GAIA SILVA GAEDE
ADVOGADOS

Cadernos de Direito Empresarial

2020

Edição Especial

LGPD - Lei Geral de Proteção de Dados

Cadernos de Direito Empresarial

Volume 15

Coordenadores:
Fernando Antonio Cavanha Gaia
Maurício Barros

São Paulo
Gaia Silva Gaede Advogados
2020

Sumário

A LGPD - LEI GERAL DE PROTEÇÃO DE DADOS CHEGOU – E AGORA, O QUE FAZER?

Por:

IVAN HASSE

Sócio e responsável pela área de Tecnologia da Informação do escritório Gaia Silva Gaede Advogados

1. INTRODUÇÃO

Em agosto de 2018 foi publicada a Lei Geral de Proteção de Dados (LGPD), com vigência a partir de 2021, que dispõe sobre o tratamento dos dados de pessoas naturais, pelas pessoas físicas ou jurídicas, "com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade".

Muito se tem falado, de forma genérica, a respeito da Lei e dos impactos que ela trará para o meio empresarial. Porém, percebe-se que ainda há uma certa apreensão a respeito das suas reais consequências no dia a dia dos negócios.

A LGPD é uma evolução para o mundo digital, foi elaborada com base na GDPR – Regulamento Geral de Proteção de Dados, vigente na Comunidade Europeia desde 2018 - idealizada em 2012 e aprovada em 2016 -, composta por um conjunto de regras que tratam da proteção e da privacidade dos dados das pessoas naturais.

O presente artigo tem como objetivo demonstrar (i) os reais impactos que a LGPD trará para o mundo dos negócios e (ii) as principais medidas que deverão ser adotadas para a sua implementação.

2. REAIS IMPACTOS DA LGPD NO MUNDO DOS NEGÓCIOS

Apesar de conter algumas imperfeições técnicas, depender da criação da ANPD – Agência Nacional de Proteção de Dados, e da edição de algumas regulamentações complementares, a LGPD entrará em vigor em 2021, impondo para seus usuários uma nova e revolucionária forma no tratamento e controle dos dados das pessoas naturais.

São direitos do titular dos dados: (i) a confirmação da existência de tratamento dos dados, (ii) o acesso aos dados quando solicitados, (iii) a correção dos dados que por ventura estejam incompletos, inexatos ou desatualizados, (iv) a anonimização, bloqueio ou eliminação de dados desnecessários, (v) a possibilidade

de transferir seus dados para outro fornecedor de serviços, e (vi) a eliminação dos dados pelo seu detentor, quando solicitado pelo titular ou quando não forem mais necessários.

A empresa que deixar de observar a LGPD no processo de controle e tratamento dos dados das pessoas naturais poderá incorrer em penalidades severas, como a aplicação de uma multa que pode chegar ao montante de R$ 50 milhões por evento, no caso de uso indevido dos dados e/ou prejuízo ao seu titular.

Após a vigência da Lei, os reflexos e consequências para quem receber, processar e armazenar dados de pessoas naturais serão grandes. Assim sendo, será necessário, por parte das empresas, a implementação de controles precisos e detalhados dos dados, desde o seu recebimento até o seu armazenamento final e/ou eliminação, caso o seu uso não seja mais necessário. Procedimentos atuais deverão ser revistos e adaptados para uma nova forma de trabalho e os sistemas de processamentos de dados deverão sofrer alterações para que tratem os dados de forma adequada, em consonância com as disposições da LGPD.

Para exemplificar tal complexidade, imagine uma situação na qual uma empresa receba por e-mail o currículo de um pretenso candidato para ocupar determinado cargo e que esse currículo seja encaminhado, por e-mail, para os gestores dos diversos departamentos da empresa, para uma eventual análise e possível contratação. O currículo, que circulou pelos diversos departamentos da organização, ficou armazenado com vários usuários, sem a adoção de qualquer medida de controle e acompanhamento, dificultando de sobremaneira a aplicação da LGPD.

Nesse exemplo, a empresa deverá inicialmente obter um consentimento prévio e formal do seu titular, bem como deverá possuir um controle detalhado por onde o currículo circulou e ficou armazenado, para que se possa futuramente, após o seu tratamento, eliminá-lo a pedido do seu titular ou pelo fato de ele não ser mais necessário.

Note-se, com o exemplo acima, a dificuldade que uma organização terá para localizar e eliminar um determinado dado, considerando que ele ficou armazenado em diversos computadores da organização, sem uma possibilidade efetiva de rastreabilidade.

A LGPD é muito clara: as empresas não poderão mais simplesmente armazenar dados de pessoas naturais, como atualmente é feito, pois somente poderão armazená-los em condições específicas previstas em lei. Deverão eliminar os dados após o seu uso, seja por solicitação expressa de seu titular, seja pelo fato de encerrar o seu tratamento, quando os dados deixam de ser necessários para o exercício da sua atividade.

A LGPD destina-se fundamentalmente a regular as relações jurídicas que envolvam qualquer manuseio de dados ou informações de pessoas naturais recebidas por pessoas físicas ou jurídicas, e que, de alguma forma, processem e/ou armazenem esses dados. A referida lei tem como principal objetivo proteger a privacidade das pessoas naturais, em um mundo hoje altamente tecnológico, onde a informação circula em altíssima velocidade. Uma eventual falha de controle no processamento e armazenamento desses dados pode acarretar consequências indesejadas, seja para o operador ou para o controlador dos dados.

O uso inadequado e a monetização dos dados de pessoas naturais pelas empresas, sem uma prévia e expressa autorização de seus titulares, é proibido pela Lei, e o seu descumprimento acarreta responsabilização para quem a praticar, com a imposição de multas severas e a reparação do dano causado ao seu titular.

A LGPD não distingue as pessoas físicas ou jurídicas que processam os dados de pessoas naturais, ela é aplicada da mesma forma para ambas, independentemente do porte econômico de seu agente (operador ou controlador).

A adequação das empresas à LGPD não será uma tarefa fácil, demandará um esforço considerável de todos os envolvidos, bem como uma mudança substancial na forma de coleta e tratamento dos dados de pessoas naturais.

Diante dessa nova realidade, as empresas devem buscar meios para se adequarem da melhor forma possível às disposições da LGPD. Assim, faz-se necessário o desenvolvimento de novos procedimentos e rotinas internas, detalhando todos os aspectos que, de alguma forma, envolvam dados pessoais, o que será visto no próximo tópico.

3. AS PRINCIPAIS MEDIDAS QUE DEVERÃO SER ADOTADAS PARA A IMPLEMENTAÇÃO DA LGPD

Os cuidados com a segurança dos dados serão de extrema importância no processo de adequação à LGPD, devendo ser implementadas medidas adicionais para a sua segurança, como forma de prevenir vazamentos de informações e evitar que tal situação acarrete prejuízos para os seus titulares.

Dentre os procedimentos necessários para adequação das empresas à LGPD, pode-se elencar alguns:

- **Obter o apoio irrestrito da alta administração da empresa**, uma vez que sem esse apoio o projeto de adequação acaba se tornando inócuo, já que a burocracia gerada acaba criando nos usuários uma resistência natural às mudanças;

- **Eleger uma pessoa ou um grupo de pessoas encarregadas pela LGDP**, como forma de organizar e controlar o processo de adequação e atendimento aos procedimentos e exigências necessárias. É muito importante que o profissional responsável por essa tarefa tenha conhecimento técnico dos sistemas de informática que a empresa utiliza, incluindo as práticas de segurança da informação. Não menos importante, esse profissional deve poder interagir e transitar livremente em todas as áreas e departamentos da empresa envolvidos com o tratamento de informação, de tal sorte que se possa conscientizar e disseminar as iniciativas implementadas;

- **Mapear as informações**, analisando a estrutura atual dos dados que a empresa possui, para que se avalie o nível de maturidade da empresa para cuidar e proteger os dados, estabelecendo um plano de ação consistente e efetivo;

- **Identificar os atores envolvidos no tratamento dos dados**, para que seja possível estabelecer com detalhe uma rotina interna para cada uma das tarefas que a empresa realiza no seu dia a dia. Nessa etapa é importante estabelecer o papel na empresa - se controlador, operador

ou encarregado -, em cada tarefa desenvolvida, uma vez que cada ator possui uma atribuição específica para com os dados. Fundamental que se mapeie também, como os dados são compartilhados com terceiros, caso aplicável, estabelecendo políticas e procedimentos necessários, de tal sorte que cada um dos atores assuma a responsabilidade que lhe cabe, na correta proporção;

- **Revisar as políticas internas de acesso à informação**, bem como os perfis dos usuários, se eles estão condizentes com o papel e com a atribuição que cada um exerce nas etapas de uso e processamento dos dados;

- **Mapear as ferramentas (*software*) e dispositivos (*hardware*)** que são utilizados no tratamento dos dados, como forma de conhecer todos os meios que os usuários utilizam e estabelecer, em todas as etapas, o controle e fluxo da informação;

- **Compreender o *business* da empresa**, como forma de identificar em conjunto com a área de gerenciamento de riscos - *Compliance* e controles internos -, as dificuldades ao cumprimento dos procedimentos estabelecidos, alinhados com os princípios da LGPD (respeito à privacidade, autodeterminação informativa, liberdade de expressão, inviolabilidade da informação, desenvolvimento econômico e tecnológico, livre iniciativa e livre concorrência, respeito aos direitos humanos e ao livre desenvolvimento da personalidade, e o exercício da dignidade pelas pessoas naturais), evitando a duplicação dos dados ou mesmo o seu armazenamento por tempo superior ao necessário. Deve-se compreender também quais são o objetivo e a estratégia da empresa para com os dados, identificando aqueles que realmente são necessários para o atingimento desses objetivos, sua essencialidade e justificativa de armazenamento. Se armazenados, deve-se verificar a possibilidade e a necessidade de anonimização, bem como se é preciso manter os dados no seu formato original por alguma questão específica ou imposição legal. Caso contrário, os dados devem ser descartados, adotando-se procedimentos específicos que permitam a comprovação do descarte,

com o estabelecimento de quem será responsável por tal procedimento, devidamente documentado;

- **Identificar, analisar e avaliar os riscos envolvidos**, contemplando os aspectos técnicos e bases legais para o tratamento dos dados pessoais, com a identificação das possíveis falhas que possam ocorrer;

- **Definir os procedimentos necessários para implementar os mecanismos de segurança das bases de dados**, bem como avaliar os riscos existentes e eventuais falhas de segurança. A ausência de medidas de segurança pode sinalizar, para agentes externos, que está havendo um tratamento irregular dos dados, trazendo consequência indesejáveis para a empresa. Sendo assim, torna-se necessário demonstrar que estão sendo adotadas medidas corretas e efetivas para evitar o vazamento de informações;

- **Implementar políticas de monitoramento periódico de segurança** dos sistemas de informática utilizados pela empresa, bem como implementar mecanismos para controle de acesso aos sistemas e ao banco de dados;

- **Adotar políticas internas de backups periódicos dos dados** com redundância e armazenamento em ambientes seguros e controlados;

- **Estabelecer uma política de monitoramento constante dos e-mails**, da rede interna e das estações de trabalho, bem como procedimentos de troca periódica das senhas de acesso aos sistemas utilizados;

- **Adequar os sistemas utilizados pela empresa** com o objetivo de possibilitar o cumprimento dos requisitos exigidos pela LGPD, adotando uma política de privacidade que deverá ser aceita pelo titular dos dados, bem como o registro dos consentimentos e solicitações por ele realizadas;

- **Implementar procedimentos administrativos**, revisando as políticas internas e externas de privacidade, com a adoção de cláusulas a se-

rem inseridas nos documentos de consentimento e controle dos dados, com a ciência e aderência, por todos, das políticas internas da empresa;

- **Analisar os atuais contratos com colaboradores e terceiros** que envolvam processamento de dados, adequá-los às políticas internas da empresa que versem sobre a LGPD, inclusive com a adoção de procedimentos de *Due Diligence*, para avaliar se determinado prestador tem condições de atender às necessidades de cumprimento exigidas pela Lei;

- **Adotar procedimentos periódicos de treinamento, conscientização e capacitação dos usuários**, inclusive terceiros, considerando que o incentivo às boas práticas de segurança e a mudança na cultura interna da empresa podem evitar um eventual vazamento de informações. A educação dos usuários sobre o uso consciente dos meios digitais é o meio mais eficiente de evitar que a empresa se exponha a riscos;

- **Documentar todos os procedimentos**, bem como implementar rotinas para o registro dos tratamentos realizados com os dados, com a adoção de metodologia própria para a rastreabilidade de todas as etapas de processamento às quais os dados foram submetidos ou compartilhados com terceiros durante o seu tratamento;

- **Definir procedimentos de controle e investigação**, com a adoção de mecanismos de boa prática e proteção dos dados, para que, caso ocorra eventual falha de segurança no tratamento dos dados, possa-se conter o evento, mitigando-se os efeitos prejudiciais à empresa e ao titular dos dados; e

- **Elaborar documentos, formulários e modelos de relatórios** que serão utilizados nos procedimentos de consentimento e ciência do titular dos dados, bem como na necessidade de eventual notificação para demonstrar os procedimentos e medidas que estão sendo adotadas ao cumprimento da LGPD. Caso ocorra um vazamento de dados, a adoção de medidas tempestivas, a informação da sua ocorrência ao titular dos dados e às autoridades governamentais é fundamental, como forma

de amenizar as sanções cabíveis. Tal informação deve conter a natureza dos dados envolvidos no incidente, seus titulares, bem como as medidas adotadas pela empresa para reverter e/ou minimizar os danos provocados pelo incidente.

4. CONCLUSÃO

Diante de todo o exposto, conclui-se que a LGPD tem como princípio fundamental proteger os direitos fundamentais de liberdade e privacidade da pessoa natural, exigindo uma mudança profunda na forma atual de trabalho com os dados de pessoas naturais, compelindo seus detentores a adequar as bases de informações, com a adoção de procedimentos rígidos de controle e gerenciamento dos dados, implementando medidas adicionais de segurança à informação em consonância com princípios da transparência, boa-fé, honestidade, confidencialidade e integridade.

A LGPD E A IMPLANTAÇÃO DA POLÍTICA DE COMPLIANCE COMO MEDIDA DE SEGURANÇA PREVENTIVA AO TRATAMENTO DE DADOS

Por

JULIANA JOPPERT LOPES

Advogada senior manager da área de Consultoria Empresarial do escritório Gaia Silva Gaede Advogados em Curitiba

Mestre em *International Business Law* pela The London College – UCK

Pós-graduada em Gestão Contábil pela Faculdade de Administração e Economia - FAE

Especialista em Direito Empresarial pela Academia Brasileira de Direito Constitucional - ABDCONST

Advogada graduada pelo Centro Universitário Curitiba – UniCuritiba.

JENIFFER MAYUMI MORI

Advogada sênior da área de Consultoria Empresarial do escritório Gaia Silva Gaede Advogados em Curitiba

Pós-graduada em Processo Civil pelo Instituto de Direito Romeu Felipe Bacellar

Especialista em Direito Empresarial Aplicado – LLM pelas Faculdades da Indústria – Sistema FIEP

Advogada graduada pelo Centro Universitário Curitiba – UniCuritiba.

1. INTRODUÇÃO

A Lei nº 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados ("LGPD"), implicará significativa mudança da cultura nacional acerca do tratamento conferido aos dados pessoais.

Esse artigo busca demonstrar um paralelo entre a LGDP e os Programas de *Compliance* decorrentes não apenas das Leis Anticorrupção e de Lavagem de Dinheiro, mas também de uma mudança de cultura exigida mundialmente, tal qual vem se percebendo com a LGPD.

2. RELAÇÃO ENTRE A LGPD E DEMAIS PROGRAMAS DE COMPLIANCE

No caso dos Programas de *Compliance*, tratados hoje como uma exigência, o Brasil viu-se compelido a legislar o assunto ante à assinatura de Tratados Internacionais, como os com a Organização para a Cooperação e Desenvolvimento Económico – OCDE, Organização dos Estados Americanos – OEA e *Convención de las Naciones Unidas Contra la Corrupción* -CNUCC, todos relacionados a um movimento global de combate à corrupção e lavagem de dinheiro.

Empresas multinacionais passaram a negar-se a contratar outras que não aderissem a seus Programas e não tivessem seus próprios. Algo parecido aconteceu em relação à LGPD, que decorre diretamente da necessidade de adequação do País às práticas de proteção de dados adotadas internacionalmente, em especial após a entrada em vigor da *General Data Protection Regulation* ("GDPR"), que nada mais é do que a lei de proteção de dados europeia.

Em vigor desde 25 de maio de 2018, a GDPR foi criada com a intenção de proteger a privacidade dos dados pessoais dos cidadãos europeus, sendo aplicada tanto às empresas localizadas dentro da União Europeia quanto às empresas estrangeiras que processam informações/dados de cidadãos europeus.

Como consequência da evolução tecnológica, com negócios sendo captados e concretizados com base em dados pessoais, esses dados tornaram-se um

verdadeiro ativo com alto valor econômico agregado. Como consequência, houve a crescente prática da comercialização dos dados pessoais, o que despertou a necessidade de edição de leis específicas para proteção dos direitos dos cidadãos, visando garantir o direito à privacidade e proteção de dados pessoais que estavam (e em muitos países ainda estão) sendo utilizados indiscriminadamente.

