

3.1. Transferência internacional de dados.

A intenção do legislador brasileiro foi a de adotar as regras muito similares às aquelas do direito europeu, inclusive para que o Brasil passasse a apresentar cenário mais atrativo do ponto de vista comercial-regulatório ao setor da TIC (Tecnologia da Informação e Comunicação). De fato, o reconhecimento da União Europeia quanto ao quesito adequação em proteção de dados é cada vez mais buscado pelos países de relevante economia.

É de suma importância que as limitações para transferência internacional de dados não impactem de maneira irrazoável e injustificada a economia digital globalizada, pautada na descentralização da localização da informação.

É considerando todo o contexto dessa economia que devemos analisar, detidamente, cada um dos requisitos trazidos pela nossa legislação, os quais devem ser interpretados em harmonia com a realidade fática de fluxo globalizado de dados que vivemos na sociedade atual.

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

A redação do *caput* do art. 33 deixa claro que o legislador pretendeu restringir as hipóteses em que é permitida a transferência internacional de dados pessoais. Nesse sentido, a possibilidade de transferência internacional de dados é exceção à regra, somente admitida se cumprida uma das hipóteses taxativamente listadas nos incisos do art. 33.

Contudo, para correta interpretação das presentes disposições, essencial entender adequadamente o que configura uma atividade de transferência internacional sob a ótica da proteção de dados.

O primeiro ponto importante é entender que, pautando-se no melhor entendimento europeu sobre o tema, um simples acesso à aplicação de internet não deve ser considerado uma transferência internacional de dados, sob pena de banalizar a aplicação do conceito e transformar o regime jurídico especial da transferência internacional em geral, o que poderia culminar, inclusive, em uma potencial situação de desarmonia com as bases legais do art. 7º¹.

O professor Luis Fernando Prado Chaves ensina que:

“Como nos recorda o *Information Commissioner’s Office* (ICO), autoridade de proteção de dados do Reino Unido, não se deve confundir *transferência de dados* com *trânsito de dados*. Isso significar dizer, por exemplo, que, se para viabilizar a troca de e-mails entre diferentes áreas de uma organização 100% brasileira (no contexto de um tratamento de dados pessoais sujeito à LGPD), por uma questão meramente de infraestrutura tecnológica, dados pessoais transitam momentaneamente por um servidor localizado na Índia, tal atividade, por si só, não deveria ser considerada uma transferência internacional de dados àquele país.

Indo além, novamente traduzindo os entendimentos europeus do ICO à realidade brasileira, temos que o mero envio de dados pessoais por um controlador a seu próprio empregado localizado no exterior não deveria configurar transferência internacional de dados, enquanto que, por outro lado, a comunicação de dados (no âmbito internacional) ocorrida entre diferentes empresas de um mesmo grupo empresarial, indubitavelmente, entra na regra do regime especial criado pela legislação.”

Nesse sentido, são exemplos de atividades que, comumente, podem envolver transferência internacional de dados:

- a) compartilhamento de base de dados de RH entre empresas do mesmo grupo (matriz-filial);
- b) armazenamento de dados em *data centers* fisicamente localizados no exterior;
- c) terceirização do serviço de atendimento ao consumidor;

¹ CHAVES, Luis Fernando Prado. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019, p. 290.

d) contratação de provedor de computação em serviço de nuvem estrangeiro;

e) contratação de provedor de e-mail estrangeiro.

Para as ocasiões em que ocorre, do ponto de vista técnico-jurídico, transferência internacional de dados, deve-se observar, ao menos, um dos requisitos do regime especial trazido pelos incisos do art. 33.

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

Primeiramente, cumpre destacar que, para viabilizar a possibilidade de atendimento a esse requisito, a ANPD deverá analisar, com base nos critérios do art. 34, o nível de adequação de países estrangeiros.

A transferência a um desses países, reconhecidos como de nível adequado pela ANPD, afastará qualquer necessidade de cumprimento de qualquer outro requisito, estando, assim, justificada a transferência.

