn.com/abstract=3457563 . Acesso: 29 nov. 2021.

STURARI, Matheus. *Contratos e Proteção de Dados Pessoais*. 2020. Disponível em: https://drive.google.com/drive/u/0/folders/12gKoxQ4ihvrjvLaRBrgbpYfC8vGJKt8Z.Acesso em: 29 nov. 2021.

TEPEDINO, Gustavo. TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. Capítulo XV: Responsabilidade Civil na Lei Geral de Proteção de Dados. In: _____. *Fundamentos do direito civil: responsabilidade civil*. v. 4. Rio de Janeiro: Forense, 2020.

WIMMER, Miriam. O regime jurídico de tratamento de dados pessoais pelo poder público. In: DONEDA, Danilo *et al*. *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021, p. 271-288.

Recebido em: 30/11/2021
1º Parecer em: 01/12/2021
2º Parecer em: 05/12/2021