Com respaldo na Constituição Federal de 1988, a LGPD dispõe sobre o tratamento de dados pessoais e tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme disposto em seu artigo 1º**.**

A LGPD deverá ser aplicada a qualquer operação de tratamento de dados pessoais realizada por pessoa natural ou jurídica, de direito público ou privado, independentemente de sua dimensão, área de atuação, do país de sua sede ou do país onde estejam localizados os dados, desde que: i) a operação de tratamento seja realizada no território nacional; ii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou iii) os dados pessoais objeto do tratamento tenham sido coletados no território nacional, excepcionadas tão somente as hipóteses expressamente previstas na lei.

Note-se, portanto, que a LGPD não fala em nacionalidade, mas sim em territorialidade. Isso significa dizer que não importa se os dados foram coletados no Brasil, pois, se houver o processamento desses dados no país, aplica-se a LGPD. Como consequência, é possível que a um mesmo grupo de dados seja aplicável tanto a LGPD quanto a GDPR, ou ainda outras legislações, e as empresas precisarão estar preparadas para isso.

Certo é que as sanções legais estabelecidas pela LGPD para o descumprimento das obrigações nela previstas tiveram grande impacto perante os empresários, desencadeando preocupação quanto às medidas necessárias para se adequarem às novas exigências, em face do exíguo prazo para uma alteração cultural tão significativa.

A penalidade imposta pode variar de uma simples advertência, com indicação

de prazo para adoção de medidas corretivas a multas e outras sanções, a saber: i) multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração (qualquer infração cometida às normas previstas na lei); ii) multa diária, observado o limite total anteriormente indicado; iii) publicização da infração após devidamente apurada e confirmada a sua ocorrência; e iv) bloqueio ou eliminação dos dados pessoais a que se refere a infração até a sua regularização. Essas multas podem, inclusive, ser cumulativas.

Sempre que uma lei gera impactos de grandes proporções, pergunta-se se sua observância será realmente atingida. Parece-nos que, nesse caso, todos os indícios indicam que sim, pois, embora a LGPD não esteja completamente em vigor, dois grandes casos foram recentemente discutidos utilizando-se o Código de Defesa do Consumidor, mas já com base nos princípios da LGPD, casos estes que destacamos adiante:

"Netshoes"

Como indenização pelos danos morais causados por vazamentos de dados em 2017 e 2018, a Netshoes fez um acordo com o Ministério Público do Distrito Federal, em que pagou multa no valor de R$ 500.000,00 (quinhentos mil reais). Além da multa, a Netshoes teve que reforçar a segurança de sua loja online, bem como ligar para todos os 2 (dois) milhões de clientes afetados pelo vazamento de tais dados. Ainda que o valor da multa esteja significativamente abaixo do máximo previsto na LGPD, é inegável o impacto de tal situação na imagem da empresa, o que certamente gerou prejuízos maiores do que a própria multa.

"**Apple/Google**"

As empresas foram multadas pelo Procon de São Paulo pelo conteúdo dos seus "Termos e Serviços" e "Política de Privacidade", referentes a violações no aplicativo FaceApp (comercializado por essas empresas). O Procon entendeu que ambos continham não apenas uma série de cláusula abusivas, como estavam escritos apenas em língua estrangeira, ferindo o direito básico à informação adequada e clara, o que certamente exige que as informações, no mínimo,

estejam em língua portuguesa.

Percebe-se, então, que a mudança de cultura no que diz respeito à proteção de dados já vem acontecendo e a cobrança em torno das empresas apenas aumentará com a entrada da LGPD em vigor.

Assim sendo, as empresas terão que alterar suas políticas internas para estar em conformidade com o que determina a nova legislação. Em razão disso, vem se fazendo uma comparação entre os Programas de *Compliance* e as necessidades de adequação das empresas à LGPD, havendo muitos comentários no sentido de que as últimas poderão, inclusive, fazer parte dos Programas de *Compliance* das empresas.

Tal comparação baseia-se no fato de que *compliance* vem do verbo inglês "*to comply*", que nada mais é do que "estar em conformidade com uma regra". Nos casos das Leis Anticorrupção e de Lavagem de Dinheiro, determinou-se que as penas atribuídas pela lei poderiam ser reduzidas caso houvesse a implementação de "*mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica*", os quais passaram a compor os chamados Programas de *Compliance*. Embora a LGPD não traga mecanismos de redução de pena decorrentes da existência de comprovação de conformidade, tem se discutido que a elaboração de documentos e mecanismos que respeitem as regras de proteção de dados nada mais é do que uma parte de um Programa de *Compliance*, o qual pode incluir conformidade com regras de diversas legislações distintas.

No caso da LGPD, um dos pontos-chave da lei é a demonstração da finalidade da coleta dos dados, ou seja, as empresas deverão expor de forma clara como serão utilizados os dados pessoais, cabendo ao detentor destes dados a escolha de consentir com essa forma. Esse consentimento passa a ser essencial e passa a ser exigível sempre que houver qualquer mudança na razão original pela qual a empresa solicitou os dados.

Portanto, as empresas precisarão estar preparadas para ter mecanismos que

permitam que o indivíduo[1]:

1) Compreenda a razão pela qual os dados estão sendo solicitados;

2) Entenda de que forma esses dados serão utilizados;

3) Decida quais permissões ele consentirá e quais não (termos gerais não serão mais aceitos, pois o detentor dos dados deve poder escolher as permissões que quiser conceder);

4) Solicite a eliminação dos dados;

5) Tenha acesso aos dados concedidos a qualquer momento.

Portanto, no caso da LGPD, para que haja um plano de adequação visando a mitigação de riscos, será necessário que a empresa busque as respostas para uma série de perguntas como, por exemplo, onde armazenar os dados, como deletá-los, onde serão tratados esses dados, se a plataforma de tecnologia é capaz de proteger as informações confidenciais recebidas, entre outras.

Nota-se que as respostas a essas perguntas não são apenas jurídicas, de modo que é necessária a realização de um diagnóstico completo (que inclua todas as áreas afetadas, inclusive a jurídica), incluindo-se a avaliação dos riscos existentes no dia a dia da condução dos negócios da empresa, verificando as condutas que possam estar em desconformidade com a previsão legal, ou mesmo ensejar qualquer tipo de consequência danosa aos interesses da empresa.

Cumpre destacar que esse *assessment* deverá ser realizado por uma equipe multidisciplinar, composta por profissionais capacitados de diversas áreas, com profundo conhecimento, por exemplo, em tecnologia da informação e recursos humanos. Tal equipe deverá atuar em conjunto com advogados ou escritórios de advocacia que tenham o necessário entendimento dos aspectos legais e contratuais que estão em jogo.

Não sendo possível à empresa compor internamente uma equipe multidisciplinar, é recomendável a contratação de especialistas nas diversas áreas, além da realização de investimentos relacionados à tecnologia da informação,

1 Destaques exemplificativos e não exaustivos.

imprescindíveis para conferir segurança aos dados pessoais que recebem o tratamento.

Será necessário não somente adequar e atualizar os códigos de ética e de conduta e as políticas internas já implementadas nas empresas, mas também implementar novas regras e procedimentos específicos no que se refere a tratamento de dados pessoais e segurança de informação e, via de consequência, realizar novos treinamentos.

Assim, independentemente de as atualizações da LGPD serem realizadas junto com os Programas de *Compliance* das empresas, a política de *compliance* é indissociável das inovações trazidas pela LGPD, na medida em que se faz necessário o monitoramento de dados por comitê constituído de profissionais de diversas áreas, incluindo especialistas na área de tecnologia, que deverão realizar um mapeamento detalhado e permanente acerca de como os dados pessoais são tratados dentro das empresas considerando um ciclo completo, ou seja, desde o momento da coleta, passando pelo armazenamento, com verificação de quem tem acesso e se há possibilidade de compartilhamento (inclusive internacional), até o eventual descarte/destruição.

3. CONCLUSÃO

Ante o exposto, estar em *compliance* com a LGPD significa estabelecer um nível seguro de privacidade, o que, consequentemente, implica em oportunidade para captação de novos negócios pelas empresas, haja vista que as alterações legalmente exigidas impõem um monitoramento contínuo, com elaboração de relatórios de impacto à proteção de dados individuais e riscos existentes, bem como de um plano de ações para as etapas seguintes, tanto para adequações e correções quanto para possíveis alternativas de melhorias.

Os desafios são enormes, e certamente haverá alterações legislativas ao longo do processo de adequação que está sendo experimentado pelas empresas. Em contrapartida, aquelas que primeiramente compreenderem a importância de acrescer às políticas de *compliance* a observância da LGPD, certamente, estarão na vanguarda empresarial da próxima década. Para tanto, Direito e Tecnologia deverão ser cuidadosamente alinhados e aplicados.

DATA MAPPING E *RISK ASSESSMENT* – MAPEAMENTO DE RISCOS PARA A LGPD

Por

VANESSA CRISTINA SANTIAGO GIUGLIANO
Sócia da área de Direito Societário do Gaia Silva Gaede Advogados em São Paulo
Mestranda em Direito dos Negócios pela Fundação Getúlio Vargas – FGV/SP
Especialista em Direito Societário pela Fundação Getúlio Vargas – FGV/SP
Pós-graduada em Processo Civil pela Pontifícia Universidade Católica de São Paulo – PUC/SP
Graduada em Direito pela Pontifícia Universidade Católica de São Paulo – PUC/SP.

MARINA MARTINEZ PRAZERES SANT' ANNA
Advogada sênior na área de Direito Corporativo do Gaia Silva Gaede Advogados em São Paulo
Pós-graduada em Direito Empresarial pelo Instituto de Ensino e Pesquisa – INSPER
Graduada em Direito pelo IBMEC-Damásio.

1. INTRODUÇÃO

A LGPD (Lei Geral de Proteção de Dados) foi sancionada em agosto do ano de 2018 e entrará em vigor em 2021. Considerando a iminente vigência da Lei e seu consequente *enforcement*, é necessário que os *players* do mercado que manipulam os dados pessoais, tutelados pela Lei, iniciem os preparativos para a implementação de políticas consistentes para adequação à LGPD.

Posto isso, o presente artigo tem como finalidade elucidar de forma prática quais são as principais diretrizes de mapeamento de dados ("*data mapping*") que devem ser observadas para início da efetivação da proteção esmerada na LGPD.

Para tanto, é necessário pressupor o domínio básico dos conceitos chave trazidos pela nova Lei, entre eles: dados pessoais e sensíveis; tratamento de dados; fins comerciais; controlador; e operador.

2. LEVANTAMENTO DE DADOS E FUNÇÃO DO *DATA MAPPING*

Uma vez que os conceitos básicos estejam claros para os potenciais controladores e operadores de tratamento de dados, é essencial levantar quais são os dados que transitam ou podem transitar na rede do controlador, o tempo de "vida" desses dados, sua destinação, bem como se tal "trânsito" pode ser enquadrado nas hipóteses da Lei. Para fins deste artigo, tal enquadramento será tratado como "Moldura Legal".

Um dos principais objetivos do levantamento **é justamente a análise de riscos** envolvidos ("*risk assessment*") no processamento e tratamento dos dados coletados direta ou indiretamente e seu enquadramento na Moldura Legal. Apenas quando a equação "levantamento de dados e análise de riscos" estiver completa, é que será viável proceder ao *data mapping.*

Levantamento de dados + análise de riscos = *data mapping*

Quando bem desenhado, o *data mapping* servirá de alicerce para a estruturação, implementação e execução de um programa de governança em proteção de dados.

Notadamente, quando esse pilar for consistente, será possível direcionar o programa de uma maneira eficaz para priorizar os principais gatilhos de coleta e tratamento de dados, bem como promover a implantação gradativa e em *compliance* com a Lei em questão.

3. QUESTIONAMENTOS NECESSÁRIOS PARA O *DATA MAPPING*

Aos controladores e operadores dos dados protegidos pela LGPD, é primordial a análise de cabimento de algumas possibilidades detectadas na rotina da sociedade à Moldura Legal. Uma das maneiras de aferir essas possibilidades é a realização de questionamentos pontuais sobre os dados pessoais que serão coletados pela empresa controladora ou operadora.

A realização do questionário pontual, pautado na Moldura Legal, permite à controladora/operadora obter um panorama sobre a aplicação ou não da LGPD em determinados casos. Alguns questionamentos importantes a serem realizados, segundo nossa prática, são:

- ✓ Quais dados o controlador/operador coletará?
- ✓ Qual será a finalidade dessa coleta? Ela é necessária?
- ✓ O tratamento será feito de forma adequada?
- ✓ Qual é o embasamento, segundo a LGPD, para o processamento desses dados?
- ✓ Como os dados serão armazenados? Por quanto tempo?
- ✓ Quem poderá acessar esses dados?
- ✓ Os dados estarão seguros?

- ✓ Os dados serão compartilhados?
- ✓ Como será feito o registro do processamento dos dados?
- ✓ Como seria o tratamento e registro em caso de vazamentos de dados?
- ✓ Como lidar com as solicitações dos titulares?

4. IMPLEMENTAÇÃO DA LGPD A PARTIR DO *DATA MAPPING* E *RISK ASSESSMENT*

Com todos os questionamentos acima feitos e respondidos, é hora de desenhar o plano de ação para a constituição e manutenção do programa de governança em proteção de dados internamente. Para efeito de exemplificação, consideraremos a adequação da LGPD em um ambiente empresarial complexo, isto é, com diversos *stakeholders* participando da coleta e tratamento de dados pessoais de colaboradores e terceiros.

4.1. Mapeamento e avaliação

Primeiramente, como já dissemos, é necessário mapear e avaliar os riscos envolvidos na manipulação de dados (*data mapping*).

No caso de uma empresa, seja de qual segmento for, é necessário que o mapeamento e a avaliação sejam feitos pelas principais áreas que possam se tornar gatilhos de manuseio de dados, como, por exemplo: **Departamento Jurídico, Informática, Recursos Humanos** e **Comercial**.

4.2. Elaboração de políticas e plano de ação

Após o mapeamento e avaliação, incluindo o enfrentamento do questionário sugerido acima, **já é possível construir uma política dirigida especificamente para as necessidades da empresa, abrangendo, inclusive, as peculiaridades de cada segmento** em consonância com a Moldura Legal.

Nessa oportunidade, é recomendando o envolvimento de pelo menos três macro áreas da empresa: **Departamento Jurídico, Informática** e **Recursos Humanos**.

O Departamento Jurídico ou a Assessoria Jurídica será responsável pela elaboração do programa de *compliance* em LGPD, enquanto as demais áreas fornecerão as diretrizes técnicas para indicação de potenciais desdobramentos da política que refletirão em suas respectivas esferas, bem como auxiliarão na criação e execução do plano de ação.

4.3. Conscientização e Treinamentos

Pilar de toda e qualquer política interna, os treinamentos periódicos com a finalidade de conscientizar funcionários e terceiros ligados à empresa são fundamentais para que se possa alcançar um patamar aceitável de conformidade com a LGPD. Importante salientar que é altamente recomendado que esses treinamentos sejam registrados, e transmitidos com recorrência e reciclagem, como forma de sempre manter todos os colaboradores atualizados e conscientes da política corporativa de proteção de dados. Nesse caso, a recorrência de treinamentos deve também ser parte integrante do plano de ação.

Novamente, o **Departamento Jurídico (e/ou Assessoria Jurídica) e Recursos Humanos** serão os protagonistas nessa fase de implementação. A instrumentária jurídica servirá de suporte técnico para propagar a informação e interpretação da norma aos colaboradores, enquanto o Departamento de Recursos Humanos ficará encarregado de disponibilizar as ferramentas e replicadores de treinamento para a aplicação e capacitação dos funcionários.

4.4. Gerenciamento de dados

A coleta e tratamento de dados deve ser uma atribuição restrita dentro do ambiente corporativo. É crucial que todos os procedimentos previstos na Lei sejam estritamente observados nesse estágio.

Nesse ponto, poucos stakeholders devem ter a permissão e alcance para gerenciar os dados que trafegam na rede da empresa, sejam o tráfego físico ou o virtual de informações. Assim, usualmente, apenas o **Departamento de Informática e o Departamento Comercial**, quando esse utiliza os dados com fins comerciais, deverão ser as instâncias acionadas nessa etapa.

4.5. Gerenciamento de consentimento e do ciclo de vida dos dados

Tendo uma política de coleta e tratamento de dados já em funcionamento, é elementar manter mecanismos de gerenciamento do consentimento dos titulares das informações e do ciclo de vida dos dados, ou seja, por quanto tempo esses dois fatores permanecem válidos, vigentes e legítimos. Os critérios desse consentimento devem ser levantados quando do estabelecimento da Moldura Legal, a qual, ao menos nesse aspecto, deve ser revisitada de tempos em tempos, vez que as autoridades podem instituir/alterar práticas específicas para determinados mercados.

Todas as áreas que por alguma razão coletaram, trataram, auxiliaram ou participaram de alguma dessas atividades devem estar envolvidas no monitoramento e gerenciamento do consentimento e ciclo de vida dos dados. Assim, é preciso criar mecanismos sistêmicos que possam abranger todas as áreas para que não haja lapsos no gerenciamento. O monitoramento correto e acurado desses critérios garantirá a continuidade, a eficácia e a perpetuidade do programa de governança em proteção de dados.

