Controlador ou operador: quem sou eu?

Cartilha sobre agentes de tratamento de dados pessoais

LAPIN

Controlador ou Operador: quem sou eu?

Cartilha sobre agentes de tratamento de dados pessoais

Autores
Alexandra Krastins
Clarisse Andreoly Monte Serrat
Sarah Fernandes
Thiago Guimarães Moraes

Coordenação editorial
Pedro Peres

Revisão
Isabela de Araújo

Diagramação
Alexandra Melo

Ilustrações
Freepik Storyset

Data de publicação
Abril de 2021

LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

lapin.org.br
@ lapin.br
/lapinbr
/lapinbr

Quem somos nós?

O Laboratório de Políticas Públicas e Internet (LAPIN) é um think tank de composição multidisciplinar com sede na capital federal brasileira. Nosso objetivo é apoiar o desenvolvimento de políticas públicas voltadas para a regulação das tecnologias digitais por meio da pesquisa e da conscientização da sociedade.

Índice

Introdução

Com a entrada da Lei Geral de Proteção de Dados (LGPD) em vigor, as organizações se veem diante da tarefa de preparar e implementar seu plano de adequação para o cumprimento das diretrizes da lei, respeitando os direitos dos titulares de dados pessoais e evitando sanções administrativas e judiciais.

Além de ter que desenvolver uma "cultura da privacidade" em sua organização, os gestores devem ser capazes de interpretar a lei da forma correta, o que pode ser um desafio. Deste modo, com o intuito de auxiliar gestores de organizações públicas e privadas a darem seus passos iniciais na conformidade à LGPD, o Laboratório de Políticas Públicas e Internet (LAPIN) lança a cartilha **Controlador ou Operador: quem sou eu?**.

Neste documento introduzimos um dos pontos mais importantes para entender as obrigações que deverão ser cumpridas pelas organizações: a diferença entre o controlador e o operador de dados, figuras centrais nas operações de tratamento de dados.

É a partir desses agentes de tratamento que se determina quem será responsável pela conformidade com a LGPD.

Depois de apresentar os agentes de tratamento, exemplos serão trazidos para ajudar a identificar qual é o papel de cada um deles em situações práticas. Por fim, listamos as principais obrigações e responsabilidades dos controladores e operadores.

A análise dos conceitos também envolve reflexões com o direito comparado, em particular com o sistema europeu de proteção de dados, substanciado na *General Data Protection Regulation* (GDPR), tendo em vista a inspiração para o direito brasileiro no que se refere à privacidade e à proteção de dados pessoais.

Esperamos que com este material as organizações possam se sentir mais confiantes em identificar o papel que assumem diante da LGPD, com o cumprimento adequado de suas obrigações e respeito aos direitos dos titulares de dados.

I. Agentes de tratamento

A LGPD define como agentes de tratamento **controlador** e o **operador**, os quais possuem diversas responsabilidades com relação às operações de tratamento de dados pessoais.

Art. 5º, IX - LGPD

Ressalta-se que, na prática, os agentes de tratamento são considerados sob o ponto de vista institucional, ou seja, a instituição é o agente de tratamento (controlador ou operador) e não uma área, equipe ou funcionário da referida instituição.

Assim, não devem ser considerados controladores ou operadores das operações de tratamento de dados o Encarregado de Proteção de Dados Pessoais[1], também chamado de *Data Protection Officer* (DPO), o presidente - ou *Chief Executive Officer* (CEO) - de uma empresa, ou o chefe de uma repartição pública. Como esses indivíduos são representantes institucionais, compreende-se que a LGPD traz a própria instituição (pessoa jurídica) como agente de tratamento[2].

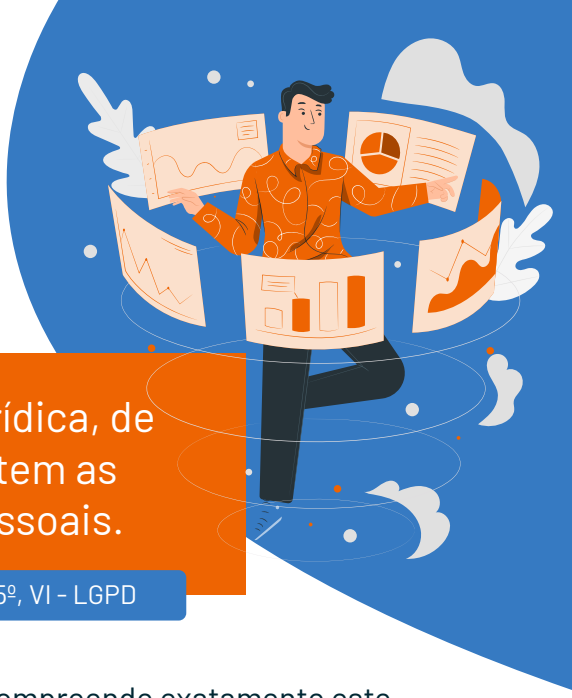
Suponhamos, por exemplo, que uma empresa colete o e-mail de um cliente para encaminhar o exemplar de um livro eletrônico. Como a empresa é a responsável por decidir o que será feito com esse dado pessoal, será a própria instituição, em sua qualidade de pessoa jurídica, a controladora de dados, e não o funcionário da equipe que efetuou na prática o envio do livro eletrônico.

O mesmo raciocínio serve para o setor público: **servidores e funcionários não podem ser considerados controladores**. Não existe um cargo público de controlador de dados! Este papel será assumido pelos entes federativos e agências estatais para os quais trabalham.

Assim, em um cenário em que o número de CPF de um contribuinte seja usado pela Receita Federal do Brasil (RFB) para a finalidade de processamento do seu imposto de renda, a controladora será a RFB, e não o auditor que fará este processamento.

A partir desta conceituação, uma pessoa física poderá ser considerada um agente de tratamento somente quando ela estiver atuando diretamente e de forma autônoma com o tratamento de dados, mas **não quando representar uma entidade**, caso em que o agente de tratamento será a própria pessoa jurídica.