Adicionalmente, em relação à exata redação adotada, o próprio legislador explica que teve como intenção, no referido inciso, deixar claro que, além dos países, organismos internacionais (pessoas jurídicas de direito internacional público) que apresentem proteção adequada poderão receber dados protegidos pela LGPD de forma facilitada, pois se considera que tal comunicação é essencial para as atividades de entidades multilaterais.

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

- a) cláusulas contratuais específicas para determinada transferência;
- b) cláusulas-padrão contratuais;
- c) normas corporativas globais;
- d) selos, certificados e códigos de conduta regularmente emitidos.

As garantias listadas acima deverão ser objeto de explicação e chancela por parte da Autoridade Nacional. Por agora, é provável que a ANPD discipline o conteúdo mínimo e razoável das cláusulas relativas à transferência internacional de dados.

Relativamente ao item “d”, ainda seguindo o padrão europeu, a ideia do legislador foi de que exista, no Brasil, mecanismos de selos, certificados e códigos de conduta que, uma vez aprovados pela ANPD e adotados pela instituição estrangeira importadora dos dados sujeitos à LGPD, subsidiem, do ponto de vista legal, a transferência internacional de dados.

De maneira geral, uma das inerentes e principais preocupações sobre as garantias previstas neste inciso diz respeito ao tempo que a ANPD tomará para editar o teor das cláusulas padrão ou mesmo para chancelar cláusulas, selos, certificações e códigos de conduta. Nesse sentido, há de se ter cautela para que as regras de transferência internacional de dados previstas pela LGPD não se tornem obstáculo indesejado ao legítimo e necessário fluxo global de dados por inércia da ANPD².

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

O inciso acima garante que serviços de inteligência internacional, investigações e atividades de cooperação jurídica internacionais não serão inviabilizados pelas regras de restrição de transferência de dados. Some-se a essa disposição o entendimento de que a LGPD, em si, não se aplica às atividades que tenham como fim exclusivo: (i) segurança pública; (ii) defesa nacional; (iii) segurança do Estado; ou (iv) atividades de investigação e repressão de infrações penais, conforme redação do art. 4º, III.

² CHAVES, Luis Fernando Prado. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019, p. 290.

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

Como não poderia deixar de ser, o inciso IV existe para garantir a prevalência do direito à vida e da integridade física, o qual não pode ser mitigado por questões relativas à limitação do fluxo de dados pessoais.

V - quando a autoridade nacional autorizar a transferência;

Este inciso traz a possibilidade genérica de apreciação e consequente autorização, pela ANPD, de transferências específicas.

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

Semelhantemente ao que ocorre no inciso III, no inciso VI percebe-se a prevalência de acordos de cooperação internacional acerca dos limites para o fluxo de dados pessoais ao exterior.

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

De forma semelhante à base legal prevista no art. 7º, III, da Lei, o inciso VII prevê a hipótese da atividade da administração pública. Ponto de relevância é que a utilização da expressão “quando a transferência for necessária” obriga o dispositivo a ser interpretado de forma restrita e limitada.

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

Neste inciso, a LGPD consagra o consentimento específico e em destaque como alternativa para legitimar a transferência internacional de dados levada a efeito pelos agentes de tratamento de dados.

Sobre o tema, claras são as lições do professor Luis Fernando Prado Chaves³:

“O consentimento especial para transferência internacional de dados não é simples de ser obtido. Relembre-se que, nos termos do art. 5º, XII, o consentimento é considerado como tal caso seja consubstanciado por meio de uma “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. Aos adjetivos “livre”, “informado” e “inequívoco” se somam as categorizações “específico” e “em destaque”, o que, notavelmente, aumenta a necessidade de participação do titular dos dados para que o consentimento seja considerado válido.