4.6. Outras medidas necessárias

Após todas as principais diretrizes da LGPD serem devidamente priorizadas, sanadas e postas em prática, é chegado o momento de implementar outros mecanismos para a conservação e preservação do programa. Importante considerar que o programa de LGPD é absolutamente ineficaz quando se torna desatualizado, obsoleto e sem desenvolvimento contínuo.

Portanto, cada uma das macro áreas deverão ser investidas de atribuições para a subsistência do programa, como, por exemplo:

Departamento Jurídico: revisão do minutário contratual e inserção de cláusulas em contratos já vigentes que assegurem de forma globalizada a observância das disposições contidas na LGPD;

Departamento de Informática: Atuação com ênfase no monitoramento, reporte e gestão de incidentes, bem como implantação de medidas e recursos de segurança da informação;

Departamento de Recursos Humanos: prosseguimento na conscientização e treinamentos sobre o tema aos funcionários, mantendo o programa sempre atualizado e disponível aos seus colaboradores;

Departamento Comercial: quando for o responsável por compartilhar os dados para fins comerciais, o departamento deve também implementar diligências que garantam a segurança das informações e destinação adequada dos dados.

5. CONCLUSÕES

Diante do exposto, concluímos que **é essencial que a fundação de um programa de governança em proteção de dados seja tão consistente quanto sua execução.** Isso porque, o mapeamento e a análise de risco feita previamente à instalação do programa direcionará todos os passos seguintes para a implantação da política, incluindo, mas não se limitando, às atribuições de cada *stakeholder* dentro da empresa.

LEI GERAL DE PROTEÇÃO DE DADOS E O DIREITO DO TRABALHO

Por

MARIA BEATRIZ RIBEIRO DIAS TILKIAN

Advogada senior manager do Gaia Silva Gaede Advogados em São Paulo

Bacharel, Especialista e Mestre em Direito do Trabalho pela Pontifícia Universidade Católica de São Paulo

Especialista em Direito Previdenciário pela Escola Paulista de Direito.

1. INTRODUÇÃO

A Lei nº 13.709, publicada em 15 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados ("LGPD"), é um marco para o tratamento de dados pessoais no Brasil, inclusive nos meios digitais, ao introduzir procedimentos para que o cidadão possa ter informação sobre o modo como seus dados pessoais são organizados, armazenados ou transferidos e sobre eventuais punições a condutas inadequadas.

Para análise dos reflexos da LGPD nas relações de emprego, necessária a compreensão dos termos adotados pela lei e sua extensão, já que não aborda especificamente dos efeitos da lei no Direito do Trabalho e trata da mesma maneira microempreendedor e multinacionais.

É o que será visto no presente artigo.

2. A LGPD E O DIREITO DO TRABALHO

O artigo 1º da LGPD define o objeto da lei: "tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

O dado pessoal objeto de tratamento e proteção da lei é a informação relacionada a pessoa natural identificada ou identificável (artigo 5º, I).

O tratamento é entendido como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração", por meios digitais ou não (artigo 5º, X).

A LGPD tem sua aplicação ao país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional (são os dados pessoais cujo titular nele se encontre no momento da coleta) (artigo 3º).

A lei exclui do seu alcance o tratamento: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (artigo 4º).

Com a nova lei, o manuseio do dado pessoal, por pessoa natural ou por pessoa jurídica (de direito público ou privado), por meios digitais ou não, deve observar as regras postas para garantir a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (artigo 1º).

Isto é reforçado pelo artigo 2º da LGPD, que expressamente enumera como seus fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Ao ter como finalidade a garantia de proteção dos direitos fundamentais de liberdade e de privacidade, além do livre desenvolvimento da personalidade da pessoa natural, a LGPD dá status de proteção constitucional às regras estipuladas, já que tais garantias são expressamente mencionadas no artigo 5º, *caput* e inciso X, da Constituição Federal:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Como norma máxima do nosso ordenamento jurídico, a Constituição Federal deve ser amplamente respeitada e interpretada de maneira a conferir maior eficácia aos direitos fundamentais nela previstos e, entre eles, os mencionados na LGPD.

Este viés regerá eventuais conflitos na intepretação e aplicação da LGPD e este aspecto se aproxima dos princípios de proteção conferidos pelo Direito do Trabalho ao empregado.

Além disso, em análise dos conceitos adotados pela LGPD percebe-se, com clareza, que a relação de emprego e a troca de informações entre empregado e empregador é diretamente atingida por suas regras e diretrizes.

O próprio conceito de empregado – toda pessoa física que presta serviços de natureza não eventual a empregador, sob a dependência deste e mediante salário (artigo 3º, CLT) – coloca o trabalhador como alvo de proteção da LGPD, que escolheu resguardar o dado pessoal (toda informação da pessoal natural).

Da mesma maneira, o conceito de empregador - empresa, individual ou coletiva, que, assumindo os riscos da atividade econômica, admite, assalaria e dirige a prestação pessoal de serviço (artigo 2º, CLT) - mistura-se com os papéis dos agentes de tratamento: (i) o controlador: pessoa natural ou jurídica, de direito

público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais ou (ii) o operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Assim, pela natureza da relação de emprego e das partes envolvidas (uma pessoa física, na qualidade de empregado, e uma pessoa física ou jurídica, na qualidade de empregador), as previsões da LGPD devem ser cuidadosamente analisadas e aplicadas especialmente pelos departamentos pessoais e de recursos humanos, que estão em contato diário com informações, muitas delas sensíveis, decorrentes da relação de emprego.

Neste aspecto, importante mencionar que a LGPD define expressamente o que é o dado pessoal sensível, considerado aquele sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual e dado genético ou biométrico, quando vinculado a uma pessoa natural. Tais dados merecem tratamento com redobrado cuidado, tendo sido objeto de regulamentação por um conjunto de artigos específicos, que determinam maior rigidez das regras de proteção de tais informações (artigo 5º, II e artigos 11 a 13).

Estas informações a todo tempo são fornecidas ao empregador: desde o recebimento de um currículo ou preenchimento de questionário para aplicação para uma vaga de trabalho, passando pelos documentos decorrentes do contrato de trabalho, como holerites ou atestados médicos, informações pessoais para plano de saúde, dados familiares, formulários sobre o perfil técnico do profissional debatido em políticas de avaliação e *feedback* ou de performance profissional, pesquisas internas sobre clima organizacional ou o conteúdo de denúncias trazidas pelos canais de ouvidoria, além de informações sobre o motivo do desligamento nas hipótese de rescisão contratual ou valores recebidos.

Neste novo cenário, as empresas precisarão ter o consentimento para coleta e tratamento de dados pessoais ou informar que os dados estão sendo obtidos para cumprimento de obrigações legais (como, por exemplo, as informações necessárias para cumprimento das declarações ao E-Social).

Isto porque o artigo 7º, da LGPD autoriza o tratamento de dados pessoais somente nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A organização das informações também é importante porque a LGPD assegura ao trabalhador a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei (artigo 18).

O descumprimento da LGPD poderá acarretar sanções administrativas, tais como a aplicação de advertência, com indicação de prazo para adoção de medidas corretivas, multa de até 2% do faturamento, bloqueio dos dados pessoais relativo à infração até sua regularização e eliminação dos dados a que se refere a infração (artigo 52), além da responsabilidade por eventuais danos patrimonial, moral, individual ou coletivo, causado pelo agente de tratamento (empregador) a outrem (empregado).

Para aplicação das sanções, após procedimento administrativo que possibilite a oportunidade da ampla defesa, serão observados os seguintes critérios: I - a gravidade e a natureza das infrações e dos direitos pessoais afetados; II - a boa-fé do infrator; III - a vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - a reincidência; VI - o grau do dano; VII - a cooperação do infrator; VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas; e XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção (artigo 52, §1º).

Neste aspecto, 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. Também é solidária a responsabilidade dos controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados (artigo 42).

Importante lembrar que a responsabilidade pelos eventuais danos causados pelo empregador já era tratada pelo Código Civil, cujos artigos 186 e 927 preveem a responsabilidade pela reparação moral ou patrimonial de eventual ato ilícito praticado. Além disso, os artigos 932, III, e 933 do mencionado Código listam a responsabilidade objetiva do empregador pelos atos praticados por seus empregados ou prepostos, o que determina o dever de reparar independentemente de culpa.

De todo modo, a LGPD, por ser mais específica, exclui a responsabilidade dos

agentes de tratamento 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 (artigo 43).

Diante destas novas diretrizes, para observância da LGPD será necessária a reorganização interna das empresas para mapeamento dos dados que envolvem todas as fases da contratação, incluindo a fase pré-contratual, a revisão de práticas de segurança, de políticas internas, de códigos de ética, de contratos e aditivos contratuais.

Assim, será essencial o mapeamento das informações que sejam relacionadas a empregados, a identificação das informações que precisam ou não do consentimento; a indicação do tipo de tratamento necessário para cada dado (se apenas são armazenados ou se serão transferidos, por exemplo) e a revisão das rotinas para o tratamento adequado das informações.

O mapeamento das informações também é necessário para a verificação do seu nível de sensibilidade e consequente organização da sua forma de tratamento, de modo a buscar o devido consentimento do candidato ao emprego ou do empregado com relação aos dados obtidos pela empresa ou indicar que os dados estão sendo coletados para cumprimento de obrigações legais.

Outro cuidado que as empresas devem tomar se refere ao fornecimento de treinamento, especialmente aos departamentos jurídico e de recursos humanos para conscientização e fiscalização dos procedimentos adotados para observância da LGPD e consequente segurança e sigilo dos dados, já que a responsabilidade por ressarcimento de dados pode ser atribuída ao controlador ou operador de dados.

Neste aspecto surge a necessidade de indicação do encarregado: a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados. Analisar o formato da contratação deste profissional, sua função e atividades é essencial para adequação da empresa à LGPD, que deve ter a iden-

tidade e as informações de contato divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

Cabe ao encarregado, pela definição da lei: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (artigo 41) e, pela natureza de suas atividades, pode ser um empregado ou não.

Além da relação direta de emprego, a relação com prestadores de serviços também está alcançada pela LGPD. Fará parte do processo de seleção a análise da adequação da empresa prestadora de serviço à LGPD, dando-se preferência àquelas confiáveis quanto ao tratamento adequado dos dados, diante da responsabilidade que pode ser atribuída à empresa contratante pelo tratamento inadequado de dados dos fornecedores, empregados ou profissionais terceirizados.

3. CONCLUSÃO

A LGPD traz profunda alteração da forma de organização das empresas e no relacionamento com os dados pessoais e inicia corrida contra o tempo para ajuste às suas diretrizes. A adequação das empresas à LGPD será um diferencial para a realização de negócios, especialmente com os países que já possuem regulamentação semelhante, como aqueles da comunidade europeia.

LGPD: UM RECUO QUANTO À TENDÊNCIA GLOBAL DE FLEXIBILIZAÇÃO DOS SIGILOS BANCÁRIO E FISCAL DOS CONTRIBUINTES?

Por

JORGE LUIZ DE BRITO JUNIOR

Advogado senior manager de Contencioso Tributário do Gaia Silva Gaede Advogados em São Paulo

Mestre em Direito Econômico Financeiro e Tributário pela Universidade de São Paulo - USP

Especialista em Direito Internacional Tributário pelo IBDT

Bacharel em Direito pela Universidade Presbiteriana Mackenzie.

1. INTRODUÇÃO

As inovações tecnológicas vêm impactando a esfera da privacidade ao longo da história. Em Direito, as primeiras discussões sobre a existência de um Direito à Privacidade remontam à virada do século XIX para o século XX, época em que os Estados Unidos haviam conhecido um processo de industrialização intensificado, sobretudo, após a guerra de secessão, com a subsequente reconstrução do país durante as décadas de 1870 e 1890 – época conhecida como *The Gilded Age* (a era dourada)[1].

É dessa época que data o célebre texto do Juiz Louis Brandeis e de Samuel Warren*, The Right to Privacy*, considerado um dos mais percucientes ensaios da história do Direito norte-americano. O texto enfrenta as perplexidades de então quanto ao surgimento de novas tecnologias e comportamentos, como as câmeras fotográficas e o jornalismo de celebridades então insurgente, e suas repercussões para a esfera da privacidade. Os autores concluem que, à semelhança dos direitos personalíssimos reconhecidos aos autores de obras literárias e artísticas, como uma manifestação de sua personalidade, a *Common Law* reconhece, de fato, um Direito à privacidade como decorrência lógica daqueles mesmos direitos. O raciocínio é que, se aos autores é reconhecido um direito personalíssimo sobre a criação, expressão de seu intelecto materializada em uma publicação, não se pode negar a existência de um direito absoluto do ser humano a deter o controle do que pode ou não ser tornado público a seu respeito.

Na mesma época, as discussões sobre a proteção de dados que tornam possíveis a identificação de uma pessoa se iniciam em razão de um censo promovido pelo governo norte-americano, tendo-se concluído, à época, que a publicação dos dados pessoais era pertinente por razões de logística, uma vez que tornaria possível aos indivíduos pesquisados zelar pela correção das informações tornadas públicas, contribuindo para a eficácia do censo.

Em pleno século XXI, diante dos fenômenos do *big data,* da inteligência artificial

1 O termo foi ironicamente cunhado por MARK TWAIN e CHARLES DUDLEY WARNER, na obra *The Gilded Age: A Tale of Today*, na qual satirizaram o que acreditavam ser uma sociedade marcada por vários problemas, escondidos por uma "camada fina de ouro".

e da multiplicação exponencial da quantidade de informações disponíveis sobre os indivíduos, retomam-se os debates sobre a preservação de uma necessária esfera de intimidade e privacidade – o que, possivelmente, se dê em parte devido ao medo, presente no inconsciente coletivo, de que possamos chegar à distopia idealizada por autores como George Orwell no clássico *1984*.

É nesse contexto que, no âmbito Europeu, se dá a introdução da GDPR, que vem, na verdade, consolidar uma série de direitos que, em grande parte, já haviam sido reconhecidos pelo ordenamento jurídico da União Europeia com base em Acordos celebrados em seu âmbito, bem como em decisões proferidas pelas Cortes europeias.

A Lei Geral de Proteção de Dados brasileira, que não apenas foi inspirada na legislação europeia como editada em caráter de urgência para atender à demanda de empresas brasileiras operando no mercado europeu, consagra direitos e garantias semelhantes.

No presente artigo, discutiremos os impactos da Lei nº 13.709/2018 (LGPD), especificamente, no que se refere às relações entre os cidadãos e as autoridades fiscais, incluindo a troca nacional e internacional de dados de contribuintes, a criação de listas de devedores *(shame lists)* e o uso de informações publicadas em redes sociais como fonte para a fiscalização.

2. TROCAS INTERNACIONAIS DE DADOS E FLEXIBILIZAÇÃO DOS SIGILOS BANCÁRIO E FISCAL DOS CONTRIBUINTES

No âmbito internacional, as trocas de dados de contribuintes entre jurisdições não são novidade, remontando ao acordo celebrado entre França e Bélgica em 1843 – primeiro tratado internacional da era moderna em que se mencionou expressamente a colaboração e troca de dados entre países em matéria fiscal.

A Convenção Modelo da OCDE, desde sua primeira edição em 1963, sempre incluiu dispositivo que versa sobre troca de informações entre contribuintes.

Contudo, houve uma mudança importante de paradigma em 2010, com o advento da legislação norte-americana denominada FATCA (*Foreign Accounts Tax Compliance Act).* O FATCA exige que instituições financeiras em nível global forneçam, ao *Internal Revenue Service* – o equivalente à Receita Federal nos EUA –, informações sobre seus correntistas norte-americanos, sob a coerção de impor pesada retenção na fonte sobre todos os pagamentos realizados de fontes norte-americanas com destino a essas instituições financeiras, caso não se tornem *compliants* com o FATCA.

A legislação norte-americana possui o objetivo declarado de prevenir crimes de lavagem de dinheiro, bem como permitir o combate à evasão fiscal, tendo em vista a caraterística peculiar dos EUA de tributar seus cidadãos em bases universais, combinada com a característica peculiar de definir a cidadania com base no critério *jus soli* (ou seja, torna-se cidadão estadunidense quem nasce no território dos EUA).

Na esteira do FATCA, os EUA negociaram uma série de tratados internacionais com vários países versando sobre intercâmbio de informações (inclusive com o Brasil), o que, na mesa de negociações envolvendo o FATCA, serve como uma promessa de contrapartida para os demais países. Ou seja, os países concordam em aderir ao FATCA e, como troca, por meio de celebração de acordos de trocas de informações, passaram, em teoria, a ter acesso a informações detidas pela autoridade fiscal dos EUA.

Logo, a partir do FATCA, a mudança de paradigma que ocorreu foi a transição de um sistema de trocas internacionais bilaterais, pontuais e sob requisição, para um sistema multilateral e automático de troca de informações fiscais de indivíduos entre jurisdições.

A despeito de reações adversas ao FATCA por parte dos cidadãos e do parlamento europeu, a OCDE, formada predominantemente por países europeus, gostou, por assim dizer, da eficácia fiscal de tais trocas de informações, tendo introduzido uma política semelhante como parte da Ação 13 do plano de combate à erosão de base fiscal (o BEPS).