II. Controlador



O controlador é toda pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões sobre o tratamento de dados pessoais.

Art. 5º, VI - LGPD

Diante da leitura desse dispositivo, parece óbvio definir uma pessoa jurídica como controladora, tendo em vista que bastará identificar o seu poder de decisão quanto à realização de tratamento de dados pessoais.

Apesar dessa conceituação aparentemente simples, diante da complexidade das relações tanto no setor público quanto no privado, precisamos entender determinadas questões como:

- O que compreende exatamente este poder de decisão?
- Qual pessoa natural ou jurídica poderá exercer o papel de controlador?

O Comitê Europeu de Proteção de Dados Pessoais, em inglês - *European Data Protection Board* (EDPB) -, escreveu sobre o tema e definiu a importância sobre a análise de determinados requisitos para a correta designação de um controlador. Este documento ajuda a traçar as primeiras respostas para tantas questões em aberto sobre o tema.

A. Quem pode ser controlador?

Em primeiro lugar, será necessário estabelecer quem pode desempenhar o papel de controlador de dados. Conforme o art. 5º, VI da LGPD, qualquer pessoa natural ou jurídica, de direito público ou privado, poderá assumir essa função.

Como explicado na seção I, a práxis prioriza a pessoa jurídica como o controlador, relegando este papel à pessoa física apenas em casos excepcionais.

Assim, ainda que o Encarregado ou o chefe de uma divisão seja nomeado para garantir o cumprimento das regras de proteção de dados, esta pessoa não será a controladora, pois apenas agirá em nome da pessoa jurídica - empresa ou ente público - sobre a qual recairá a responsável final em caso de violação das regras no tratamento de dados pessoais.[3]

Os elementos pertinentes à definição do controlador são:

- Poder de decisão
- Finalidade
- Meios de tratamento

B. Poder de decisão

Uma característica fundamental para definir quem assume o papel de controlador de dados é o poder de decisão. Para identificar quem o detém, deve-se responder às seguintes perguntas:

- Quem iniciou o tratamento?
- Por que o tratamento está ocorrendo?
- Quem se beneficia com a realização do tratamento de dados pessoais?[4]

Caso a sua instituição tenha decidido iniciar o tratamento de dados pessoais, sabe o motivo pelo qual os dados estão sendo tratados e se beneficia de tal tratamento, existem grandes chances de ela estar atuando como controladora.

O Comitê Europeu de Proteção de Dados (EDPB) aponta duas circunstâncias principais que dão origem ao controle:

(i) determinação legal, seja de forma direta (i.e. competência legal explícita) ou indireta (ex. atribuições legais que implicam o dever de tratar dados pessoais);

(ii) influência fática, quando as atividades concretas do agente em um contexto específico explicitam seu poder de controle.[5] O Comitê ainda alerta que, embora contratos possam ajudar a identificar quem é o controlador, apenas a situação fática irá estabelecer se a entidade age como tal.

O fator mais relevante para caracterizar o controlador é a sua capacidade de decidir sobre a finalidade e os elementos essenciais dos meios de tratamento.

B.1. Finalidade

A finalidade, pelo próprio sentido literal da palavra, significa a escolha sobre o propósito para o qual os dados serão tratados, ou seja, *para que* serão utilizados. É um princípio-chave para a disciplina da proteção de dados pessoais, uma vez que estabelece as fronteiras dentro das quais um dado poderá ser utilizado e garante que ele não seja aplicado para fins inapropriados ou inesperados. A finalidade, nesse sentido, é o primeiro passo para analisar o cumprimento de outros princípios da LGPD, como necessidade, adequação e transparência.[6]

Esta finalidade deve ser informada de forma detalhada para o titular de dados desde o início das operações de tratamento. Cabe ao controlador garantir que quaisquer usos supervenientes dos dados pessoais do titular sejam feitos de forma compatível com o(s) propósito(s) inicial(is) informado(s) ao titular. Neste sentido, é necessário que o controlador apresente da forma mais específica e transparente possível as finalidades que motivarão as operações envolvendo dados pessoais do titular.

Uma instituição normalmente terá diversas finalidades para o tratamento de dados, algumas associadas a suas atividades finalísticas e outras relacionadas a suas atividades-meio.

Suponhamos, por exemplo, que uma loja de comércio irá tratar dados pessoais de seus clientes (ex. nome, endereço, email) com a finalidade de ofertar produtos. Paralelamente, a mesma loja tratará dados de seus funcionários para fins de gestão laboral. Neste caso, a loja é controladora de dados dos clientes e de sua equipe.

É muito importante que uma instituição mapeie os diversos casos de tratamento de dados e os associe às respectivas finalidades. Este é o primeiro passo para identificar quais dados a entidade controla e quais as bases legais que legitimam as operações de tratamento, processos essenciais para que uma organização se adeque à LGPD.

B.2. Meios de tratamento

Os meios de tratamento se relacionam a *como* os dados pessoais serão tratados, e se dividem em **elementos essenciais** e **não essenciais**. Será controladora a organização que tiver o poder de determinação sobre os elementos essenciais.

Os elementos essenciais[7] são:

- o poder de escolha sobre os dados a serem tratados;
- a identificação dos indivíduos sobre quem ocorrerá o tratamento de dados;
- o período de armazenamento; quem terá acesso aos dados (controle de acesso);
- o poder de escolha sobre a base legal que será utilizada para justificar o tratamento;
- a responsabilidade pela garantia dos direitos dos titulares.

Por outro lado, os **elementos não essenciais** compreendem a escolha sobre as medidas técnicas que serão utilizadas para proteger os dados pessoais durante o tratamento, bem como a escolha do sistema, *hardware* ou *software*. Tais atividades podem ser desempenhadas pelo operador de dados, sobre quem falaremos adiante.