Neste ponto, deve-se lembrar de que o consentimento na LGPD deve sempre ser “para uma finalidade determinada”. No entanto, está claro que, ao expandir os elementos do consentimento na disposição acima, o legislador trouxe à tona um consentimento especial, que deve apresentar nível de robustez proporcional ao risco, para o titular, de uma transferência de seus dados pessoais a país que não possui nível considerado adequado (e que esteja desacompanhada de robustas garantias contratuais que vincule a parte importadora dos dados).”

Para o Professor Bruno Bioni⁴, aqui não bastam cláusulas contratuais destacadas, devendo ser todo o processo de obtenção do consentimento específico e pontual, garantindo-se que a ação do titular em concordar seja *gritante*. Ainda, o meio de obtenção do consentimento, além de pontual e gritante, deve ser acompanhado de suficiente informação acerca do caráter internacional da operação de comunicação de dados, distinguindo a atividade de outras, inclusive de outros tipos de compartilhamento de dados.

³ CHAVES, Luis Fernando Prado. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019, p. 297.

⁴ BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2018. P. 202-203.

Assim, pode-se perceber que o consentimento especial para transferência internacional não se trata de uma via fácil para os controladores legitimarem o tratamento. O consentimento não poderá/deverá ser condição para fornecimento de bens, produtos ou serviços, e sempre quando da sua obtenção deverá haver a possibilidade de recusa pelo titular.

Pode-se concluir que na prática, ante as particularidades da atividade e dos requisitos legais para esse consentimento em específico, essa hipótese legal será preterida pelas demais, especialmente pelas garantias previstas no inciso II (que, na teoria, trazem menos riscos jurídicos aos próprios agentes de tratamento).

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

As hipóteses do art. 7º citadas por este inciso são: para o cumprimento de obrigação legal ou regulatória pelo controlador; quando necessário para execução do contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; e para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do [art. 1º da Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

O parágrafo único acima deve ser verificado sob duas óticas: (1) pessoas jurídicas de direito público (parágrafo único do art. 1º, da Lei de Acesso à Informação), que são órgãos públicos integrantes da Administração Direta dos Poderes Executivo, Legislativo, do Judiciário e do Ministério Público, e as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios; e (2) pessoas jurídicas de direito privado.

Em relação às primeiras, a normativa é expressa em referir que essas entidades poderão realizar provocação da ANPD para que realize avaliação do nível de proteção de dados pessoais de determinado país, que, se considerado adequado, dispensa a adoção de qualquer outra salvaguarda para legitimar a transferência internacional.

Relativamente às segundas entidades, deve-se realizar análise cautelosa do emprego do termo “responsáveis” utilizado pelo legislador, de modo que se torna imperioso realizar um retrospectivo histórico da legislação relativo aos projetos de LGPD, no intuito de alcançar o correto entendimento.

O Professo Luis Fernando Prado Chaves⁵ refere que:

“Quanto à segunda, há de se analisar com cautela o emprego do termo “responsáveis” pelo legislador, que demanda uma análise do histórico legislativo em relação aos Projetos de LGPD para se alcançar o correto entendimento. Em versões anteriores do Projeto de LGPD, o termo “responsáveis” designava a figura dos controladores.

Assim, parece certo que a vontade do legislador foi a de que não somente as pessoas jurídicas de direito público supramencionadas pudessem pleitear o exame de um nível de adequação, mas também quaisquer controladores (nesse inciso inapropriadamente denominados responsáveis) no âmbito de suas atividades.”

Diante desse cenário, pode-se referir que a LGPD possibilita às empresas privadas que provoquem a ANPD para que esta avalie o nível de adequação da proteção de dados pessoais dado por um país ou organismo internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

⁵ CHAVES, Luis Fernando Prado. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019, p. 301.

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

Os critérios de avaliação do nível de adequação de um país estrangeiro que devem ser adotados pela ANPD encontram clara inspiração nos dispositivos do GDPR. Segundo o legislador brasileiro, a intenção do art. 34 foi a de evidenciar a necessidade de se observar, no país de destino dos dados, “a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais”, atribuindo-se maior destaque, portanto, ao inciso V⁶.