A OCDE introduziu um *Country-by-Country* report (CBC), que obriga as em-

presas transnacionais que atuam dentro de seu âmbito a fornecer informações sobre suas operações e alocação de lucros entre jurisdições. Semelhantemente ao FATCA, a OCDE propôs, como moeda de troca para que os países possam usufruir dessa base de dados, a celebração de acordos de troca de informações fiscais em nível multilateral.

Com o advento do FATCA e o plano BEPS, há uma intensa troca multilateral de informações sobre contribuintes entre países, levando à crescente preocupação quanto à segurança e proteção às regras de sigilo e privacidade.

As principais preocupações derivam dos seguintes fatores: (i) a multilateralização torna cada vez mais difícil assegurar que a jurisdição receptora dos dados transferidos possui regras para assegurar a proteção dos dados, ou mesmo estrutura de TI suficiente para assegurar tal proteção; (ii) há o tráfego de dados sensíveis entre várias jurisdições, que poderiam acabar sendo compartilhados com regimes ditatoriais; e (iii) falta de transparência, em violação às garantias do Devido Processo Legal e do Direito a um Julgamento Justo[1], reconhecidas no âmbito da União Europeia antes mesmo da GDPR.

3. TROCAS DE DADOS FISCAIS NO ÂMBITO DO DIREITO BRASILEIRO

O quadro anteriormente citado aponta para uma tendência de privilegiar o compartilhamento de dados fiscais entre jurisdições em detrimento de garantias individuais, como os sigilos bancário e fiscal.

No âmbito nacional, verifica-se tendência semelhante desde a reforma promovida pela Lei Complementar nº 104/01, que, além de prever que as instituições financeiras deverão informar à Administração Tributária as operações financeiras efetuadas pelos usuários de seus serviços, instituiu a possibilidade de prestação de assistência mútua entre as Fazendas Públicas da União, Estados e Municípios, para permuta de informações (art. 199 do CTN).

Atualmente, no que se refere aos dados pessoais (foco da LGPD, que não se

1 European Convention of Human Rights (ECHR), Article 6th

aplica a dados de Pessoas Jurídicas), a RFB possui um enorme influxo de dados dos Contribuintes, incluindo os dados do Sistema da Nota-Fiscal eletrônica e outras obrigações acessórias, tais como Declaração de Operações liquidadas em Moeda (DME, instituída pela IN RFB 1761/17), informações prestadas pelos fundos de investimento institucionais quanto aos seus investidores (*e-financeira,* instituída pela IN RFB 1.571/15), operações efetuadas com cartão de crédito (DECRED, instituída pela IN RFB 341/03), operações realizadas com imóveis (DIMOB, instituída pela IN RFB 1.115/10) e – mais recentemente – operações realizadas com criptomoedas (IN RFB 1.888/19).

Com fundamento no art. 199 do CTN e na Solução de Consulta Interna COSIT nº 2/2018, permitiu-se a celebração de convênios entre os entes da federação para intercâmbio dessas informações, convênios esses que, como já mencionado, satisfazem a garantia de reserva legal prevista na LGPD.

4. DIREITOS RECONHECIDOS AOS CONTRIBUINTES EM FACE DAS TROCAS DE DADOS ENTRE JURISDIÇÕES SOB A GDPR/LGPD

O consentimento para o tratamento de dados é um elemento fundamental da LGPD (art. 7º, I). Contudo, o tratamento, inclusive compartilhamento, de dados pela administração púbica para execução de políticas públicas previstas em leis e regulamentos, ou respaldadas em contratos, convênios ou instrumentos congêneres (art, 7º, III), consiste em caso específico de aplicação, não se sujeitando, portanto, ao consentimento prévio.

Esse dispositivo (art. 7º, III) representa, de partida, não uma cláusula de isenção da administração pública às disposições da LGPD, mas uma garantia de reserva legal, sendo que o termo "lei" nesse caso deve ser tomado em seu sentido mais lato, para abarcar, também, os acordos internacionais celebrados pelo Brasil com outras nações, desde que, naturalmente, atendidos os pressupostos formais (aprovação parlamentar, ratificação e troca de instrumentos).

Em se tratando de tratamento de dados pela administração pública (art. 7º,

III), a LGPD remete a capítulo específico que regulamenta esse tratamento (Capítulo IV).

Ainda que não aplicável o consentimento, há que se ter em mente o Princípio da Autodeterminação informativa, que aparece positivado no art. 2º, II, da LGPD, cujas implicações são mais profundas do que a própria exigência de consentimento, abrangendo o direito dos indivíduos de, em última análise, tomar conhecimento e controlar o uso dos seus dados, podendo intervir para evitar abusos e corrigir incorreções.

Derivam desse princípio maior duas ordens de garantias que deverão ser observadas pela Administração Pública no tratamento de dados dos jurisdicionados, quais sejam: o Direito à Privacidade e o Direito a ser Ouvido. Ambos os direitos já foram consagrados no âmbito da União Europeia, derivando de documentos como a Convenção Europeia de Direitos Humanos, a Carta Fundamental de Direitos da União Europeia e o próprio Tratado para Funcionamento da União Europeia.

Do Direito à Privacidade, por sua vez, derivam as regras que impõem, à administração pública, o dever de zelar pela observância das regras de sigilo vigentes, incluindo a exigência de padrões técnicos e administrativos mínimos capazes de assegurar a segurança e proteção dos dados pessoais, resguardando-os de acessos não autorizados, bem como medidas de prevenção (art. 6º, VII e VIII), assegurada a responsabilização e prestação de contas, ficando o agente público obrigado a adotar medidas capazes de comprovar a observância e o cumprimento de tais normas (art. 6º, X).

Ainda como decorrência lógica do Direito à Privacidade, tem-se a necessidade de observância da regra de Proporcionalidade pela administração, que envolve, de um lado, a total adstrição da Administração Pública à finalidade do uso dos dados, tal como expressamente positivado nos arts. 23 e 26, *caput,* da LGPD, e, de outro, o limite do uso dos dados àquele estritamente necessário para atingimento da finalidade legalmente prevista.

Como decorrência do Direito a ser Ouvido, tem-se o Direito dos contribuintes de terem pleno conhecimento quanto ao uso de seus dados e, inclusive, de serem informados com clareza sobre o fundamento legal e finalidade que justificam tal

uso (cf. art. 23, I, e 25). Por outro lado, também deriva desse Direito a garantia ao devido processo legal, incluindo o Direito de Petição e o Direito à correção de dados constantes dos cadastros das Autoridades públicas.

Na LGPD, esses direitos restam resguardados pela remissão expressa, feita pelo art. 23, § 3º, à Lei do *Habeas Data* (9.507/97), à Lei Geral do Processo Administrativo (Lei nº 9.784/99) e à Lei de Acesso à Informação (Lei nº 12.527/2011).

Todos os direitos acima referidos já foram discutidos e reconhecidos no âmbito da União Europeia desde antes do GDPR e, em nosso entendimento, encontram-se positivados na LGPD brasileira. Tais direitos dos indivíduos são oponíveis à troca de dados entre jurisdições, inclusive no plano doméstico.

No âmbito internacional, há, inclusive, um caso recente em que uma contribuinte, cidadã do Reino Unido, ajuizou ação contra a HMRC (*Her Majesty Revenue and Customs)* – o equivalente à Receita Federal no Reino Unido – para impedir o compartilhamento de seus dados com a autoridade fiscal dos EUA no âmbito do FATCA.

Em sua ação, a Contribuinte sustenta a violação à GDPR, inclusive, em razão da violação à proporcionalidade, pois a autora da ação sustenta que seus rendimentos estão dentro da faixa de isenção fiscal prevista pela legislação dos EUA, não se justificando a intrusão imposta pelo FATCA. O processo judicial movido por essa Contribuinte foi custeado por um *crowdfunding,* havendo grande mobilização de grupos contrários ao FATCA, em especial por uma associação de *acidental americans*[2].

5. COMPARTILHAMENTO DE DADOS PESSOAIS PELA ADMINISTRAÇÃO A ENTIDADES PRIVADAS

A LGPD veda, como via de regra, o compartilhamento de dados pessoais pela Administração Pública com entidades privadas, ressalvadas as hipóteses, previstas no art. 26, §1º, de (i) execução descentralizada de atividade pública que exija a transferência, (ii) casos em que os dados forem acessíveis

2 Termo que designa pessoas que nasceram circunstancialmente nos EUA, mas que, por vezes, embora jamais tenham chegado a viver no país, ficaram passíveis de tributação nos Estados Unidos.

publicamente, desde que observadas as demais disposições da Lei, (iii) quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres, ou (iv) para a prevenção de fraudes e irregularidades ou para proteger e resguardar a segurança e a integridade do titular dos dados, vedado o tratamento para outras finalidades.

Em matéria de acordos e convênios para transferência de dados pessoais por entes da Administração Pública a entidades privadas, há previsão expressa de que tais acordos devem ser previamente comunicados à Autoridade Nacional (art. 26, §2º).

É importante notar que, ainda que diante de convênios celebrados por entes da administração pública para compartilhamento de dados pessoais com entidades privadas, tais acordos devem observar, estritamente, a finalidade. Isso implica não apenas que a finalidade pela qual o compartilhamento está sendo realizado deve ser preservada, como, também, que tal finalidade deve estar prevista em lei (em sentido lato) ou, no mínimo, resguardada pela LGPD. Implica, ainda, que o compartilhamento deve estar em linha com a finalidade institucional do ente da administração pública em questão.

Vale ressalvar, nesse aspecto, que a LGDP também inclui, entre as hipóteses de tratamento de dados pessoais que não dependem de consentimento, a proteção ao crédito. Isso significa que a finalidade de proteção ao crédito se coaduna, em princípio, com o compartilhamento de dados pela Administração Pública. Dito de outro modo, não é proibido, como via de regra, o compartilhamento de dados pessoais por entes da Administração Pública com empresas privadas, tais como a SERASA, com a finalidade de proteção ao crédito.

Entretanto, deve-se examinar se tal compartilhamento se coaduna com a missão institucional do ente da administração pública em si. Questiona-se, por exemplo, a possibilidade de um Acordo de Cooperação Técnica entre o Tribunal Superior Eleitoral (TSE) e a SERASA (Acordo de Cooperação Técnica 07/2013). A finalidade de proteção ao crédito estaria em linha com a missão institucional do TSE – garantir a legitimidade do processo eleitoral e a efetiva prestação jurisdicional? Entendemos que esse acordo de compartilhamento seria questionável sob a perspectiva da LGPD.

6. USO DE DADOS DISPONÍVEIS EM REDES SOCIAIS COMO FONTE PELA FISCALIZAÇÃO

A cláusula na Constituição Federal que prevê o Princípio da Capacidade Contributiva resguarda a prerrogativa da Administração Tributária de, visando à efetividade do Princípio, identificar o patrimônio, os rendimentos e as atividades econômicas do contribuinte, *respeitados os direitos individuais e nos termos da lei.*

Não há dúvidas de que a LGPD representa, portanto, um limite à prerrogativa fiscal de investigar a capacidade contributiva dos jurisdicionados.

Nesse aspecto, uma vez que o Contribuinte disponibilize, em suas redes sociais, informações que denotem indícios de riqueza, a questão que se apresenta é: essas informações são públicas? Esse dado dependerá da política de privacidade de dados à qual aderiu o Contribuinte quando criou a conta na rede social. Ainda que se admita que as informações são públicas, nota-se que o fato de o dado ter sido tornado público, voluntariamente, pelo próprio titular ainda condiciona o seu tratamento, que deve considerar *"a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização"* (art. 7º, §3º).

Não há dúvidas de que, ao ostentar sinais de riqueza em redes sociais, o Contribuinte não o faz com o propósito de transmitir ao Fisco informações sobre sua situação financeira. Pode ser, inclusive, que tais manifestações em rede sociais não sejam sequer a melhor representação de tal situação, podendo tal exteriorização ter sido realizada com as mais diversas motivações.

Entendemos, portanto, que os mais diversos entes da Fiscalização não podem contrapor informações publicadas em redes sociais às declarações prestadas pelo próprio contribuinte, de modo a autorizar o lançamento por arbitramento, nos termos do art. 148 do CTN, o que estabeleceria uma indevida inversão do ônus da prova.

Ainda que o Contribuinte venha a externar indícios de riqueza em suas redes sociais, em nosso entendimento, o ônus de produzir provas da efetiva situação patrimonial dos Contribuintes continua a tocar à Fiscalização. Nesse contexto, os dados tornados públicos em redes sociais podem ser considerados como

meros indícios, que podem motivar a instauração de procedimento fiscalizatório específico mas jamais ser considerados como meios hábeis de prova para arbitramento ou inversão do ônus probatório.

7. CONCLUSÃO

Ainda que o tratamento de dados pela Administração Pública seja caso específico de aplicação da LGPD, que não se submete à regra de consentimento, entendemos que a LGPD pode representar uma retomada, em parte, do escopo dos sigilos bancário e fiscal, que vinham sendo flexibilizados em face dos interesses da fiscalização nos níveis global e doméstico.

Nesse contexto, ainda que o Contribuinte não possa se opor, na maioria das vezes, ao tratamento de seus dados pessoais pela Administração Pública, a LGPD estabelece um rol considerável de direitos que condiciona este tratamento, resguardando o Contribuinte de abusos e desvios de finalidade.

O IMPACTO DA LGPD NAS RELAÇÕES DE CONSUMO

Por

LUDMILA ALBUQUERQUE KNOP HAUER

Advogada senior manager da área de Cível Empresarial do escritório Gaia Silva Gaede Advogados em Curitiba

Pós-graduada em Processo Civil – Instituto Romeu Bacelar – PR

Advogada graduada pela Pontifícia Universidade Católica do Paraná – PUC/PR.

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD), que entrará em vigor em 2021, tem como objetivo a proteção dos direitos fundamentais de liberdade e privacidade, bem como visa garantir o livre desenvolvimento da personalidade. A concretização desse fim ocorre mediante o estabelecimento de regras detalhadas para o tratamento dos dados das pessoas naturais, o qual poderá ser realizado por pessoas jurídicas ou naturais, seja por meio físico ou digital.

Entre os Princípios que norteiam a LGPD, expressamente mencionados no seu art. 6º[1], constata-se que alguns são aplicáveis também às relações de consumo, tais como transparência, livre acesso, prevenção e responsabilização. Além disso, no art. 2º, inciso VI, da LGPD, a defesa do consumidor é mencionada expressamente como um dos fundamentos que regem a proteção dos dados pessoais.

1 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

O presente artigo tem como objetivos (i) demonstrar as previsões da LGPD quanto à responsabilização e reparação de danos por parte dos agentes de tratamento (controlador e operador) e suas consequências, especialmente porque a maior parte das relações que implica coleta de dados é considerada relação de consumo; e (ii) indicar algumas cautelas que deverão ser tomadas quanto à relação contratual a ser estabelecida entre controlador e operador, seja na sua concepção ou na sua execução.

2. LGPD E RELAÇÕES DE CONSUMO

Antes de tratar do tema central, cabe informar, de forma simples e direta, quem são os personagens envolvidos no tratamento de dados de acordo com a nomenclatura definida pela própria LGPD.

Os agentes de tratamento são o controlador e o operador, sendo que esse é quem efetivamente realiza o tratamento e processamento dos dados e o controlador é o responsável pela sua coleta. O titular é a pessoa natural cujos dados serão tratados.

O art. 42 da LGPD estabelece que o controlador ou operador que causarem dano material ou moral, individual ou coletivo, decorrente da violação das normas estabelecidas na lei, serão obrigados a repará-lo. Ou seja, a regra geral é a responsabilização individual de cada um dos agentes, na medida e proporção em que seus atos praticados em contrariedade à lei tenham nexo com o dano efetivamente causado ao titular.

Por outro lado, o legislador também estabeleceu duas hipóteses para a responsabilização solidária dos agentes de tratamento pelos danos causados ao titular, a saber: (i) responsabilidade solidária do operador quando ele não tiver seguido as instruções lícitas do controlador, e (ii) solidariedade entre os controladores que estiverem diretamente envolvidos no tratamento. A implicação da solidariedade é que qualquer um desses agentes, isolada ou conjuntamente, poderá ser acionado para reparar o dano, sendo garantido, também por expressa previsão legal (art. 42, § 4º, LGPD), o direito de regresso em face daquele(s)

responsável(is) que não tenha(m) respondido, na proporção de sua participação no evento danoso.

Além disso, muito embora todo ato praticado em desacordo com a LGDP seja considerado como irregular e seja passível de indenização, a segurança dos dados é tratada pela norma com destaque:

> *"Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:*
>
> *I - o modo pelo qual é realizado;*
>
> *II - o resultado e os riscos que razoavelmente dele se esperam;*
>
> *III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.*
>
> *Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano."*

Assim, é essencial aos agentes de tratamento a adoção de medidas de segurança dos dados pessoais estabelecidas também na lei, quais sejam, adoção e implementação de parâmetros técnicos e administrativos aptos a proteger acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

A exclusão da responsabilidade dos agentes de tratamento pela reparação civil dos danos só ocorrerá se esses provarem que (i) não realizaram o tratamento de dados pessoais que lhes é atribuído; (ii) embora tenham realizado o tratamento, 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 terceiros.