III. Operador

O operador é toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

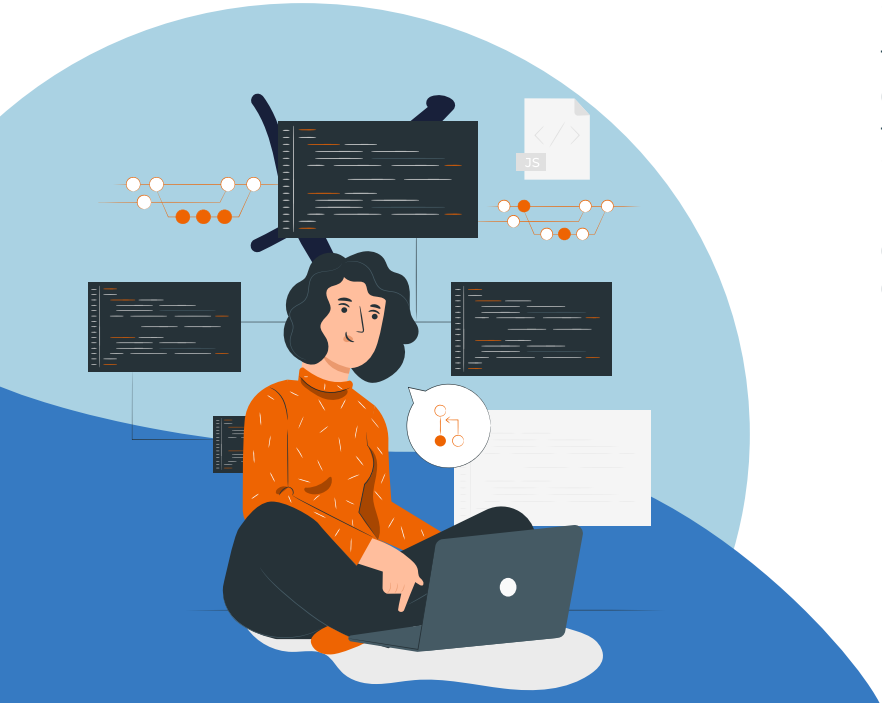
Art. 5º, VII - LGPD

Segundo orientações do EDPB, duas condições são necessárias para qualificar um operador:

(i) ele deve ser uma pessoa (física ou jurídica) **distinta** do controlador;

(ii) ele deve ser responsável por tratar os dados em nome do controlador.[8]

Ser uma pessoa distinta do controlador significa dizer que o controlador decide delegar parte do tratamento de dados pessoais para um terceiro, o qual pode ser tanto uma pessoa natural como uma pessoa jurídica, de direito público ou privado.



Destacamos que não se deve confundir o operador com os funcionários e outras pessoas que estão agindo sob o poder diretivo do controlador, como empregados que firmaram contrato de trabalho, uma vez que estes tratam os dados como parte integrante do controlador de dados pessoais. Da mesma forma, **diferentes equipes e unidades organizacionais de uma instituição que atua como controladora não serão suas operadoras!**[9]

Dando continuidade, tratar os dados em nome do controlador não significa "agir" sob autoridade ou controle deste, significa agir conforme os interesses dele, de acordo com a finalidade e os meios de tratamento decididos por ele. O operador será tão somente responsável pela implementação do tratamento, o que não afasta sua própria independência quanto à *expertise* dos serviços que lhe foram contratados.

Ainda segundo o EDPB[10], o operador não deverá ser considerado um subordinado. Ele **poderá decidir sobre os elementos não essenciais dos meios de tratamento** - como as medidas técnicas de segurança da informação - mas não poderá definir sobre a finalidade e os elementos essenciais dos meios de tratamento, sob pena de responder como se controlador o fosse.

No âmbito europeu, o EDPB estabelece que a relação entre o controlador e o operador deve ser estabelecida por meio de um **contrato de tratamento de dados pessoais ou outro ato legal de efeito vinculativo.**[11] Este contrato costuma ser referido em inglês como *Data Processing Agreement* (DPA). Apesar de a LGPD ser omissa quanto à essencialidade de tal instrumento, a formalização de um contrato deve ser considerada boa prática para estabelecer não só a posição de cada agente como também suas obrigações e responsabilidades conforme as diretrizes legais.

IV. Controladoria conjunta

Uma vez compreendidos os conceitos de controlador e operador de dados, pode-se questionar: "É possível haver mais de um controlador envolvido no tratamento de dados pessoais?"

A resposta é positiva. Na GDPR, quando dois ou mais controladores determinam em conjunto as finalidades e os meios de tratamento, eles devem ser controladores conjuntos (ou co-controladores).[12] O regulamento europeu dedica um artigo inteiro para explicar questões relacionadas à controladoria conjunta.

No caso da LGPD, também vemos o conceito, embora apresentado de uma forma mais simples:

> **Art. 42, §1º, II - LGPD** - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei

Antes de discutirmos a questão da responsabilidade solidária e suas hipóteses de exclusão, foquemos na questão mais importante: como identificar a controladoria conjunta.

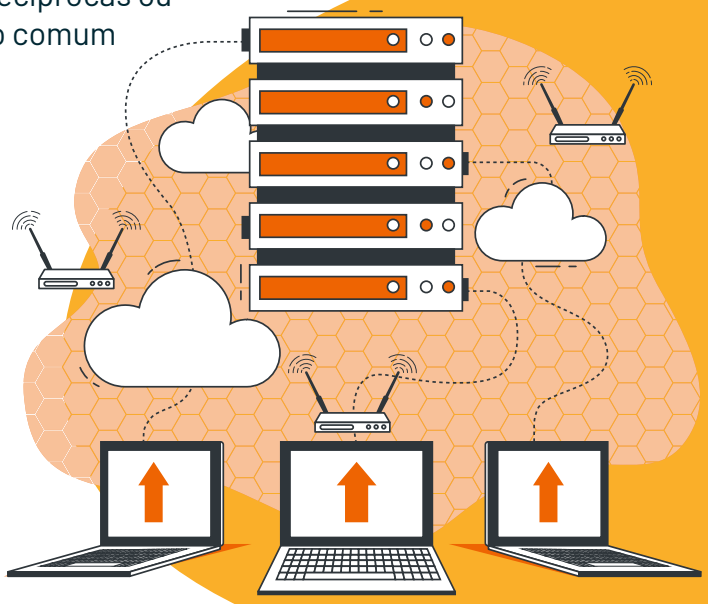
Para responder a esta pergunta, recorremos à parente europeia da LGPD. A GDPR deixa claro que o aspecto central para identificar a controladoria conjunta é identificar quando há uma "participação conjunta" na determinação de finalidades e meios de tratamento. O EDPB explica que esta participação conjunta pode ocorrer de diferentes formas e destaca duas delas: **decisões comuns** e **decisões convergentes.**[13]