A ANPD, por certo, não poderá apenas realizar uma análise fria e textual da legislação de proteção de dados do país terceiro, mas deverá observar, especialmente, se o país em análise possui formas e meios efetivos para tornar eficaz a sua legislação.

No entanto, a LGPD deixa de prever que a ANPD poderá revogar a decisão de reconhecimento do nível de adequação caso, em revisão dos fatores que devem ser levados em conta, o país anteriormente chancelado se mostre faltoso em relação aos requisitos impostos pelo art. 34. Nesse ponto, em homenagem ao princípio da legalidade que rege os atos praticados pelos entes da Administração Pública e considerando que os critérios aqui examinados estão atrelados a elementos dinâmicos e

⁶ CHAVES, Luis Fernando Prado. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019.

mutáveis, seria extremamente importante que a ANPD contasse com o subsídio legal para revisar ou mesmo revogar suas decisões de adequação, tal como previsto no direito europeu e de forma similar ao previsto no art. 35, § 4º da LGPD⁷.

Art. 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.

⁷ Idem.

O art. 35 prevê o dever da Autoridade em disciplinar questões relativas às cláusulas para transferência internacional de dados, normas corporativas globais adotadas por empresas multinacionais, bem como selos, certificados e códigos de conduta.

O § 1º define critérios a serem considerados pela ANPD, contudo vale destacar que são critérios genéricos, o que acaba possibilitando uma certa discricionariedade à Autoridade para definir o conteúdo das cláusulas padrão, bem como deliberar sobre as demais garantias previstas no já comentado art. 33, II.

O § 2º, por sua vez, garante à ANPD a possibilidade de solicitação de informações acerca da operação de tratamento que envolver transferência internacional, antes mesmo de deliberar sobre os documentos e cláusulas a ela submetidos. O § 3º inaugura a possibilidade de existir instituições certificadoras, que atuarão sob a fiscalização da ANPD, nos termos de regulamentação própria a ser editada, de modo que os atos praticados pelas certificadoras poderão ser objeto de revisão e/ou anulação, conforme disposto no § 4º.

Por fim, o § 5º dita que, para além de questões legais e contratuais, a Autoridade, ao decidir sobre a validade de uma transferência internacional baseada no inciso II, do art. 33, observará que não apenas o quanto garantido em contrato ou atestado por selos, certificados e códigos de conduta, mas também medidas técnicas organizacionais que efetivamente garantam a segurança dos dados protegidos pela LGPD e tratados no exterior.

Nesse sentido, ao fazer referência ao previsto nos §§ 1º e 2º do art. 46, referido dispositivo dispõe que deverão ser observados os padrões de segurança a serem estabelecidos via decreto regulamentador, bem como a máxima do *security by design*, regra pela qual as medidas técnicas e organizacionais de segurança devem ser observadas desde a fase de concepção do produto ou do serviço até a sua execução⁸.

⁸ CHAVES, Luis Fernando Prado. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019, p. 304.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

O art. 36 elenca que mudanças provocadas pelos agentes de tratamento nas garantias apresentadas (art. 33, II) deverão ser comunicadas à Autoridade, a qual possuirá o poder de revisão da nova garantia adotada, a fim de legitimar o tratamento.

3.2. Agentes de Tratamento.

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Relativamente à conformidade com a Legislação, recomenda-se aos agentes de tratamento manter o registro de operação de tratamento de dados pessoais, na medida em que o mapeamento dessas operações é imprescindível para mitigação dos riscos.

A menos que a ANPD venha dispor sobre parâmetros objetivos mínimos sobre os parâmetros de obrigatoriedade do registro de atividade de tratamento, é razoável recomendar aos agentes de tratamento que realizem todos os registros das suas atividades de tratamento, independentemente do tipo de dado pessoal tratado.