Regra geral, o ônus da prova incumbe a quem alega, ou seja, caberia ao titular provar a prática do ilícito por parte dos agentes de tratamento, o efetivo dano

e o nexo entre essa prática e o dano alegado. Mas, a LGPD já deixa claro que a comprovação do enquadramento às hipóteses de ausência de responsabilização cabe aos agentes de tratamento (que serão réus nas medidas judiciais), bem como autoriza o juiz a inverter o ônus da prova quando sua produção for muito cara ao titular ou quando esse for considerado hipossuficiente para produzi-la.

Percebe-se que essa inversão, independentemente da relação que deu origem ao tratamento dos dados ser ou não de consumo, tem um grande potencial de aplicação pelo poder judiciário. Isso porque o titular (sempre pessoa física) não terá condições técnicas de comprovar por quem e de que forma seus dados foram efetivamente tratados. Além disso, a prova apta a comprovar por quem e como os dados foram tratados, bem como se a culpa é exclusiva do titular ou de terceiro, é a pericial, cujos custos são altos para a realidade financeira média da população brasileira. Mesmo que o requerente do ressarcimento civil seja beneficiário da justiça gratuita – quando é dispensado de arcar com as custas do processo e os peritos são pagos pelo Estado conforme tabela pré-estabelecida –, no âmbito do judiciário brasileiro observa-se uma enorme dificuldade de encontrar peritos bem qualificados e que aceitem o encargo de realizar seus trabalhos mediante a retribuição tabelada. Logo, para garantir o acesso à justiça de forma célere e eficaz, o julgador poderá e provavelmente colocará sobre os ombros dos agentes de tratamento o encargo (técnico e financeiro) de produzir a prova.

A LGPD visivelmente tentou estabelecer regras específicas e o mais completas possível para balizar a responsabilização decorrente dos danos causados pelos agentes de tratamento aos titulares dos dados. Todavia, ao prever (no art. 45) que a violação do direito do titular dos dados decorrente de uma relação de consumo estará sujeita às regras do CDC, os conceitos e hipóteses mencionados acima não mais prevalecerão e o titular consumidor será visto pelo poder judiciário necessariamente como parte hipossuficiente, o que lhe traz algumas vantagens.

A LGPD também estabelece (art. 4º) as hipóteses de tratamento de dados pessoais que não estão abarcadas pelas suas regras, quais sejam: (i) realizada por pessoa natural para fins exclusivamente particulares e não econômicos; (ii)

que tenham fins exclusivamente relacionados a (a) fins acadêmico, jornalístico ou artístico; (b) segurança pública; defesa nacional; segurança do Estado ou atividades de investigação e repressão de infrações penais; ou (iii) dados provenientes do exterior.

Analisando as hipóteses para as quais não se aplicam as regras de proteção de dados, constata-se que, por exclusão, toda coleta de dados realizada por pessoa jurídica, com ou sem fins econômicos, está sujeita às suas normas. Ou seja, o controlador deverá tratar os dados coletados dos seus empregados, pessoas que ingressam no seu estabelecimento mediante registro, informados em currículos enviados, entre outros. Mas também deverá tratar os dados obtidos com fins econômicos, ou seja, as informações pessoais dos seus clientes, relações essas que terão um volume maior de dados coletados e que serão consideradas como relação de consumo quando o controlador for considerado fornecedor do produto/serviço e o seu cliente for consumidor – destinatário final do produto/serviço[2].

Nas relações de consumo, aplicam-se as regras de reparação civil objetiva, que exclui a necessidade de comprovação de culpa pelo fornecedor, bastando a simples comprovação do dano e nexo decorrentes da falha na prestação dos serviços/produto. A inversão do ônus da prova e solidariedade entre os fornecedores (todos os envolvidos na cadeia de prestação dos serviços/produto) são também regras de aplicação automática.

Considerando que as figuras do controlador e do operador poderão ou não ficar sob a ingerência de uma mesma pessoa, e diante da complexidade estrutural e técnica necessárias à efetiva e segura proteção dos dados coletados, é muito provável que as empresas não tenham condições técnicas ou até mesmo financeiras de realizar internamente o tratamento de dados coletados. Portanto,

2 A relação de consumo é formada por dois polos: o consumidor e o fornecedor. O consumidor é todo aquele (pessoa física ou jurídica) que, nos termos do art. 2º do Código de Defesa do Consumidor (CDC), *"adquire ou utiliza produto ou serviço como destinatário final."*. O fornecedor é assim conceituado pelo CDC: *"Art. 3º Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços."*

vislumbra-se um cenário no qual a contratação de um operador será recorrente, assim como a responsabilidade solidária entre eles por eventuais danos.

Portanto, essa contratação deverá ser muito bem estruturada, seja para garantir ao controlador auditar os trabalhos realizados pelo operador, seja para que ao operador tenha a exata e clara compreensão das instruções repassadas pelo controlador, não presumindo que trabalho realizado esteja de acordo com a LGPD.

Tendo em vista que cabe ao controlador estabelecer quais são os dados mínimos e adequados à sua atividade, bem como suas especificidades de tratamento, ele não poderá contratar um operador de forma automática, ou seja, sem lhe repassar de forma detalhada tais informações, sem ter o mínimo de compreensão sobre as técnicas que serão aplicadas e sem assegurar-se de que essas serão aptas a garantir a eficácia e segurança estabelecidas pela lei.

Caberá então ao controlador definir contratualmente de forma clara e detalhada os deveres de cada uma das Partes, garantindo que o operador demonstre a adequação e a segurança das técnicas que serão aplicadas, bem como o seu direito de, no curso da relação, ter acesso e/ou auditar o operador e solicitar adequações e atualizações das suas práticas.

A possibilidade de atualização dos procedimentos utilizados para o tratamento de dados deve estar prevista no contrato, uma vez que, conforme já mencionado acima, as técnicas disponíveis à época em que o dado foi tratado serão levadas em consideração para fins de averiguar a regularidade ou não desse tratamento. Assim, o controlador e o operador não devem poupar esforços para garantir a implantação das técnicas mais seguras possíveis à época do tratamento.

Muito embora a LGPD já tenha previsto que o agente que responder pelo dano terá direito de regresso perante o outro agente também ou unicamente causador do dano, a delimitação dessa responsabilidade poderá ser de difícil comprovação. Por essa razão, o ideal é estabelecer no contrato de prestação de serviços firmado entre controlador e operador exemplos concretos de eventuais falhas e definição do responsável por cada uma delas. Alternativamente, quan-

do não for possível individualizar essa responsabilidade, parece recomendável estabelecer o percentual para responsabilização de cada uma das Partes envolvidas, evitando que apenas uma de fato arque com tal prejuízo ou que fique à mercê do julgador estabelecer a extensão dessa responsabilidade.

Além dos benefícios que as práticas acima destacadas podem trazer à relação a ser pactuada entre os agentes de tratamento e respectivas obrigações, também poderá ser útil para comprovar que esses tomaram todas as cautelas necessárias para cumprimento das normas da LGPD. Ainda na relação de consumo, tal questão poderá ser levada em consideração para fins de arbitramento do valor dos danos.

3. CONCLUSÃO

Diante do demonstrado acima, a mitigação dos danos aos titulares ocorrerá se houver sinergia entre o controlador e o operador para garantir o correto e seguro tratamento dos dados pessoais, uma vez que a chance de responsabilização solidária entre esses agentes é muito grande nas relações gerais e certa nas relações de consumo. Uma vez havendo a responsabilização solidária, estabelecer contratualmente critérios concretos para o exercício do direito de regresso também é atitude que se recomenda.

TRANSFERÊNCIA DE DADOS PESSOAIS E SEUS REFLEXOS TRIBUTÁRIOS

Por

MAURÍCIO BARROS
Sócio do Gaia Silva Gaede Advogados
Doutor em Direito Econômico, Financeiro e Tributário pela USP
Mestre em Direito Tributário pela PUC/SP
Especialista em Direito Tributário pelo IBET/SP
Graduado em Direito pela PUC/SP
Ex-Juiz do Tribunal de Impostos e Taxas de São Paulo
Ex-Professor Convidado de Direito Tributário – Mackenzie e FGV.

RAPHAEL ALESSANDRO PENTEADO RODRIGUES
Advogado sênior do Gaia Silva Gaede Advogados em São Paulo
Especialista em Direito Tributário pelo IBDT/SP
Graduado em Direito pela FMU.

1. INTRODUÇÃO

Com a chegada da economia digital e o desenvolvimento de novas tecnologias, cada vez mais as pessoas têm disponibilizado seus dados para empresas e entes públicos com os mais diversos objetivos (obtenção de crédito, cadastro em aplicativos ou sites, exames de saúde, consultas médicas, formulários de emprego etc.). Os dados fornecidos pelo titular podem variar muito, sendo meramente cadastrais ou de qualificação, como nome e número do documento de identidade, ou mesmo mais pessoais e sensíveis, como dados biométricos, questões genéticas, opinião política e convicção religiosa.

Na maior parte desses casos, o titular dos dados não tem qualquer conhecimento sobre o que será feito com suas informações. Via de regra, as pessoas não sabem por quanto tempo seus dados serão armazenados, com qual finalidade ou se haverá compartilhamento com terceiros.

Apesar desse desconhecimento geral sobre o que é feito com os dados das pessoas, é inegável que tais informações têm um valor agregado enorme, de modo que, em razão disso, existem empresas que buscam se beneficiar e lucrar por meio de seu compartilhamento, o que vem intensificando o debate sobre o tratamento adequado dos dados pessoais obtidos por empresas e entes públicos há muitos anos.

Em 2016, a União Europeia, após identificar a falta de regulamentação específica, atualizada e consolidada sobre o tema, aprovou a *General Data Protection Regulation* ("GDPR"), que regulamenta a proteção e o tratamento dos dados pessoais do titular/pessoa natural. Assim, quando a GDPR passou a viger em maio de 2018, as empresas e os entes públicos que coletavam e tratavam dados de cidadãos residentes na Europa (inclusive empresas brasileiras) precisaram adaptar suas operações à nova regulamentação, de forma a garantir a efetiva proteção das informações tratadas.

Por sua vez, no Brasil, as informações e dados pessoais de brasileiros eram (e ainda são) protegidos pela Constituição Federal de 1988, pelo Código Civil, pelo Código de Defesa do Consumidor e outras legislações específicas. No entanto, nenhuma dessas legislações têm como principal objetivo garantir e

regulamentar o adequado tratamento dos dados pessoais das pessoas naturais tratados por empresas e por entes públicos no ambiente da economia digital.

Além disso, tanto a União Europeia, por meio da GDPR, quanto outros países que adotam legislação no mesmo sentido (como Chile, Argentina e Uruguai), passaram a exigir que os parceiros comerciais também tivessem regulamentação que tratasse sobre a proteção de dados, o que influenciou o governo brasileiro a dispor de forma mais clara sobre o tema.

Nesse sentido, em linha com a GDPR, foi publicada a Lei nº 13.709/18 ou Lei Geral de Proteção de Dados ("LGPD"), que vem tendo o início de sua vigência discutido, podendo entrar em vigor ainda em 2020 ou mesmo em 2021, e cuja intenção é regulamentar a forma de proteção dos dados pessoais tratados dos titulares brasileiros.

Um dos pontos regulamentados na LGPD é a possibilidade de transferência/compartilhamento de dados pessoais do titular, desde que observados alguns requisitos da legislação, principalmente quando a finalidade do compartilhamento é a obtenção de vantagem econômica.

É o caso, por exemplo, das redes sociais, que podem deter diversas informações de usuários (nome, número de documento, endereços de residência e do local de trabalho, interesses pessoais, localização em tempo real, hábitos de consumo etc.) que podem, se for de interesse, ser compartilhados com outras empresas. Nesse caso, o adquirente de tais dados, que pode variar desde empresas de marketing até fornecedores de crédito, consegue traçar um perfil completo do titular e utilizar tais informações em suas atividades.

A título de exemplo o Instituto de Defesa do Consumidor ("IDEC") obteve uma liminar em ação civil pública[1] para que a Linha 4, do Metrô do Estado de São Paulo, deixasse de coletar dados por meio de câmeras especiais, relacionados com a reação dos passageiros às publicidades na Linha. Embora essa informação não esteja clara, há possibilidade de que o metrô estivesse disponibilizando esses dados às empresas para fins de venda de seus espaços de publicidade.

1 Processo nº 1090663-42.2018.8.26.0100

Assim, é possível concluir que o compartilhamento de dados pessoais, como no exemplo indicado acima, pode ocorrer com o objetivo de obter vantagem econômica, ou seja, mediante determinada contraprestação entre os controladores dos dados. Na prática, trata-se de uma venda (em sentido lato) de dados, o que lhes atribui inegável valor comercial.

Nessas situações, poderá haver uma série de reflexos tributários para o vendedor (que podem ser diferentes, dependendo da observância dos requisitos da legislação e do tipo de dado comercializado), tendo em vista a obtenção de receita e a possibilidade de exigência do ICMS ou do ISS pelos Estados e Municípios, respectivamente.

Por conta disso, e levando em consideração as disposições trazidas pela LGPD, é importante analisar os efeitos tributários decorrentes das operações com dados pessoais, aplicável tanto aos dados coletados de maneira eletrônica, tendo em vista a expansão da economia digital, quanto aos dados físicos, constantes em formulários, relatórios etc.

É o que será analisado neste artigo.

2. LGDP: QUESTÕES GERAIS, CONCEITOS E MANIFESTAÇÃO DO CONSENTIMENTO

Antes de analisar os pontos tributários relacionados à venda de dados pessoais, é necessário traçar alguns conceitos estabelecidos pela LGDP, bem como mencionar os fundamentos trazidos pela legislação que deverão ser observados em todas as operações de tratamento dos dados, como o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico, a livre iniciativa, a livre concorrência, a defesa do consumidor e os direitos humanos.

A LGPD, em seu artigo 5º, apresenta uma série de conceitos que são de extrema importância para a correta análise da lei, dentre os quais destacam-se:

(i) dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

(ii) dado pessoal sensível: dado pessoal sobre a origem racial, étnica, convicção política ou religiosa, dados referentes à saúde ou à vida, dado genético ou biométrico;

(iii) titular: pessoal natural a quem se referem os dados pessoais que são objeto de tratamento;

(iv) tratamento: toda operação realizada com dados pessoais, tais como recepção, classificação, acesso, reprodução, transmissão, distribuição e transferência (desde a coleta até a eliminação);

(v) consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

(vi) transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

(vii) uso compartilhado de dados: comunicação, difusão e transferência internacional de dados por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

(viii) controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento dos dados pessoais; e

(ix) operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

De início, é possível notar que há uma diferenciação entre dados pessoais e dados pessoais sensíveis, de modo que o tratamento do primeiro tem regras

menos rígidas se comparadas as do segundo. Entretanto, em ambos os casos, existe a possibilidade de tratamento mediante consentimento do titular ou outras hipóteses trazidas pela lei.

Vale notar ainda que as regras estabelecidas pela LGPD se aplicam no território brasileiro e ao tratamento realizado no exterior no caso de os dados terem sido coletados no Brasil ou estarem relacionados a indivíduos localizados no Brasil.[2] Por outro lado, as regras estabelecidas pela LGPD não se aplicam ao tratamento de dados realizado por pessoa natural para fins particulares e não econômicos, para fins acadêmicos, jornalísticos, artísticos e realizados para fins específicos de segurança nacional.[3]

2 Artigo 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
I - a operação de tratamento seja realizada no território nacional;
II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

3 Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II - realizado para fins exclusivamente:
a) jornalístico e artísticos; ou
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
III - realizado para fins exclusivos de:
a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou
IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

Os dados pessoais podem ser tratados apenas nas hipóteses determinadas pela legislação, quais sejam: consentimento pelo titular; cumprimento de obrigação legal ou regulatória; realização de estudos por órgão de pesquisa; execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular; pedido do titular dos dados; tutela da saúde, exclusivamente, em procedimento realizado por profissionais da saúde; ou quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Dentre os pontos acima, destaca-se a possibilidade de tratamento de dados pessoais mediante consentimento do titular, que deverá ser fornecido por escrito ou por outro meio que demonstre a sua manifestação de vontade, de maneira destacada e para as finalidades determinadas, sendo vedadas autorizações genéricas. O consentimento pode ser revogado a qualquer tempo, mediante manifestação do titular.

Já o tratamento dos dados pessoais considerados sensíveis só pode ocorrer quando o titular ou responsável legal consentir de forma específica e destacada. O tratamento dos dados sensíveis sem consentimento somente poderá ocorrer nas hipóteses em que for indispensável para o cumprimento de obrigação legal; a realização de estudos por órgãos de pesquisa (garantida a anonimização, sempre que possível), a proteção da vida ou da incolumidade física do titular ou de terceiro; a tutela da saúde; entre outros.

Uma vez verificados os conceitos acima, passamos a analisar a possibilidade de compartilhamento de dados pessoais, sensíveis ou não, com o objetivo de obter vantagem econômica.

3. POSSIBILIDADE DE VENDA DE DADOS

Algumas das formas de tratamento de dados previstas na LGPD são a comunicação, transmissão, distribuição, transferência e uso compartilhado dos dados pessoais. Os dados pessoais não considerados sensíveis podem ser tratados e

transferidos, observadas as hipóteses legais de tratamento, sobretudo o consentimento do titular.