As **decisões comuns** implicam duas ou mais entidades decidirem conjuntamente, com uma intenção comum, sobre as finalidades e meios de tratamento. Já as **decisões convergentes** ocorrem quando as decisões complementam uma à outra de forma que as operações de tratamento são indissociáveis, de modo que a participação de cada entidade se faz essencial. Nesse caso, a Corte de Justiça Europeia (CJE) entende que as operações de tratamento são "inextricavelmente ligadas".

A seguir, analisamos os elementos de finalidade e meios de tratamento sob a perspectiva da controladoria conjunta.

No que diz respeito à **finalidade**, a controladoria conjunta significa que dois controladores estão perseguindo um objetivo em comum, convergente ou, ainda, complementar. Quanto a esta última hipótese, sugerimos verificar o quadro sobre o caso *FashionID*, em que a CJE concluiu que uma empresa online de roupas era controladora conjunta com o Facebook por ter participado na determinação das finalidades e dos meios de tratamento ao incluir um plugin de "Curtir" para otimizar sua publicidade na rede social.

Vale frisar que a controladoria conjunta pode ocorrer tanto no contexto público quanto no privado. Deste modo, dois ou mais entes públicos, ou estes e agentes privados, podem ser controladores conjuntos quando juntam esforços e tratam dados pessoais para o alcance de um objetivo, com fins lucrativos ou não. Uma boa forma de visualizar isso corresponde aos acordos de cooperação. Nestes instrumentos, firma-se uma parceria entre duas ou mais entidades públicas, ou, ainda, com entidades privadas, de modo que as partes envolvidas apresentam interesses e condições recíprocas ou equivalentes a fim da realização de um propósito comum voltado ao interesse público.[14]



Contudo, também é importante estabelecer que a mera existência de um benefício mútuo (por exemplo, comercial) advindo da operação de tratamento não implica, necessariamente, a controladoria conjunta.[16] Por exemplo, esta não ocorre se o mesmo conjunto de dados é tratado por dois controladores que perseguem objetivos distintos. Imagine que dados de câmera de segurança de um shopping center são entregues para a polícia no evento de um crime. As finalidades do shopping center (segurança privada) e da polícia (segurança pública), apesar de similares, são substancialmente distintas. Isto pode ser observado pelo fato de que esta última finalidade está excluída do escopo da LGPD, como enunciado no art. 4º, III, alínea a). Logo, nesta hipótese não há controladoria conjunta.

Com relação ao **meio**, como já explicado, o que caracteriza o controlador é o controle sobre os elementos essenciais desse meio de tratamento. Se dois ou mais controladores tomaram a decisão sobre esses elementos essenciais de forma coletiva, tem-se a controladoria conjunta. Não é necessário que cada controlador determine todos os meios envolvidos em uma operação de tratamento para que a controladoria conjunta se estabeleça.

É importante entender que na controladoria conjunta não há relação de subalternidade ou prestação de serviço, ao contrário do que se verifica na relação controlador-operador, em que o primeiro pode delegar a competência de determinar os meios de tratamento para o último.

Identificar casos de controladoria conjunta não é uma tarefa fácil e irá depender muito do caso-a-caso, para que se analisem finalidades e meios de tratamento comuns. Além disso, em um mesmo contexto, podem existir operações de tratamento em que exista a controladoria conjunta, e outras operações em que isto não ocorra (ver quadro do caso *FashionID*).

Quanto às obrigações, elas serão as mesmas da controladoria convencional, com um adicional: a responsabilidade é solidária. Ou seja, ainda que um vazamento de dados tenha ocorrido por falhas de segurança do controlador A, o controlador B poderá ser integralmente responsabilizado pelos danos causados ao titular de dados (assumindo que A e B são controladores conjuntos).

Isso ressalta a importância de que controladores conjuntos devem se certificar que todos os envolvidos possuem um programa de conformidade à LGPD bem-implementado.

Além disso, uma boa prática é a transparência das atribuições respectivas de cada controlador conjunto para a conformidade com a LGPD. Essa alocação de atribuições deve ser feita entre as partes por meio de um contrato ou outro acordo legalmente válido.[17]

Por fim, cabe observar que uma mesma organização pode ser controladora conjunta nas operações de tratamento de um determinado serviço, e controlador simples para outras operações. Para distinguir cada caso, deve-se sempre observar quantos agentes estão responsáveis por definir a finalidade e os meios de tratamento. Para uma melhor ilustração verificar a seção VI.

Caso *Fashion ID* (C-40/17 da CJE)[18]

Em 2019, a Corte de Justiça Europeia julgou o caso *Fashion ID*. Nele, a corte concluiu que o administrador de um site que apresenta um botão de "Curtir" do Facebook pode ser um controlador em conjunto com a rede social no que diz respeito à coleta e à transmissão para o Facebook dos dados pessoais dos visitantes de seu site.

A fundamentação da Corte foi que a incorporação do botão "Curtir" no site da varejista online de roupas *Fashion ID* permitia que esta otimizasse a publicidade dos seus produtos, tornando-os mais visíveis na rede social do Facebook quando um visitante do seu site clicasse naquele botão.

Assim, as operações de coleta e transmissão dos dados pessoais de visitantes do site da Fashion ID ao Facebook eram realizadas no interesse econômico de ambas.