Adicionalmente, a lei brasileira reforça a necessidade do registro das operações de tratamento de dados que possuem como base legal o legítimo interesse, situação que pressupõe, além do registro, relatório específico de impacto, a teor do art. 10, § 3º, da LGPD.

De acordo com as melhores práticas, e com base no modelo europeu, que inspira a legislação brasileira, no caso do controlador, os registros das operações de tratamento de dados pessoais devem conter, minimamente, as seguintes informações⁹:

a) nome e contato do(s) responsável(eis) por cada atividade de tratamento de dados pessoais, do operador, se aplicável, e do encarregado pelo tratamento de dados pessoais;

b) as finalidades de cada atividade de tratamento de dados pessoais;

c) a descrição dos tipos de dados pessoais objeto do tratamento, assim como a descrição da categoria dos titulares daqueles dados pessoais;

d) a descrição dos terceiros com os quais aqueles dados pessoais foram ou serão compartilhados de qualquer forma, incluindo terceiros ou organizações localizadas em outros países;

e) se aplicável, no caso de transferência de dados pessoais para países estrangeiros ou organizações internacionais, a identificação desses países ou organizações, e, no caso das transferências sob o art. 33, inciso II, da LGPD, a documentação que demonstre garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD;

f) o prazo para a exclusão de cada categoria de dados pessoais objeto de tratamento, se possível; e

g) descrição das medidas técnicas organizacionais de seguranças referidas no art. 46 da LGPD, quando possível.

No caso de operadores de dados pessoais, estes deverão manter registros específicos para as atividades executadas por ordem de cada controlador, contendo, minimamente, as seguintes informações:

⁹ BRUNO, Marcos Gomes da Silva. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019.

a) nome e contato do(s) responsável(eis) por cada atividade de tratamento de dados pessoais, do controlador e do encarregado pelo tratamento de dados pessoais;

b) as categorias de dados pessoais tratados em nome de cada controlador;

c) se aplicável, no caso de transferência de dados pessoais para países estrangeiros ou organizações internacionais, a identificação desses países ou organizações e, no caso das transferências sob o art. 33, inciso II, da LGPD, a documentação que demonstre garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD;

d) descrição das medidas técnicas organizacionais de segurança referidas no art. 46 da LGPD, quando possível.

No que tange à forma como os registros devem ser efetuados, considerando o princípio da prestação de contas (art. 6º, inciso X), tais registros devem ser escritos, ainda que armazenados de forma eletrônica, uma vez que poderão ser requisitados pela ANPD, ou outras autoridades com poderes para tanto.

Finalmente, é importante destacar que os controladores deverão manter esses registros de suas atividades de tratamento sempre atualizados, de modo que as organizações deverão adotar políticas e processos para registrar toda nova operação de tratamento.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das

informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Sobre o tema, essencial trazer a doutrina do professor Marcos Bruno¹⁰:

“Conforme se depreende do art. 38 acima, caberá à ANPD estabelecer as situações em que o relatório de impacto à proteção de dados pessoais será recomendável, sendo certo que, independentemente dessa futura resolução da ANPD, a LGPD já sinaliza pela necessidade do relatório de impacto nas atividades que desenvolvem o tratamento de dados sensíveis, citado no *caput* do art. 38, bem como nas operações de tratamento de dados envolvendo legítimo interesse, a teor do art. 10, §3º, da LGPD.

Muito embora sejam similares o relatório de impacto com o registro de atividades, as finalidades são distintas. Enquanto o registro das atividades de tratamento de dados pessoais se presta a meramente documentar os processos ao tratamento dos dados pessoais, o relatório de impacto à proteção de dados pessoais apresenta um foco específico no mapeamento dos riscos decorrentes da atividade de tratamento de dados pessoais objeto do relatório.