Cumpre ressaltar que, no caso do tratamento dos dados pessoais com base na hipótese legal de consentimento do titular, a forma como esse consentimento será obtido fará toda a diferença para estar em cumprimento ou não com a nova legislação. Isso porque, o consentimento deve ser realizado por escrito ou por outro meio que demonstre a vontade inequívoca do titular, constando em cláusula ou termo destacado quando por escrito e com finalidade determinada, pois autorizações genéricas são tidas como nulas pela legislação.

Assim se determinada empresa pretender realizar a transferência/compartilhamento dos dados pessoais de um titular e não for possível enquadrar tal operação numa das demais bases legais de tratamento, deverá haver consentimento expresso do titular nesse sentido, uma vez que não há na legislação uma vedação para que os dados pessoais não considerados sensíveis sejam transferidos/compartilhados com terceiros.

A própria LGPD, ao tratar do término do tratamento de dados pessoais, admite a possibilidade de sua conservação no caso de uma possível transferência a terceiro, desde que respeitados os requisitos previstos na legislação. Essa previsão reforça a possibilidade de o controlador poder realizar a venda dos dados pessoais, desde que observadas as bases legais de tratamento, além da observação dos princípios da necessidade, finalidade e transparência previstos na lei.

Por outro lado, os dados pessoais considerados sensíveis têm uma proteção mais restritiva/rígida pela legislação. Embora a principal base legal para tratamento desses dados seja o consentimento do titular, o § 3º, do artigo 11, da LGPD, dispõe que a comunicação ou o uso compartilhado entre controladores com o objetivo de obter vantagem econômica poderá ser vedado ou ter uma regulamentação específica por parte da ANPD.

Dessa forma, é nítido que o legislador pretendeu garantir uma melhor proteção aos dados pessoais sensíveis, existindo a possibilidade de a venda de dados pessoais sensíveis ser vedada ou ao menos sofrer uma significativa restrição, caso esse seja o entendimento da ANPD, de modo que as empresas precisarão

estar atentas ao tema para não correrem riscos desnecessários de descumprimento da lei.

Dentre os dados pessoais sensíveis, os relacionados à saúde possuem uma proteção ainda maior, visto que, nesses casos, já há vedação expressa na legislação de sua transferência com o objetivo de obter vantagem econômica, independentemente de qualquer entendimento exarado pela ANPD. Essa vedação apenas não se aplica nas hipóteses concernentes à prestação de serviço de saúde, de assistência farmacêutica e de assistência à saúde, em benefício dos interesses dos titulares de dados, e para permitir a portabilidade de dados quando solicitada pelo titular ou as transações financeiras e administrativas resultantes do uso e da prestação dos serviços.

Além disso, a LGPD também prevê que é vedado o compartilhamento de dados com planos de saúde com o objetivo de vantagem econômica em qualquer hipótese, não se aplicando as exceções mencionadas anteriormente.

Fazemos a ressalva de que no presente artigo serão verificados os reflexos tributários da venda de dados pessoais, seja ela consentida ou não, realizada dentro das possibilidades previstas na LGPD, de modo que não serão compreendidas na análise possíveis vedações de compartilhamento a serem impostas pela ANDP.

4. ASPECTOS TRIBUTÁRIOS NAS OPERAÇÕES INTERNAS

4.1 "Venda" de Dados: ICMS ou ISS?

Já foi dito que os dados são o mais valioso recurso, não mais o petróleo[4], e que os dados são o novo ouro[5]. De fato, o mercado que coleta e comercializa dados parece estar em bastante evidência, considerando todos os serviços e vantagens disponibilizados "gratuitamente" (sobretudo na internet). Lembrando de outra expressão bastante difundida – "não existe almoço grátis", parece que o

4 https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
5 https://www.ceotodaymagazine.com/2018/04/is-data-the-new-gold/

tratamento e a transferência de dados de usuários que utilizam tais serviços e vantagens rendem montantes suficientes não apenas para cobrir esses custos, mas capazes de gerar receitas exorbitantes para muitas empresas.

De fato, parece haver poucas dúvidas de que os dados são bens jurídicos[6], categoria das mais genéricas no direito que expressa qualquer coisa que tem proteção da ordem jurídica à exceção dos seres humanos (que são excluídos do conceito de "bem jurídico"[7]). Os dados, como visto, contam com severa proteção jurídica no Brasil, razão pela qual é possível afirmar que se amoldam a um conceito amplo de "bem jurídico".

Contudo, nem sempre os dados são transferidos a terceiros de forma bruta ou sequer existem em linguagem acessível, razão pela qual se faz necessária uma *atividade* apta a coletá-los e tratá-los. Por outro lado, uma vez que estejam disponíveis, podem ser disponibilizados a diversas pessoas.

Diante dessas duas possibilidades, uma das primeiras questões que surgem quando se fala em venda de dados é sobre como classificá-lo para fins de incidência do ICMS ou do ISS. Isso porque, o atual sistema tributário brasileiro faz uma distinção entre mercadorias e serviços para fins de cobrança desses impostos e, atualmente, considerando o desenvolvimento da economia digital, não é tarefa fácil enquadrar os dados em uma dessas categorias.

Os serviços de empresas que têm como principal atividade a coleta de dados para realização de análises e posterior fornecimento dessas informações, via de regra, são enquadrados no item 17.01 da lista anexa à Lei Complementar nº 116/03 ("LC 116/03")[8]. O referido enquadramento foi recentemente discutido na Solução de Consulta SF/DEJUG nº 8/2019, em que a Prefeitura do Município

6 Ao serem considerados "bens", em contraposição a "coisas", reconhece-se o valor jurídico dos dados. "Entretanto, ainda dentro do conceito econômico, nem todas as coisas úteis são consideradas bens, pois, se existirem em grande abundância na natureza, ninguém se dará ao trabalho de armazená-las. Assim, nada mais útil ao homem do que o ar atmosférico, mas, como ele abunda na natureza, não é um bem econômico." (...) "Desse modo, poder-se-iam definir bens econômicos como aquelas coisas que, sendo úteis ao homem, existem em quantidade limitada no universo, ou seja, são bens econômicos as coisas úteis e raras, porque só elas são suscetíveis de apropriação." Cf. RODRIGUES, Silvio. *Direito Civil 1 - Parte Geral*. 33ª edição. São Paulo: Saraiva, 2003, p. 115.

7 PEREIRA, Caio Mário da Silva. *Instituições de Direito Civil – Volume 1*. 18ª edição. São Paulo: Forense, 1997, pp. 252-255.

8 17.01 – Assessoria ou consultoria de qualquer natureza, não contida em outros itens desta lista; análise, exame, pesquisa, coleta, compilação e fornecimento de dados e informações de qualquer natureza, inclusive cadastro e similares.

de São Paulo concluiu que uma empresa que realizava um serviço de reconhecimento da autenticidade de pessoas por meio de biometria facial deveria classificá-lo no item 17.01 da lista anexa à LC 116/03.

Nesse caso, a possibilidade de cobrança do ICMS deveria ser afastada, tendo em vista a previsão do § 2º, do artigo 1º, da LC 116/03, para o qual, ressalvadas as exceções expressas, os serviços previstos na LC 116/03 não ficam sujeitos ao ICMS, ainda que sua prestação envolva fornecimento de mercadorias (previsão que resolve eventual conflito de competência).

Por outro lado, a questão não é tão clara quando se fala de empresa que tem os dados dos titulares como uma mera consequência de suas outras atividades (estabelecimentos comerciais, aplicativos de transporte, redes sociais, clínicas de saúde etc.) e, por opção, resolve por disponibilizá-los a terceiros.

A empresa, nessa hipótese, não foi contratada para coletar os dados, processá-los e transferi-los, ela apenas os detém e, por opção, os compartilha com terceiros, mediante determinado pagamento. Nesses casos, não há um esforço efetivo para a obtenção dos dados com a finalidade de compartilhamento, sendo essa uma mera decorrência da atividade da empresa, ou seja, não há qualquer prestação de serviço efetivamente.

De qualquer forma, o item 17.01, da LC 116/03, dispõe expressamente que o fornecimento de dados é hipótese de serviço sujeita ao ISS. Sendo assim, haveria tributação normal pelo imposto mesmo no caso de um controlador que detém os dados como uma mera consequência de sua atividade principal.

Nesse ponto, cumpre esclarecer que, até recentemente, o Supremo Tribunal Federal ("STF") segregava a incidência do ISS e do ICMS entre hipóteses de obrigação de fazer e obrigação de dar, respectivamente. Desse entendimento, decorreu a Súmula Vinculante nº 31[9], para a qual não cabe a incidência do ISS em operações envolvendo locação de coisas, por não haver uma efetiva prestação de serviço, mas apenas a disponibilização de um bem (não há obrigação de fazer). Esse também foi o entendimento no caso que envolveu a classificação

9 É inconstitucional a incidência do imposto sobre serviços de qualquer natureza - ISS sobre operações de locação de bens móveis.

do software de prateleira como uma mercadoria, sujeito ao ICMS, e o software encomendado como um serviço, sujeito ao ISS.[10]

Seguindo essa linha de raciocínio, na mera disponibilização de dados (ainda que haja previsão na LC 116/03) seria possível argumentar que também não há uma efetiva obrigação de fazer, de modo que essas operações não poderiam ser alcançadas pelo ISS. Entretanto, vale destacar que o STF tem relativizado a conceituação de serviços como "obrigações de fazer", em contraponto as "obrigações de dar", sobretudo com o julgamento do Recurso Extraordinário nº 651.703, embora a Súmula 31 ainda esteja plenamente vigente (o que é uma contradição).

No referido julgamento, que tratou da cobrança do ISS no caso das operadoras de planos de saúde, com base no artigo 156, inciso III, da Constituição Federal e na previsão do item de plano de medicina na LC 116/03, o STF concedeu uma interpretação mais ampla ao conceito de serviço, nos seguintes termos:

> *(...) 3. Tese: "As operadoras de planos de saúde realizam prestação de serviço sujeita ao Imposto Sobre Serviços de Qualquer Natureza - ISSQN, previsto no art. 156, III, da CRFB/88." (...)*
>
> *20. A classificação (obrigação de dar e obrigação de fazer) escapa à ratio que o legislador constitucional pretendeu alcançar, ao elencar os serviços no texto constitucional tributáveis pelos im-*

10 Recurso extraordinário nº 176.626: *Ementa: I. Recurso extraordinário: prequestionamento mediante embargos de declaração (Súm. 356). A teor da Súmula 356, o que se reputa não prequestionado é o ponto indevidamente omitido pelo acórdão primitivo sobre o qual "não foram opostos embargos declaratórios". Mas se, opostos, o Tribunal a quo se recuse a suprir a omissão, por entendê-la inexistente, nada mais se pode exigir da parte (RE 210.638, Pertence, DJ 19.6.98). II. RE: questão constitucional: âmbito de incidência possível dos impostos previstos na Constituição: ICMS e mercadoria. Sendo a mercadoria o objeto material da norma de competência dos Estados para tributar-lhe a circulação, a controvérsia sobre se determinado bem constitui mercadoria é questão constitucional em que se pode fundar o recurso extraordinário. III. Programa de computador ("software"): tratamento tributário: distinção necessária. Não tendo por objeto uma mercadoria, mas um bem incorpóreo, sobre as operações de "licenciamento ou cessão do direito de uso de programas de computador" " matéria exclusiva da lide ", efetivamente não podem os Estados instituir ICMS: dessa impossibilidade, entretanto, não resulta que, de logo, se esteja também a subtrair do campo constitucional de incidência do ICMS a circulação de cópias ou exemplares dos programas de computador produzidos em série e comercializados no varejo - como a do chamado "software de prateleira" (off the shelf) - os quais, materializando o corpus mechanicum da criação intelectual do programa, constituem mercadorias postas no comércio.*

postos (v.g., serviços de comunicação – tributáveis pelo ICMS, art. 155, II, CRFB/88; serviços financeiros e securitários – tributáveis pelo IOF, art. 153, V, CRFB/88; e, residualmente, os demais serviços de qualquer natureza – tributáveis pelo ISSQN, art. 156. III, CRFB/88), qual seja, a de captar todas as atividades empresariais cujos produtos fossem serviços sujeitos a remuneração no mercado.

(...)

A finalidade dessa classificação (obrigação de dar e obrigação de fazer) escapa totalmente àquela que o legislador constitucional pretendeu alcançar, ao elencar os serviços no texto constitucional tributáveis pelos impostos (por exemplo, serviços de comunicação – tributáveis pelo ICMS; serviços financeiros e securitários – tributáveis pelo IOF; e, residualmente, os demais serviços de qualquer natureza – tributáveis pelo ISS), qual seja, a de captar todas as atividades empresariais cujos produtos fossem serviços, bens imateriais em contraposição aos bens materiais, sujeitos a remuneração no mercado. (...) (Recurso Extraordinário nº 651703, Relator Ministro Luiz Fux, de 29/09/16)

Nesse sentido, embora não seja possível afirmar que a dicotomia entre obrigação de dar e obrigação de fazer tenha sido efetivamente abolida pelo STF, é fato que o Tribunal a relativizou. Sendo assim, e considerando que o ISS deve incidir sobre os serviços expressamente previstos na legislação, seria possível enquadrar o fornecimento de dados no item 17.01, da lista anexa à LC 116/03.

De qualquer forma, a discussão sobre a questão da relativização da dicotomia existente entre ISS e ICMS quanto à classificação de uma obrigação de fazer ou de dar deve voltar a ser abordada pelo STF quando do julgamento do Recurso Extraordinário nº 688.223, no qual o referido Tribunal analisará a incidência do ISS sobre o licenciamento de softwares, considerando o argumento que se trata de uma obrigação de dar e portanto, não sujeita ao imposto.

No que tange ao ICMS, apesar da previsão do fornecimento de dados na LC 116/03, destaca-se a nítida intenção dos Estados de exigir ICMS nas operações envolvendo a economia digital, tendo em vista a publicação dos Convênios Confaz ICMS nº 181/15[11] e 106/17[12]. A aplicação automática dessa legislação poderia levar à incidência de ICMS sobre as operações de compra e venda de dados, sobretudo pela amplitude do texto da Cláusula primeira, do Convênio ICMS 106/17:

> **Cláusula primeira** As operações com bens e mercadorias digitais, tais como softwares, programas, jogos eletrônicos, aplicativos, arquivos eletrônicos e congêneres, que sejam padronizados, ainda que tenham sido ou possam ser adaptados, comercializadas por meio de transferência eletrônica de dados observarão as disposições contidas neste convênio.

Com efeito, a venda de dados padronizados poderia se enquadrar no texto acima, sujeitando o provedor desses dados a incidência do imposto estadual.

Contudo, sem prejuízo do enquadramento da atividade na lista anexa à LC 116/03, conforme apontado acima, parece ser inadequada a instituição de qualquer ICMS sobre as operações de compra e venda de dados, por não se tratar de "circulação de mercadoria".

Com efeito, sedimentou-se na doutrina clássica a ideia de que o signo "mercadoria" deveria ser entendido como o bem móvel sujeito à mercancia, ou seja, o que está inserido no processo econômico mercantil[13]. Nesse sentido, ROQUE ANTONIO CARRAZZA[14] entende "que toda mercadoria é bem móvel, mas nem todo bem móvel é mercadoria. Só o bem móvel que se destina à prática de operações mercantis é que assume a qualidade de mercadoria (...), portanto, é

11 Autoriza as unidades federadas que especifica a conceder redução de base de cálculo nas operações com softwares, programas, jogos eletrônicos, aplicativos, arquivos eletrônicos e congêneres na forma que especifica.
12 Disciplina os procedimentos de cobrança do ICMS incidentes nas operações com bens e mercadorias digitais comercializadas por meio de transferência eletrônica de dados e concede isenção nas saídas anteriores à saída destinada ao consumidor final.
13 BORGES, José Souto Maior. "O fato gerador do ICM e os estabelecimentos autônomos". In *Revista de Direito Administrativo* 103, 1971, p. 34.
14 In CARRAZZA, Roque Antonio. *ICMS*. 12ª edição. São Paulo: Malheiros, 2007, p. 43.

a destinação do objeto que lhe confere, ou não, o caráter de mercadoria". No mesmo sentido, Paulo de Barros Carvalho ensina que "a natureza mercantil do produto não está, absolutamente, entre os requisitos que lhe são intrínsecos, mas na destinação que se lhe dê"[15].

A posição segundo a qual o ICMS somente poderia incidir sobre operações envolvendo bens móveis/corpóreos objeto de mercancia encontra guarida no art. 191, do Código Comercial de 1850[16], que conceituava contrato mercantil como aquele que tinha como objeto a compra e venda de coisa de efeitos móveis ou semoventes. Diante disso, a doutrina defendia que essa era a concepção corrente de mercadoria quando o constituinte de 1988 desenhou o sistema tributário nacional e distribuiu aos Estados a competência de tributar as operações relativas à circulação de mercadorias[17]. Mesmo a doutrina que não reconhecia o conceito de operação mercantil proveniente do Código Comercial, como era o caso de Alcides Jorge Costa[18], entendia que somente coisas móveis poderiam ser objeto de mercancia[19], razão pela qual a corporalidade/tangibilidade sempre foi, pacificamente, uma condição para a incidência do ICMS.