Contudo, a CJE também estabeleceu que a *Fashion ID* não pode ser considerada controladora no que diz respeito às operações de tratamento de dados efetuadas pelo Facebook após esses dados terem sido transmitidos a esta última.

V. Exemplos

A seguir, são apresentados alguns exemplos práticos que ajudam a ilustrar os conceitos apresentados nas seções anteriores. Os exemplos são fictícios e inspirados em outros guias sobre o tema, como os guias do EDPB[19] e da *European Data Protection Supervisor* (EDPS).[20]

Exemplo 1

A associação ABC decide contratar a empresa XYZ, prestadora de serviços de armazenamento em nuvem para armazenar os dados de seus associados.

Ao decidir realizar o tratamento (coleta e armazenamento) desses dados, bem como quais dados seriam tratados (dos associados), para quais finalidades (armazenamento) e período de armazenamento (enquanto durar a associação ou cumprimentos legais decorrentes).

A empresa XYZ, fará o armazenamento para o qual foi contratada, em seus servidores remotos, para acesso pelas pessoas específicas determinadas pela associação, pelo período por esta solicitado.

É possível que a associação ABC solicite requisitos técnicos específicos de segurança da informação, por exemplo. Contudo, a segurança da informação trata-se de especialidade da empresa XYZ. Natural, portanto, que esta empresa defina diversas medidas técnicas para a prestação adequada dos serviços.

Neste exemplo, a associação ABC é a controladora, pois possui poder decisório e determina os meios de tratamento. Quanto aos meios, determinou elementos essenciais e eventualmente algum elemento não essencial.

Por sua vez, a empresa XYZ, prestadora dos serviços de nuvem, seguiu o que foi solicitado pela associação na contratação e definiu apenas elementos não essenciais do tratamento, assumindo o papel de operadora de dados. Ainda que venha fazer sugestões sobre os meios essenciais de tratamento (por exemplo, regras sobre coleta e armazenamento), caberá à controladora, a associação ABC, tomar a decisão final sobre a forma que se dará o tratamento de dados.

Exemplo 2[21]

A Empresa ABC deseja entender quais tipos de consumidores têm maior probabilidade de se interessar por seus produtos e contrata um Provedor de Serviços, XYZ, para obter as informações relevantes.

A Empresa ABC instrui a XYZ sobre o tipo de informação em que está interessada e fornece uma lista de perguntas a serem feitas aos participantes da pesquisa de mercado.

A Empresa ABC recebe apenas informações estatísticas de XYZ (por exemplo, informações que identificam tendências de consumo por região) e não tem acesso aos dados pessoais em si.

No entanto, a Empresa ABC que decidiu como o tratamento deve ocorrer; o tratamento é realizado para seus propósitos e para a sua atividade e a Empresa ABC forneceu à XYZ instruções detalhadas sobre quais informações esta deveria coletar.

Portanto, a Empresa ABC deve ser considerada controladora, no que diz respeito ao tratamento de dados pessoais que foi realizado para fornecer as informações solicitadas pela Empresa. XYZ só pode tratar os dados para os fins fornecidos pela Empresa ABC e de acordo com suas instruções detalhadas, devendo, portanto, ser considerada uma operadora.

Exemplo 3

Uma loja virtual de sapatos deseja ampliar as suas vendas. Com a finalidade de realizar estudo do comportamento dos seus clientes e melhorar as suas estratégias de marketing, a loja se cadastra junto a um serviço de analytics, que fornece estatísticas de visitação de páginas web.

Nesse caso, a própria loja virtual decidiu decidiu sobre o início do tratamento de dados pessoais, sua finalidade (estudo do comportamento dos seus próprios clientes), os dados pessoais que serão objeto do tratamento (registros de log, interação do consumidor com o site, localização, etc), sobre quais indivíduos tratar (consumidores da sua loja), a base legal que justifica o tratamento, e o controle de acesso.

Sendo assim, a loja virtual atuará como controladora dos dados pessoais, ao passo que o serviço de analytics agirá como operador de dados pessoais, tendo-se em vista que será responsável tão somente pela implementação do tratamento de dados pessoais e possuindo liberdade para agir conforme o seu *know how* e de acordo com a finalidade e os elementos essenciais dos meios de tratamento definidos pelo controlador.

Exemplo 4[22]

Uma agência de viagens, uma rede de hotéis e uma companhia aérea decidem criar uma plataforma na Internet para facilitar a gestão de reservas de viagem. Elas decidem que dados serão armazenados na plataforma, como as reservas que serão alocadas e confirmadas, quem poderá acessar as informações, etc. Também compartilham dados de clientes para realizar ações integradas de marketing.

Nesse caso, os três agentes - agência de viagens, rede de hotéis e companhia aérea - serão **controladores conjuntos** com relação aos dados pessoais tratados na plataforma de serviços, pois definem conjuntamente a finalidade "facilitar a gestão de reservas de viagem".

Também é possível notar que vários elementos essenciais dos meios de tratamento - tipos de dados armazenados, alocação de reservas, controle de acesso - são definidos de forma conjunta.

Para outras atividades de tratamento, como serviços oferecidos por fora do sistema integrado (ex. voos que sejam comprados direto pelo site da companhia aérea) e gestão de recursos humanos, não haverá controladoria conjunta.

Exemplo 5

O Empregador A trata dados pessoais de seus funcionários para fins de pagamento, exercício das atividades contratadas, concessão de benefícios, acesso às suas dependências, entre outras finalidades.

Além disso, por imposição legal, compartilha os dados pessoais de seus funcionários com o Governo Federal, por meio do Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas (eSocial) para fins de cadastro geral de empregados, concessão de auxílio-doença quando aplicável, INSS, FGTS, entre outros.

Embora o Empregador A e o Governo Federal tratem os mesmos dados pessoais, a ausência de determinação conjunta quanto à finalidade e aos meios de tratamento resulta na atuação de dois controladores autônomos e independentes.