Nesse sentido, a finalidade principal do relatório de impacto à proteção de dados pessoais é de apontar qualquer risco que possa advir daquela operação de tratamento de dados pessoais, e direcionar o controlador e/ou o operador à mitigação daqueles riscos mapeados.

Importante salientar que, do ponto de vista da proteção de dados pessoais, é recomendável a empresa conduzir a elaboração do relatório de impacto não apenas nas hipóteses em que a LGPD e o futuro regulamento exigem, mas em todas as situações em que possa antever risco aos titulares dos dados pessoais tratados. Trata-se de postura mais segura, e recomendável, notadamente em operações que possam envolver avaliações sistemáticas de aspectos pessoais, tratamento de dados pessoais em grande escala, decisões automatizadas com efeitos significantes, monitoramento automático, processamento de dados pessoais de titulares vulneráveis, limitação no exercício dos direitos dos titulares, entre outras operações onde o risco ao titular seja potencial.”

¹⁰ BRUNO, Marcos Gomes da Silva. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019. P. 307-308.

Diante dos ensinamentos, cumpre concluir que, se a organização não está de fato convicta quanto à necessidade de um relatório de impacto para determinada atividade de tratamento, recomenda-se, por cautela, fazê-lo, a fim de que sejam mitigados eventuais riscos e responsabilidades.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

O art. 39 esclarece que o operador somente poderá realizar o tratamento dos dados pessoais conforme as instruções apresentadas pelo controlador, sem, portanto, qualquer discricionariedade sua para realizar qualquer tipo de tratamento diverso daquele requerido pelo controlador.

Contudo, vale salientar que essa atuação em nome do controlador não exime o operador de adotar, independentemente das instruções do controlador, medidas para conformidade com a legislação de proteção de dados, bem como medidas técnicas e organizacionais de segurança referidas no art. 46 da LGPD. A disposição do art. 39 também é relevante considerando a possibilidade de responsabilização solidária do controlador, por falhas do operador, disposta no art. 42 da LGPD.

Diante desse panorama, não se pode ignorar o fato de que muitos incidentes relacionados a dados pessoais decorrem de falhas dos operadores, que agem em desacordo com as instruções dos controladores, o que, de fato, pode ser um fato que exime o controlador de responsabilidade por eventual incidente.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Sem dúvidas, o direito à portabilidade trata-se de novidade introduzida pela Legislação, seja em termos de garantir ao titular o controle sobre seus dados, seja para fazer a interseção com outras Leis.

Para que a portabilidade se torne realmente aplicável, é necessário estabelecer padrões e normativas. Relativamente a essa necessidade, o art. 40 prevê padrões de interoperabilidade para o exercício dos direitos dos titulares e tempo de guarda de registro, remetendo o assunto à futura regulamentação pela Autoridade.

O Professor Marcos Bruno¹¹ explica que:

“De fato, diversas dificuldades podem advir da garantia do exercício dos direitos dos titulares, onde se inclui a portabilidade e o livre acesso dos dados. A segurança mencionada no art. 40 é uma das primeiras preocupações do controlador, na medida em que qualquer sistema ou interface que permita acesso a dados pessoais deve ser revestido de camadas de segurança para inibir o acesso não autorizado aos dados pessoais lá disponibilizados.

No ato do exercício de qualquer direito do titular, o primeiro desafio do controlador é efetivamente identificar aquele titular que se apresenta e pede o exercício dos seus direitos, na medida em que a falha nessa identificação positiva da pessoa natural poderá acarretar um incidente de segurança relacionado a dados pessoais.”

Desafio posto aos controladores é o mapeamento do tempo de guarda dos dados pessoais tratados, de modo independente de qualquer pedido do titular nesse sentido. Recordar-se que o princípio da necessidade enseja ao controlador ter processos bem definidos de exclusão de dados pessoais, que devem ser de fato excluídos após o término do seu tratamento, como expresso pelo art. 16 da LGPD.