Evidentemente, outra não poderia ser a posição doutrinária à época da criação do ICM ou mesmo da promulgação da Constituição Federal de 1988 (ICMS), ante a inexistência de circulação de bens incorpóreos nesses momentos. A questão que deve ser respondida, portanto, é se bens incorpóreos atualmente

15 *Direito Tributário Linguagem e Método*. 2ª edição. São Paulo: Noeses, 2009, p. 730.
16 Art. 191 - O contrato de compra e venda mercantil é perfeito e acabado logo que o comprador e o vendedor se acordam na coisa, no preço e nas condições; e desde esse momento nenhuma das partes pode arrepender-se sem consentimento da outra, ainda que a coisa se não ache entregue nem o preço pago. Fica entendido que nas vendas condicionais não se reputa o contrato perfeito senão depois de verificada a condição (artigo nº. 127).
É unicamente considerada mercantil a compra e venda de efeitos móveis ou semoventes, para os revender por grosso ou a retalho, na mesma espécie ou manufaturados, ou para alugar o seu uso; compreendendo-se na classe dos primeiros a moeda metálica e o papel moeda, títulos de fundos públicos, ações de companhias e papéis de crédito comerciais, contanto que nas referidas transações o comprador ou vendedor seja comerciante.
17 CARRAZZA (2007), p. 44.
18 Para Alcides Jorge Costa, "a noção de mercadoria, para aplicação da legislação do ICM, é mais extensa do que a corrente no direito comercial". Assim, para fins de ICM, "mercadoria é toda cousa móvel corpórea produzida para ser colocada em circulação, ou recebida", a qualquer título, para ter curso no processo de circulação, mesmo se por transferência de um outro estabelecimento da mesma pessoa jurídica. In COSTA, Alcides Jorge. *ICM na Constituição e na Lei Complementar*. São Paulo: Resenha Tributária, 1978. p. 99.
19 COSTA (1978), p. 99.

podem ser objeto de cobrança de ICMS, em um esforço de ampliação da materialidade do imposto.

A resposta há de ser negativa.

Isso porque, a Constituição Federal, ao delimitar e dividir a competência tributária para que os entes políticos subnacionais (União, Estados, Distrito Federal e Municípios) instituíssem impostos de acordo com as materialidades eleitas, fê-lo com base no contexto normativo-social de 1988. Ao assim fazer, os conceitos adotados para a divisão das materialidades para a instituição de impostos adotados pelo constituinte originário foram aqueles vigentes à época, pois não parece razoável que o constituinte pudesse fazer uma divisão de algo incerto ou ainda em aberto, já que a divisão federativa e a autonomia municipal não são compatíveis com esse tipo de insegurança jurídica. Não se trata, que fique bem claro, de fechar os olhos para a nova realidade que se descortina com o avanço tecnológico, mas reconhecer alguma utilidade à demarcação de competência e blindá-la de subjetivismos inconsequentes. Reforça essa constatação o fato de a CF/88 ter relegado à União Federal a competência para tributar as operações não abrangidas pelos demais impostos e ao Congresso Nacional para criar normas para dirimir conflitos de competência. Essas são as cláusulas, por excelência, para abranger as operações futuras que não se amoldam a nenhum ou adotam traços de mais de um dos conceitos adotados pela CF/88, de modo a acomodar, inclusive, novas operações inexistentes à época. Essa constatação também parece ser a única capaz de atribuir à CF/88 uma funcionalidade permanente em seu capítulo voltado ao sistema tributário nacional, pois, do contrário, necessariamente o sistema quedaria impraticável para o futuro.

Com efeito, o conceito consolidado de "mercadoria", vigente à época da promulgação da CF/88, correspondia a bens corpóreos produzidos em série e objeto de mercancia, na linha da majoritária doutrina sobre o tema. Tanto é assim que a legislação vigente à época (art. 1º, do Decreto-lei 406/68[20]), assim como a

20 Art. 1º. O imposto sobre operações relativas à circulação de mercadorias tem como fato gerador:
I - a saída de mercadorias de estabelecimento comercial, industrial ou produtor;
II - a entrada, em estabelecimento comercial, industrial ou produtor, de mercadoria importada do exterior pelo titular do estabelecimento;
III - o fornecimento de alimentação, bebidas e outras mercadorias em restaurantes, bares, cafés e estabelecimentos similares.

atual (Lei Complementar 87/96), condicionava a incidência do então ICM à "saída" das mercadorias do "estabelecimento", situação incompatível, obviamente, com bens incorpóreos. O Supremo Tribunal Federal confirmou esse entendimento, ao apontar, no julgamento do Recurso Extraordinário 176.626[21], que "o conceito de mercadoria efetivamente não inclui os bens incorpóreos, como os direitos em geral: mercadoria é bem corpóreo objeto de atos de comércio ou destinado a sê-lo" (excerto do voto do relator do recurso, Ministro Sepúlveda Pertence). Essa posição, adotada quando do julgamento das operações envolvendo software em suportes físicos, foi confirmada na decisão do Recurso Extraordinário 199.464[22].

Ainda que a energia elétrica pudesse, em princípio, estar fora desse conceito de "mercadoria" ligado à corporalidade, fato é que a incidência do imposto estadual sobre a energia apenas foi admitida com a CF/88 e o texto do art. 155, expressamente, a ela se refere em duas passagens. Desse modo, ainda que a energia elétrica não se enquadre na acepção de "bem corpóreo", o simples fato

21 "I. Recurso extraordinário: prequestionamento mediante embargos de declaração (Súm. 356). A teor da Súmula 356, o que se reputa não prequestionado é o ponto indevidamente omitido pelo acórdão primitivo sobre o qual 'não foram opostos embargos declaratórios'. Mas se, opostos, o Tribunal a quo se recuse a suprir a omissão, por entendê-la inexistente, nada mais se pode exigir da parte (RE 210.638, Pertence, DJ 19.6.98).
II. RE: questão constitucional: âmbito de incidência possível dos impostos previstos na Constituição: ICMS e mercadoria. Sendo a mercadoria o objeto material da norma de competência dos Estados para tributar-lhe a circulação, a controvérsia sobre se determinado bem constitui mercadoria é questão constitucional em que se pode fundar o recurso extraordinário.
III. Programa de computador ("software"): tratamento tributário: distinção necessária. Não tendo por objeto uma mercadoria, mas um bem incorpóreo, sobre as operações de "licenciamento ou cessão do direito de uso de programas de computador" " matéria exclusiva da lide ", efetivamente não podem os Estados instituir ICMS: dessa impossibilidade, entretanto, não resulta que, de logo, se esteja também a subtrair do campo constitucional de incidência do ICMS a circulação de cópias ou exemplares dos programas de computador produzidos em série e comercializados no varejo - como a do chamado "software de prateleira" (off the shelf) - os quais, materializando o *corpus mechanicum* da criação intelectual do programa, constituem mercadorias postas no comércio." (RE 176626, Relator(a): Min. SEPÚLVEDA PERTENCE, Primeira Turma, julgado em 10/11/1998, DJ 11-12-1998 PP-00010 EMENT VOL-01935-02 PP-00305 RTJ VOL-00168-01 PP-00305).

22 "TRIBUTÁRIO. ESTADO DE SÃO PAULO. ICMS. PROGRAMAS DE COMPUTADOR (SOFTWARE). COMERCIALIZAÇÃO. No julgamento do RE 176.626, Min. Sepúlveda Pertence, assentou a Primeira Turma do STF a distinção, para efeitos tributários, entre um exemplar standard de programa de computador, também chamado "de prateleira", e o licenciamento ou cessão do direito de uso de software. A produção em massa para comercialização e a revenda de exemplares do *corpus mechanicum* da obra intelectual que nele se materializa não caracterizam licenciamento ou cessão de direitos de uso da obra, mas genuínas operações de circulação de mercadorias, sujeitas ao ICMS. Recurso conhecido e provido." (RE 199464, Relator(a): Min. ILMAR GALVÃO, Primeira Turma, julgado em 02/03/1999, DJ 30-04-1999 PP-00023 EMENT VOL-01948-02 PP-00307).

de o texto constitucional atribuir a competência tributária aos Estados para instituir o ICMS sobre operações que envolvam energia elétrica já torna essa incidência um pressuposto no exercício da competência tributária, ante a expressa menção constitucional. No mínimo, há uma ficção constitucional de que energia elétrica é mercadoria, pela expressa equiparação de ambos.

Por tudo isso, não se pode admitir que a circulação de bens incorpóreos esteja abrangida pela competência tributária para instituir o ICMS, uma vez que de "mercadoria" não se trata[23].

Entretanto, ainda que se pudesse considerar bens intangíveis como "mercadorias", fato é que outro elemento intrínseco a esse conceito não é observado nos dados, que é a destinação ao *consumo*. Isso porque, por serem bens inconsumíveis[24], ou seja, que podem ser usados de forma contínua e reiterada sem que isso importe sua destruição, os dados nunca serão propriamente destinadas ao consumo, no sentido de exaurimento de suas propriedades físicas, químicas ou mesmo tecnológicas (obsolescência etc.), que é um traço característico das mercadorias. Ainda que os dados possam ser impressos e vendidos em massa tal como livros, ainda assim não se trataria, propriamente, da comercialização dos dados em si, mas de seu suporte físico, que poderia ensejar a incidência do ICMS, uma vez superada a discussão quanto a eventual imunidade da ope-

23 Essa visão, embora predominante, não conta com unanimidade por parte da doutrina, havendo vozes que aceitam uma maior abertura semântica das regras de competência tributária, de modo a abarcar novas realidades. Nesse sentido, é a lição de MARCO AURELIO GRECO, que ressalta a necessidade de se atualizar os conceitos constitucionais no contexto de um Estado Democra1tico de Direito. Embora trate do software antes da LC 116/03, a posição de MARCO AURELIO GRECO é clara quanto à possibilidade de enquadrar intangíveis no conceito de "mercadoria" para fins de incidência de ICMS. In *Internet e direito*. 2ª edição. São Paulo: Dialética, 2000, pp. 93-94. No mesmo sentido: BEIJA, Osvaldo Bispo de. "ICMS e comércio de 'mercadorias' intangíveis, via internet". In *Revista Dialética de Direito Tributário* 88, pp. 66 e ss.; CEZAROTI, Guilherme. *ICMS no comércio eletrônico*. São Paulo: MP, 2005, pp. 152-153.

24 "Ensina Beviláqua que a distinção (entre bem consumível e inconsumível) se funda numa consideração econômico-jurídica, pois há coisas que se destinam ao simples uso, delas tirando-se as utilidades, sem lhes destruir a substância - são as coisas não consumíveis; e há outras que se destroem imediatamente, à medida que são utilizadas, ou aplicadas - são as consumíveis. Além das coisas consumíveis por sua natureza, que desaparecem com o primeiro uso, a lei classifica igualmente como consumíveis as que se destinam à alienação. Assim o livro, para o estudante, é bem inconsumível, porque ele sobrevive à utilização; mas para o livreiro é consumível, porque sua utilização (alienação) conduz ao seu perecimento para o alienante. A máquina não é consumível para quem a explora, mas o é para o fabricante que a produz e a destina à venda." In RODRIGUES (2003), pp. 129-130.

ração. Ademais, considerando que não haverá consumo, tampouco se poderá falar em circulação, pois essa, no âmbito do ICMS, pressupõe uma circulação com destino ao consumo do bem[25].

Por tudo isso, nunca haverá o consumo exigido inerente ao conceito de "mercadoria", razão pela qual não há competência tributária para a instituição de ICMS sobre operações envolvendo dados puramente considerados.

Além disso, a utilização dos dados sempre ocorreria a título precário, considerando a prerrogativa de seu titular de revogar, a qualquer momento, o consentimento antes manifestado. Nesse sentido, como a empresa não é titular dos dados (não pode usar, gozar e usufruir de maneira integral e livre), não haveria como ela realizar uma efetiva transferência de propriedade, o que também colocaria em dúvida a efetiva circulação jurídica dos dados, considerando a regra matriz de incidência tributária do ICMS.

4.2 Tributação do Ato Ilícito

Conforme destacado anteriormente, existe a possibilidade de venda de dados pessoais entre empresas, independentemente de se tratar de dados sensíveis ou não, desde que observadas as regras estabelecidas na LGPD para cada uma dessas hipóteses. Via de regra, se a empresa realizar a venda dos dados observando as exigências e limitações da LGPD, tal operação será considerada legal. Nesse caso, a receita decorrente do compartilhamento deverá ser tributada normalmente pela contribuição ao PIS e pela Cofins, bem como submetida à apuração do Imposto de Renda da Pessoa Jurídica ("IRPJ").

Entretanto, em relação à receita decorrente das vendas de tais dados, surge a questão se existe a possibilidade de tributação quando a operação realizada pela empresa não observar as regras/hipóteses estabelecidas pela LGPD, tratadas nos tópicos anteriores, o que a tornaria ilegal/ilícita.

Com efeito, o Código Tributário Nacional define, por um lado, que "tributo é toda prestação pecuniária compulsória, em moeda ou cujo valor nela se possa exprimir, **que não constitua sanção de ato ilícito**, instituída em lei e co-

25 Alcides Jorge Costa conclui que "circulação é o encaminhamento da mercadoria em direção ao consumo". Cf. COSTA (1978), p. 88.

brada mediante atividade administrativa plenamente vinculada" (grifo nosso). Nessa linha, nenhum tributo pode ter como materialidade um fato ilícito, na medida em que esse apenas pode ter como consequências pecuniárias imposições sancionatórias (ex.: multas, juros de mora etc.).

Por outro lado, o artigo 118, do mesmo Código, dispõe de maneira expressa que "a definição legal do fato gerador é interpretada abstraindo-se a validade jurídica dos atos efetivamente praticados pelos contribuintes, responsáveis, ou terceiros, bem como da natureza do seu objeto ou dos seus efeitos". Trata-se da positivação do chamado princípio da *pecunia non olet* (o dinheiro não cheira).

Como ficariam as operações ilícitas de transferências de dados a terceiros? Poderiam ou não ser tributadas?

Com efeito, a linha adotada pelo CTN demonstra-se coerente, uma vez que, se por um lado veda que as materialidades dos tributos sejam fatos ilícitos, por outro permite que as materialidades lícitas decorrentes de negócios ilícitos sejam regularmente tributadas. Não se trata de tributar o ato ilícito em si, mas a efetiva percepção de renda, receita etc. percebidas a partir do ilícito. Seria o caso, por exemplo, de tributar a renda ou a receita obtida com o compartilhamento de dados pessoais sem o devido consentimento do titular ou não sem observância de qualquer outra das hipóteses da LGPD que permitam o seu compartilhamento.

O próprio STF já se manifestou de forma favorável à tributação de fatos geradores decorrentes de negócios ilícitos, como se depreende da seguinte decisão:

> *"Sonegação fiscal de lucro advindo de atividade criminosa: "non olet". Drogas: tráfico de drogas, envolvendo sociedades comerciais organizadas, com lucros vultosos subtraídos à contabilização regular das empresas e subtraídos à declaração de rendimentos: caracterização, em tese, de crime de sonegação fiscal, a acarretar a competência da Justiça Federal e atrair pela conexão, o tráfico de entorpecentes: irrelevância da origem ilícita, mesmo quando criminal, da renda subtraída à tributação. A exoneração tributária dos resultados econômicos de fato criminoso - antes de ser corolário*

> *do princípio da moralidade - constitui violação do princípio de isonomia fiscal, de manifesta inspiração ética."* (HC 77530-RS, Primeira Turma, Relator Ministro Sepulveda Pertence, de 25/08/1998)

Nesse sentido, receitas decorrentes das vendas de dados pessoais realizadas sem consentimento do titular, ou que não observem outras bases legais previstas na LGPD (e que, portanto, sejam consideradas ilegais/ilícitas), poderão ser tributadas normalmente com relação às contribuições ao PIS e a Cofins e pelo IRPJ. Não seria, no caso, a operação em si a ser tributada, mas o resultado financeiro obtido a partir dela.

Contudo, o mesmo entendimento não poderia ser aplicado para o ICMS ou ISS, visto que, nesses casos, estar-se-ia exigindo impostos sobre a circulação de bens que não poderiam ser comercializados[26] ou sobre uma prestação de serviço efetivamente ilícita. Nesse caso, o núcleo do fato gerador em si e ilícito, o que impede qualquer incidência dos tributos incidentes sobre as operações. O STJ já se pronunciou nesse sentido sobre a exigência do imposto de importação em uma operação ilícita:

> *TRIBUTÁRIO. APREENSÃO DE MERCADORIAS. IMPORTAÇÃO IRREGULAR. PENA DE PERDIMENTO. CONVERSÃO EM RENDA.*
>
> *1. Nos termos do Decreto-lei nº 37/66, justifica-se a aplicação da pena de perdimento se o importador tenta ingressar no território nacional, sem declaração ao posto fiscal competente, com mercadorias que excedem, e muito, o conceito de bagagem, indicando nítida destinação comercial.*
>
> *2. O art. 118 do CTN consagra o princípio do "non olet", segundo o qual o produto da atividade ilícita deve ser tributado, desde que realizado, no mundo dos fatos, a hipótese de incidência da obrigação tributária.*
>
> ***3. Se o ato ou negócio ilícito for acidental à norma de tributação (= estiver na periferia da regra de incidência), surgirá a***

26 Sem prejuízo da ilegalidade e inconstitucionalidade dessa cobrança, como visto antes neste texto.

obrigação tributária com todas as consequências que lhe são inerentes. Por outro lado, não se admite que a ilicitude recaia sobre elemento essencial da norma de tributação.