VI. Responsabilidades e obrigações dos agentes de tratamento

A. A natureza da responsabilidade civil na LGPD

A LGPD destaca em seu texto, nos artigos 42 a 45, as regras que irão estabelecer os limites das responsabilidades do controlador e do operador.

Em primeiro lugar, a Lei afirma que qualquer dano, seja ele patrimonial, moral, individual ou coletivo decorrente da violação da legislação de proteção de dados pelo controlador ou operador, em razão do exercício da atividade de tratamento de dados pessoais, deve ser reparado.[23] Entretanto, a LGPD não estabeleceu de forma expressa qual deve ser o regime de responsabilidade civil aplicável: objetivo ou subjetivo.[24]

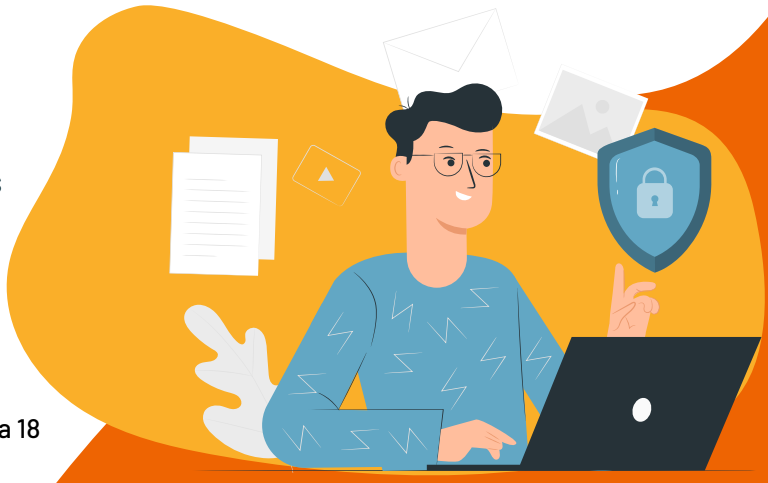
Danilo Doneda e Laura Schertel entendem que **a responsabilidade dos agentes de tratamento é preponderantemente objetiva, levando-se em consideração o risco da atividade, independentemente da culpa do agente de tratamento.[25]**

Para os doutrinadores, em razão de a LGPD ter como um dos seus principais fundamentos a minimização do riscos de dano, é possível inferir que o legislador adotou o regime de responsabilidade objetiva. Isto se justifica pela existência de um risco intrínseco à atividade de tratamento de dados que está relacionado à capacidade iminente de gerar dano aos titulares dos dados caso seus direitos sejam violados ou princípios da lei não sejam observados.

No sentido oposto, Gisela Sampaio e Rose Meireles ressaltam que a LGPD é estruturada com base na criação de obrigações dos agentes de tratamento,[26] sob pena de estes serem responsabilizados pelo seu não cumprimento. De acordo com as autoras, não faria muito sentido o legislador dispor sobre deveres aos agentes de tratamento de dados pessoais se não fosse para implementar um regime de responsabilidade subjetiva.

Considerando as visões distintas dos autores, é necessário salientar que a depender das disposições da LGPD - e do caso concreto - o regime de responsabilidade poderá ser subjetivo ou objetivo, observadas as hipóteses previstas em lei.

Podemos tomar como exemplo tratamentos de dados que envolvam relações de consumo. Nestes casos, a responsabilização dos agentes se dará pelo regime da responsabilidade objetiva, uma vez que a obrigação de indenizar as lesões causadas aos titulares de dados será dos agentes de tratamento, o que afasta dos indivíduos o ônus de comprovar a existência de sua culpa.[27]



De acordo com a LGPD, o controlador possui responsabilidade ampla em relação ao tratamento de dados pessoais sob sua gestão, visto que este responde pela observância desta Lei, bem como pelos danos que causar ao titular.[28] O controlador responderá **solidariamente** por qualquer violação à legislação e/ou danos causados tanto pelo operador quanto por outros controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados.[29] Assim, **a responsabilidade do controlador é solidária e também abrangerá as ações do operador dos dados**, quando este realizar tratamentos para as finalidades do controlador.

Em contrapartida, o **operador** apenas será solidariamente responsável quando não observar a LGPD, ou realizar atividades de tratamento de dados fora do escopo das instruções do controlador dos dados pessoais, hipótese em que se equipara ao controlador.[30] Assim, **a responsabilidade do operador será restrita apenas às suas próprias ações, desde que não se equipare ao controlador ou não desrespeite a LGPD.**

O **direito de regresso** em face do responsável pelo dano será reservado àquele que repará-lo, na medida de sua participação no evento danoso.[31] Por outro lado, a LGPD prevê algumas hipóteses de **exclusão de responsabilidade** dos agentes de tratamento. Isto ocorrerá quando os agentes provarem:[32]

(i) que não realizaram o tratamento de dados que lhes foi atribuído;

(ii) que mesmo tendo realizado o tratamento dos dados pessoais, não violaram a legislação de proteção de dados; ou

(iii) que o dano ao titular dos dados foi decorrente de culpa exclusiva deste ou de terceiro.

B. Obrigações do Controlador e Operador

A seguir, listamos as principais obrigações do controlador e do operador no tratamento de dados pessoais, com base no que dispõe a LGPD, e com o auxílio das boas práticas endereçadas pela autoridade de proteção de dados do Reino Unido, o *Information Commissioner's Office* (ICO):[33]

Controlador

- **Conformidade com os princípios da LGPD**

  Art. 6º - LGPD

  Os controladores devem cumprir todos os princípios de proteção de dados listados na LGPD.

- **Direitos dos indivíduos**

  Art. 18 - LGPD

  O controlador deve garantir que os indivíduos possam exercer seus direitos em relação aos seus dados pessoais.

- **Segurança**

  Art. 46 - LGPD

  O controlador deve implementar medidas de segurança técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais. No mesmo sentido, o controlador deve **contratar operadores de dados que forneçam garantias suficientes** de que serão implementadas medidas técnicas e organizacionais adequadas para assegurar que o tratamento atenda aos requisitos de segurança da LGPD. Assim, o controlador é responsável por avaliar se seu operador é competente para processar os dados pessoais de acordo com a lei. Embora a LGPD não defina critérios, o EDPB recomenda que o **conhecimento técnico** do operador, sua **confiabilidade** e seus **recursos**[34] sejam elementos a serem observados.