4. Assim, por exemplo, a renda obtida com o tráfico de drogas deve ser tributada, já que o que se tributa é o aumento patrimonial e não o próprio tráfico. Nesse caso, a ilicitude é circunstância acidental à norma de tributação. No caso de importação ilícita, reconhecida a ilicitude e aplicada a pena de perdimento, não poderá ser cobrado o imposto de importação, já que "importar mercadorias" é elemento essencial do tipo tributário. Assim, a ilicitude da importação afeta a própria incidência da regra tributária no caso concerto. (...) (Recurso especial nº 984.607, Relator nº Ministro Castro Meira, de 05/11/2008)

Dessa forma, embora seja possível que os fiscos estadual ou municipal exijam o tributo em operações consideradas ilícitas/ilegais, há fundamentos para o afastamento de quaisquer cobranças.

5. ASPECTOS TRIBUTÁRIOS NAS OPERAÇÕES INTERNACIONAIS

5.1 Exportação de Dados

O artigo 33, da LGPD, dispõe sobre as hipóteses em que é possível a transferência internacional de dados, dentre quais destacamos as seguintes: para países ou organismos internacionais que tenham grau de proteção de dados pessoais adequados ao da LGPD; quando o controlador comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados, considerando as cláusulas contratuais específicas para a transferência, cláusulas padrão contratuais, normas corporativas globais; quando a autoridade nacional autorizar a transferência; quando o titular fornecer consentimento específico e em destaque para a transferência, com a informação prévia sobre o caráter internacional da operação.

A legislação, ao tratar das operações internacionais, não traz qualquer vedação sobre o intuito de obter ou não vantagem econômica, o que leva à conclusão de que existe a possibilidade de venda nesses casos, observadas as demais disposições e vedações da lei quanto à transferência de dados pessoais, inclusive quanto aos considerados sensíveis.

Vale notar que a definição do conteúdo de eventuais cláusulas estabelecidas pelas empresas para a realização de transferências internacionais será realizada pela autoridade nacional, de modo que será necessário observar um padrão mínimo o que, em caso de inobservância, tornará a transferência ilegal.[27]

Na hipótese de exportação, não haverá efeitos relevantes para fins de ICMS, ISS ou PIS e Cofins, independentemente do entendimento dos entes federativos, tendo em vista que tais tributos não são exigidos nessa modalidade operação. Apesar disso, a renda auferida pela venda dos dados deverá ser tributada pelo IRPJ, de acordo com o regime adotado pela empresa, mesmo que o compartilhamento não observe as regras da LGPD, em razão do princípio *pecúnia non olet* já mencionado no item 4.2 acima.

Vale ponderar ainda que, de acordo artigo 15-B, inciso I, do Decreto nº 6.306/07[28], bem como com o entendimento da Receita Federal do Brasil

27 Artigo 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.
§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.
§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.
§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.
§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.
§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.
28 Artigo 15-B. A alíquota do IOF fica reduzida para trinta e oito centésimos por cento, observadas as seguintes exceções:
I - nas operações de câmbio relativas ao ingresso no País de receitas de exportação de bens e serviços: zero; (...)

("RFB")[29], no caso de operações de câmbio relativas ao ingresso no país de receitas de exportação de bens e serviços, o IOF está sujeito à alíquota zero. Assim, independentemente de se considerar os dados pessoais como mercadoria ou serviço, no fechamento do câmbio decorrente da entrada de receitas relacionadas com a exportação não haverá pagamento de IOF.

5.2 Importação De Dados

Diferentemente da exportação, a importação de dados com a respectiva remessa de valores ao exterior pode gerar algumas discussões. Isso porque, conforme destacado anteriormente, existe a possibilidade de enquadramento dos dados pessoais como mercadoria ou serviço, tendo em vista a ânsia dos entes federativos em tributar operações envolvendo a economia digital.

A LC 116/03 dispõe que o imposto será devido também sobre o serviço proveniente do exterior do País. Nesse caso, sendo possível enquadrar a remessa

29 Solução de Consulta Cosit nº 231/2019: RECURSOS PROVENIENTES DE EXPORTAÇÕES. MANUTENÇÃO NO EXTERIOR. INOCORRÊNCIA DO FATO GERADOR. Não incide IOF quando da manutenção de recursos em moeda estrangeira em instituição financeira fora do país, relativos aos recebimentos de exportações brasileiras de mercadorias e de serviços para o exterior, realizadas por pessoas físicas ou jurídicas. Nesta situação, não há liquidação de contrato de câmbio e, portanto, não se verifica a ocorrência do fato gerador do imposto conforme definido no art. 63, II do Código Tributário Nacional (CTN) e no art. 11 do Decreto 6.306, de 2007. OPERAÇÕES DE CÂMBIO RELATIVAS AO INGRESSO NO PAÍS DE RECEITAS DE EXPORTAÇÃO DE BENS E SERVIÇOS. ALÍQUOTA ZERO. a) No caso de operações de câmbio relativas ao ingresso no país de receitas de exportação de bens e serviços, há a incidência do IOF, à alíquota zero, conforme expressa previsão no art. 15-B, I, do Decreto nº 6.306, de 2007. b) No entanto, para a incidência da alíquota zero devem ser observados a forma e os prazos estabelecidos pelo Conselho Monetário Nacional -CMN e pelo Banco Central do Brasil - BCB, independentemente de os recursos terem sido inicialmente recebidos em conta mantida no exterior, conforme autoriza a legislação pátria. c) Nos termos da legislação vigente (art. 16-A da Resolução CMN nº 3.568, de 2008, e do art. 99 da Circular BCB nº 3.691, de 2013), para que se caracterize como operação de câmbio relativa a ingresso no país de receitas de exportação de bens e serviços, na forma do art. 15-B, I, do Decreto nº 6.306, de 2007: c.1) O contrato de câmbio de exportação deverá ser celebrado para liquidação pronta ou futura, prévia ou posteriormente ao embarque da mercadoria ou da prestação do serviço, observado o prazo máximo de 750 (setecentos e cinquenta) dias entre a contratação e a liquidação, bem como o seguinte: I - no caso de contratação prévia, o prazo máximo entre a contratação de câmbio e o embarque da mercadoria ou da prestação do serviço é de 360 (trezentos e sessenta) dias; II - o prazo máximo para liquidação do contrato de câmbio é o último dia útil do 12º mês subsequente ao do embarque da mercadoria ou da prestação do serviço. c.2) Para os contratos de câmbio de exportação, no caso de requerimento de recuperação judicial, ajuizamento de pedido de falência do exportador ou em outra situação em que fique documentalmente comprovada a incapacidade do exportador para embarcar a mercadoria ou para prestar o serviço por fatores alheios à sua vontade, o embarque da mercadoria ou a prestação do serviço pode ocorrer até 1.500 (mil e quinhentos) dias a partir da data de contratação da operação de câmbio, desde que o prazo entre a contratação e a liquidação do contrato de câmbio não ultrapasse 1.500 (mil e quinhentos) dias.

de dados pessoais do exterior como uma prestação de serviço, considerando uma empresa cuja principal atividade não seja a coleta, análise e tratamento de dados, os municípios poderão exigir o ISS nessas operações.

Além disso, é provável que a RFB exija o PIS e a Cofins devidos em razão da importação do serviço, conforme previsão do artigo 1º, da Lei nº 10.865/04[30]. Também deverá haver retenção do imposto de renda referente aos valores remetidos ao exterior, considerando a alíquota de 25%, conforme previsão do artigo 7º, da Lei nº 9.779/99, exceto para os casos em que haja tratado para evitar a dupla tributação. Cumpre ressaltar que essa alíquota pode ser de 15%, caso a RFB entenda que a remessa dos dados é uma espécie de serviço técnico, o que atrairia a incidência da Contribuição de Intervenção no Domínio Econômico ("CIDE"), cuja alíquota é de 10%.

Apesar da possibilidade de os Municípios considerarem a transferência de dados pessoais do exterior como um serviço, também não se descarta a possibilidade de os Estados exigirem o ICMS na operação, caso entendam que se trata de uma operação mercantil com um bem intangível. Entretanto, conforme destacado anteriormente, existem diversos argumentos contra a incidência desse imposto.

Nesse sentido, como reforço à impossibilidade de cobrança do ICMS, vale destacar a Lei Complementar nº 87/96, que dispõe que um dos fatos geradores do ICMS é o desembaraço aduaneiro. No caso de transferência internacional de dados, não haveria efetivamente qualquer desembaraço, de modo que, ao menos se for levada em consideração a literalidade desse dispositivo, a exigência do ICMS na importação não encontraria respaldo legal.

30 Artigo 1º Ficam instituídas a Contribuição para os Programas de Integração Social e de Formação do Patrimônio do Servidor Público incidente na Importação de Produtos Estrangeiros ou Serviços - PIS/PASEP-Importação e a Contribuição Social para o Financiamento da Seguridade Social devida pelo Importador de Bens Estrangeiros ou Serviços do Exterior - COFINS-Importação, com base nos arts. 149, § 2º, inciso II, e 195, inciso IV, da Constituição Federal, observado o disposto no seu art. 195, § 6º.
§ 1º Os serviços a que se refere o caput deste artigo são os provenientes do exterior prestados por pessoa física ou pessoa jurídica residente ou domiciliada no exterior, nas seguintes hipóteses:
I - executados no País; ou
II - executados no exterior, cujo resultado se verifique no País.

6. CONCLUSÃO

A lei brasileira não veda expressamente o compartilhamento de dados com o objetivo de obter vantagem econômica, salvo quando se tratar do compartilhamento de dados sensíveis referentes à saúde ou outros dados sensíveis conforme futuramente deverá ser regulamentado pela autoridade nacional. Logo, a LGPD, em regra, permite a venda de tais informações, inclusive em operações de exportação ou importação.

Para fins fiscais, parece ser mais adequada a exigência do ISS sobre as operações de fornecimento de dados, não do ICMS, tendo em vista a previsão da LC 116/03 e a tendência mais recente do STF sobre o conceito de prestação de serviços. Além disso, existem diversos argumentos que afastam a possibilidade de incidência do ICMS, sobretudo a evidente inconstitucionalidade do Convênio ICMS nº 106/17.

Seguindo a linha do enquadramento como serviço, no caso de importações de dados também haveria pagamento do imposto de renda retido na fonte em relação aos valores remetidos ao exterior e do PIS/COFINS, com risco de cobrança também da CIDE, tendo em vista a possibilidade de a RFB enquadrar a operação como serviço técnico.

Em suma, o compartilhamento oneroso de dados pessoais tem sido uma operação cada vez mais comum com o desenvolvimento da economia digital, o que incontestavelmente estimula a tributação dessas atividades. Considerando ainda todas as incertezas envolvendo a legislação tributária brasileira, independentemente dos comentários apresentados no presente estudo, é necessário aguardar quais serão os entendimentos das autoridades fiscais sobre o tema e seus respectivos reflexos para os contribuintes, para compreendermos as implicações que decorrerão efetivamente das referidas operações.

TRATAMENTO DE DADOS SEM CONSENTIMENTO DO TITULAR

Por

LUDMILA ALBUQUERQUE KNOP HAUER

Advogada senior manager da área de Cível Empresarial do escritório Gaia Silva Gaede Advogados em Curitiba

Pós-graduada em Processo Civil – Instituto Romeu Bacelar – PR

Advogada graduada pela Pontifícia Universidade Católica do Paraná – PUC/PR.

LUCAS A. BOHUN

Advogado da área de Cível Empresarial do escritório Gaia Silva Gaede Advogados em Curitiba

Pós-graduando em Processo Civil – Instituto Romeu Bacelar – PR

Advogado graduado pelo Centro Universitário Curitiba – UniCuritiba.

A Lei de Proteção Geral de Dados (LGPD)[1] estabeleceu regras para tratamento e compartilhamento de dados pessoais, sejam eletrônicos ou físicos, objetivando a proteção dos direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural[2].

Ao fundamentar a proteção de dados, a LGPD faz clara referência aos princípios constitucionais[3], como por exemplo, respeito à privacidade, liberdade de expressão, inviolabilidade da intimidade e da honra, desenvolvimento econômico e tecnológico, bem como estabelece que o tratamento dos dados deverá observar a boa-fé e os princípios elencados no art. 6º da referida legislação[4].

1 Lei nº 13.709 de 2018

2 Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

3 Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

4 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Diante da amplitude da aplicabilidade da LGPD – qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, vinculada aos dados coletados, utilizados ou tratados em território nacional[5], faz-se necessário destacar alguns cuidados a serem adotados para o tratamento de dados, a fim de evitar o descumprimento da legislação e, consequentemente, sofrer uma punição.

Inicialmente, cumpre esclarecer que o tratamento de dados é restrito às hipóteses elencadas no art. 7º da LGPD, quais sejam:

1) fornecimento de consentimento pelo titular;

2) cumprimento de obrigação legal ou regulatória pelo controlador;

3) tratamento e uso compartilhado de dados necessários pela administração pública à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

4) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

5) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

6) exercício regular de direitos em processo judicial, administrativo ou

---

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

5 Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
I - a operação de tratamento seja realizada no território nacional;
II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

arbitral (nos termos da Lei de Arbitragem);

7) proteção da vida ou da incolumidade física do titular ou de terceiro;

8) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

9) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

10) proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Apesar da relevância destacada na legislação com relação à necessidade de consentimento do titular, expresso e determinado[6], para obtenção de dados, verifica-se que esta é apenas uma das dez hipóteses legais para tratamento de dados dos usuários. Ou seja, existe a possibilidade de dispensa do consentimento do titular para tratamento de dados em alguns casos.

Entre todas as hipóteses de tratamento sem o consentimento do titular, importante destacar a possibilidade de armazenamento, utilização, compartilhamento, distribuição ou qualquer ação com dados quando necessário para atender aos interesses legítimos do controlador[7] ou de terceiros, ressalvados os casos em que prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Ainda, outras duas hipóteses chamam a atenção: o "exercício regular de direitos em contrato, processo judicial, administrativo ou arbitral" e o "cumprimento de obrigação legal pelo controlador".

Entretanto, não há delimitação na LGPD sobre o conceito de "interesse legítimo" do controlador ou de terceiro e nem sobre os limites para tratamento de dados pautados no exercício regular de direitos ou no cumprimento de obrigação legal pelo controlador.

6 Art. 8º. (...) § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
7 Art. 5º. (...) VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Apesar de ainda não ter entendimento jurisprudencial sobre o assunto, o que ocorre em razão da LGDP não ter entrado em vigor, referida lacuna certamente será suprida por meio de interpretação judicial e/ou administrativa.

De todo modo, a partir da análise da LGPD como um todo, é possível estabelecer uma linha de interpretação de conduta a ser adotada em qualquer hipótese de tratamento de dados, para evitar o cometimento de alguma infração prevista na legislação em questão, que, inclusive, podem ser sancionadas com multa de até R$ 50.000.000,00 por infração[8].

Conforme destacado anteriormente, a LGPD fundamenta a proteção de dados com base em alguns princípios constitucionais, na boa-fé e nos princípios elencados no art. 6º, demonstrando que qualquer interpretação desta Lei estará pautada nesses pontos.

Um exemplo para essa interpretação é a limitação legal para tratamento de dados tornados manifestamente públicos pelo titular. Apesar da dispensa da exigência de consentimento nessa hipótese, o tratamento deve considerar a finalidade, a boa-fé, resguardados os direitos do titular e os princípios previstos na LGPD[9].

Além disso, o art. 7º, § 6º, da LGPD[10] estabelece que a eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

---

8 Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (...) II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

9 Art. 7º. (...) § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

10 Art. 7º. § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Ou seja, apesar da ausência de delimitação específica sobre o tratamento de dados pautados em algumas hipóteses em que não é essencial o consentimento do titular, qualquer conduta adotada pelo agente deverá levar em conta os princípios previstos na LGPD.

Portanto, a realização de tratamento de dados com finalidade específica, limitada ao mínimo necessário de informações, com utilização de medidas técnicas adequadas para proteção dos dados e evitando discriminação dos usuários e que estes sofram algum dano, praticamente minimizariam eventuais riscos de descumprimento da legislação.

SÃO PAULO
Rua da Quitanda, 126 - Centro
CEP: 01012-010 - São Paulo, SP
Tel.: +55 11 3797 7400

RIO DE JANEIRO
Av. Almirante Barroso 81 – 24º andar - Centro
Edifício Torre Almirante
CEP: 20031-004 - Rio de Janeiro, RJ
Tel.: +55 21 2506 0900

CURITIBA
Rua Eurípedes Garcez do Nascimento, 1281 - Ahú
CEP: 80540-280 - Curitiba, PR
Tel.: +55 41 3304 8800

BELO HORIZONTE
Av. do Contorno, 7.069 - salas 508 a 512
CEP: 30110-043 - Belo Horizonte, MG
Tel.: +55 31 2511 8060

BRASÍLIA
SRTVN Quadra 701, Edifício Centro Empresarial Norte
Salas 519, 521, 532 e 534 - Bloco A
CEP: 70719-903 - Brasília, DF

www.**gsga**.com.br