  A aderência a códigos de conduta ou mecanismos de certificação aprovados também é bem-vinda. A avaliação do operador deve levar em consideração a natureza do tratamento dos dados e os riscos para os titulares dos dados pessoais.

- **Comunicação de incidentes de segurança com dados pessoais**

  Art. 48 - LGPD

  O controlador é responsável por comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, conforme as orientações adicionais da Autoridade.[35]

- **Registro de operações de tratamento de dados**

  Art. 37 - LGPD

  O controlador deve manter registro das operações de tratamento de dados pessoais que realizar, especialmente quando baseado no legítimo interesse.

- **Elaboração de Relatórios de Impacto de Proteção de Dados (RIPD)**

  Art. 38 - LGPD

  O controlador deve estar preparado para elaborar RIPDs conforme venha a ser determinado pela ANPD. Como boa prática, recomenda-se que operações de alto risco para os titulares de dados sejam precedidas da elaboração de um RIPD.

- **Nomeação de encarregado de dados**

  Art. 41 da LGPD

  O controlador deverá indicar encarregado pelo tratamento de dados pessoais, que atuará como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

- **Transferências internacionais**

  Art. 33 a 36 - LGPD

  O controlador deve cumprir as diretrizes da LGPD em relação às transferências de dados pessoais para países estrangeiros ou organismos internacionais dos quais o país de origem do controlador seja membro.

Operador

- **Instruções do controlador**

  Art. 39 e Art. 42, § 1º, I - LGPD

  O operador só pode processar os dados pessoais por meio de instruções de um controlador. Se o operador agir fora de suas instruções ou tratar dados pessoais para suas próprias finalidades sairá de sua função como operador e se tornará um controlador desse tratamento.

- **Contratos com o controlador**

  É aconselhável que o operador celebre um contrato vinculativo com o controlador. Este instrumento deve conter uma série de disposições obrigatórias, nas quais o operador deverá basear-se para o cumprimento de seus deveres.

- **Sub-Operadores**

  Recomenda-se que o operador não envolva outro operador sem a autorização prévia, por escrito, específica ou geral do controlador. Se a autorização for concedida, o operador deve firmar um contrato com o subcontratado, com termos que ofereçam um nível de proteção equivalente para os dados pessoais como aqueles dispostos no contrato entre o operador e o controlador.

- **Segurança**

  Art. 46 - LGPD

  O operador deve implementar medidas técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais.

- **Notificação de incidentes de dados pessoais**

  Se o operador tomar conhecimento de um incidente de segurança envolvendo dados pessoais, deverá notificar o controlador sem atrasos injustificados. O operador também deve colaborar com o controlador para que este mitigue os riscos causados em relação a violações de dados pessoais.

- **Notificação de possíveis violações de proteção de dados**

  Art. 48 - LGPD

  O operador deve notificar o controlador imediatamente se alguma de suas instruções levar a uma violação da LGPD ou demais leis aplicáveis.

- **Transferências internacionais**

  Qualquer transferência internacional deve ser autorizada pelo controlador, bem como estar em conformidade com as disposições de transferência internacional da LGPD.

- **Registro de operações de tratamento de dados**

  Art. 37 - LGPD

  O controlador deve manter registro das operações de tratamento de dados pessoais que realizar, especialmente quando se basear no legítimo interesse.

C. Contratos entre controlador e operador

A LGPD não é expressa quanto ao uso de cláusulas contratuais para regular a relação entre controladores e operadores, entretanto, a utilização de disposições em contrato e acordos, com o fim de resguardar cada uma das partes e estabelecer seus direitos e obrigações é a melhor medida para mitigar riscos e divergências na relação entre os agentes de tratamento.

Além de estabelecerem disposições acerca de procedimentos para a cooperação do operador junto ao controlador em caso de incidentes de segurança envolvendo dados pessoais, bem como resposta a requisições de titulares, as cláusulas contratuais poderão dispor entre outros elementos sobre:

- procedimentos de cooperação entre operador e controlador em caso de incidentes de segurança envolvendo dados pessoais;
- procedimentos de resposta a requisições de titulares;
- a adoção de boas práticas de segurança e governança de dados.

É importante ressaltar que alguns pontos relacionados às obrigações dos agentes de tratamento devem estar transparentes no contrato, considerando que a Lei 13.874/2019 adicionou o art. 421 no Código Civil, o qual estabelece que nas "relações contratuais privadas, prevalecerão o princípio da intervenção mínima e a excepcionalidade da revisão contratual". Portanto, ajustes específicos sobre obrigações e responsabilidades que não estão dispostas na LGPD deverão ser pontuados claramente pelas partes do contrato.

Finalmente, no caso de operações que envolvam transferências internacionais de dados, é comum a adoção de **cláusulas-padrão contratuais** - em inglês, *Standard Contractual Clauses* (SCCs). Estas cláusulas são aprovadas por uma autoridade competente que legitima a operação. Como exemplo, citam-se as cláusulas para transferência internacional de dados entre controladores ou entre controlador e operador aprovados pela Comissão Europeia.[36]

Nesse contexto, é importante entender o sentido do fluxo de dados! As SCCs supramencionadas são válidas para hipóteses em que o controlador exportador se encontra na União Europeia (UE). Além disso, com a recente decisão da Corte de Justiça Europeia no caso *Schrems II*,[37] essas cláusulas por si só não são suficientes para validar operações de transferência da UE para outros países. Os controladores deverão fazer uma análise caso-a-caso sobre se o nível de proteção oferecido pela legislação do país-destino é compatível com aquele oferecido pela GDPR.

Embora cláusulas-padrão contratuais sejam hipóteses previstas legalmente para legitimar operações de transferência internacional de dados originadas no Brasil[38], caberá à ANPD regulamentar o tema.

Conclusão

O primeiro passo para um programa de adequação à LGPD bem-sucedido é entender o papel que a organização assumirá frente à lei. A compreensão do papel de uma entidade, como controladora ou operadora, em relação às atividades desempenhadas (especialmente àquelas atividades que envolvam outras organizações) é fundamental para conduzir processos que envolvam o tratamento de dados em conformidade com a LGPD e demais legislações aplicáveis.

Identificar os agentes de tratamento é primordial não só para a atribuição de obrigações e responsabilidades contratuais como também para o cumprimento de obrigações perante os titulares e a Autoridade Nacional de Proteção de Dados.

O LAPIN espera que esta cartilha tenha lhe ajudado a definir com mais segurança a posição que sua instituição ocupa no tratamento de dados. Continuaremos trabalhando para a promoção de um ecossistema próspero de proteção de dados pessoais no Brasil! Até a próxima!

Notas de fim

[1] **Art. 5º, inciso VIII, da Lei 13.709/18 (LGPD):**
"Para os fins desta Lei, considera-se: (...) VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)."

Art. 42, caput, da LGPD:
"O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo."

[2] MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2 ed. revista, atualizada e ampliada. São Paulo Thomson Reuters Brasil, 2019, p.109.

[3] EUROPEAN DATA PROTECTION BOARD (EDPB). **Guidelines 07/2020 on the concepts of controller and processor in the GDPR**. Version 1.0. 2. set. 2020, p.10. Disponível em: **<https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf>**. Acesso em: 22 out. 2020.

[4] EUROPEAN DATA PROTECTION SUPERVISOR (EDPS). **Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725**. 7 nov. 2019, p.9. Disponível em: **<https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf>**. Acesso em: 19 mai. 2020.

[5] EDPB, op.cit. p.11.

[6] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 03/2013 on purpose limitation**. 2 abr. 2013. Disponível em: **<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>**. Acesso em: 17 set. 2020.

[7] EDBP, op.cit. p.24.

[8] Ibid., p.24.

[9] Ibidem.

[10] Ibid., p.14.

[11] Ibid., p.30.

[12] **Art.26, ponto 1, da GDPR:**
"1. Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento.

Estes determinam, por acordo entre si e de modo transparente as respetivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respetivos deveres de fornecer as informações referidas nos artigos 13º e 14º, a menos e na medida em que as suas responsabilidades respetivas sejam determinadas pelo direito da União ou do Estado-Membro a que se estejam sujeitos. O acordo pode designar um ponto de contacto para os titulares dos dados."

[13] EDBP, op.cit. p.18.

[14] UNIFESP. **Acordo de Cooperação**. 2019. Disponível em: **<https://www.unifesp.br/reitoria/proadmin/documentos/convenios/acordo-de-cooperacao>**. Acesso em: 06 out. 2020.

[15] EDBP, op.cit. p.19.

[16] Ibidem.

[17] Ibid., p.43.

[18] COMISSÃO DE JUSTIÇA EUROPEIA (CJE). **Processo C-40/17**. Fashion ID GmbH & Co.KG v.Verbraucherzentrale NRW eV Disponível em: **<https://curia.europa.eu/juris/document/document.jsf;jsessionid=618F476358B0BB793D53A5B9A74F0316?text=&docid=218050&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=2310591>**. Acesso em: 22 out. 2020.

[19] EDPB, op.cit.

[20] EUROPEAN DATA PROTECTION SUPERVISOR (EDPS). **Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725**. 7 nov. 2019, p.9. Disponível em: **<https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf>**. Acesso em: 19 mai. 2020.

[21] EDPB, op.cit., p.16.

[22] EDPB, op.cit., p.20.

[23] Art.42, caput, da LGPD. Ver nota de fim número [1].

[24] MULHOLLAND, Caitlin. **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?** Rio de Janeiro. 30 jun.2020. Disponível em: **<https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais-culpa-ou-risco>**. Acesso em: 14 set.2020.

[25] MENDES, Laura Schertel; DONEDA, Danilo. **Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil**. Revista de Direito do Consumidor. v.120, 2018, p. 555.

[26] GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. **Término do tratamento de dados**. In.: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. Lei Geral de Proteção de Dados. São Paulo: Editora RT, 2019, p.122.

[27] MULHOLLAND, Caitlin. Op. cit.

[28] Art.42, caput, da LGPD. Ver nota de fim número [1].

[29] **Art.42, §1º, II, da LGPD:**
"§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei."

[30] **Art.42, §1º, I, da LGPD:**
"[...] I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei."

[31] **Art.42, §4º, da LGPD:**
"§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso."

[32] **Art.43 , incisos I, II e III, da LGPD:**
"Os agentes de tratamento só não serão responsabilizados quando provarem:
I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro."

[33] INFORMATION COMMISSIONER'S OFFICE (ICO). **What does it mean if you are a controller?** Reino Unido. Disponível em: **<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-a-controller/#1>**. Acesso em: 13 set. 2020.

[34] EDPB, op.cit., p. 30.

[35] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Incidentes de Segurança com Dados Pessoais e sua Avaliação para fins de Comunicação à ANPD**. Disponível em: **<https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>**. Acesso em: 15 mar. 2021.

[36] COMISSÃO EUROPEIA. **Standard contractual clauses for data transfers between EU and non-EU countries**. Disponível em: **<https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en>**. Acesso em: 06 out. 2020.

[37] COMISSÃO DE JUSTIÇA EUROPEIA (CJE). **C-311/18 - Facebook Ireland e Schrems**. Data Protection Commissioner v. Facebook Ireland Ltd e Maximillian Schrems.16 jul.2020. Disponível em: **<https://curia.europa.eu/juris/liste.jsf?num=C-311/18>**. Acesso em: 06 out. 2020.

[38] **Art. 33, II, alínea b) da LGPD:**
"A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
[...]
II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
[...]
b) cláusulas-padrão contratuais"