Complica-se mais a questão quando o titular solicita o exercício do direito de eliminação de seus dados pessoais, pois tal direito não pode ser absoluto, sendo possível a manutenção dos dados pessoais, mesmo com pedido expresso de eliminação pelo titular, quando, por exemplo, houver obrigação regulatória ou legal de guarda daqueles dados, entre outras situações que justifiquem a continuidade do armazenamento do dado pessoal objeto do pedido de eliminação, o que também deverá

¹¹ BRUNO, Marcos Gomes da Silva. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019. P. 311-312.

ser mapeado pela empresa em relação a todos os dados pessoais por ela tratados, de acordo com cada finalidade desse tratamento¹².

Adicionalmente, a portabilidade tem contornos com a responsabilidade dos agentes de tratamento dos dados pessoais. Isso porque, a partir do momento em que o dado pessoal é portado de um controlador para o outro, ele pode deixar de existir junto ao controlador que enviou o dado, transferindo a responsabilidade, naquele mesmo ato, ao controlador que recebeu o dado. Por outro lado, o exercício do direito à portabilidade é independente de outros direitos do titular do dado pessoal, e não necessariamente pressupõe essa exclusão automática dos dados pelo controlador que os enviou, que continua autorizado a observar os seus prazos mínimos e justificativas para retenção do dado, mesmo além da vontade do titular. Esse fato também reforça a necessidade de padrões dessa interoperabilidade, para que se estabeleça, fielmente, o momento dessa transferência da responsabilidade¹³.

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

¹² BRUNO, Marcos Gomes da Silva. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019. P. 313.

¹³ Idem.

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

§ 4º (VETADO).

A LGPD prevê a obrigatoriedade da figura do encarregado pelo tratamento de dados pessoais (DPO). Contudo, diferentemente da GDPR, a LGPD não estabeleceu critérios objetivos para a nomeação dessa figura, tarefa que ficará a cargo da ANPD.

A primeira questão a ser pontuada é a análise de quem está legalmente obrigado a nomear o Encarregado, o que se dá pela análise das orientações e resoluções expedidas pela ANPD, conforme previsto no § 3º, do art. 41, da LGPD.

A análise quanto à obrigatoriedade ou não da organização em nomear um Encarregado deverá ser devidamente documentada, visando a possibilitar a demonstração de que tudo que era relevante foi considerado para aquela decisão, em observância ao princípio da prestação de contas. Essa documentação poderá ser solicitada pela ANPD, e deverá ser atualizada sempre que necessário, sobretudo quando a empresa lançar produtos ou serviços que importem em novos tratamentos de dados pessoais.

A empresa poderá optar em nomear o Encarregado de forma voluntária, ainda que a conclusão seja o contrário, de que o Encarregado não seja obrigatório para aquela determinada organização.

Por oportuno, importante pontuar que o fato de a organização não designar um Encarregado pelo tratamento de dados pessoais, por entender desnecessária a função, não desobriga do cumprimento das obrigações previstas na LGPD, muito menos exime a organização de alocar seu pessoal ou consultores externos em assuntos relacionados à proteção de dados pessoais, situação em que o conflito de interesses, comentado mais adiante, também deverá ser evitado¹⁴.

Chegando à conclusão pela obrigatoriedade da nomeação de um Encarregado em sua estrutura, ou optando voluntariamente por essa nomeação, a empresa necessita verificar as funções que serão exercidas por esse colaborador, o perfil do profissional e sua posição dentro da estrutura organizacional da empresa.

As funções do Encarregado estão estabelecidas de forma cristalina no § 2º, do art. 41 da LGPD, mas não se trata de uma relação exaustiva.

No que se refere à responsabilidade do Encarregado pelo Tratamento de Dados Pessoais em face de uma eventual não conformidade da empresa com requisitos de proteção de dados, como regra geral, esta inexistente. O Encarregado não é pessoalmente responsável, pois o controlador e o operador são responsáveis por garantir e demonstrar que suas atividades são conduzidas de acordo com a regulamentação, de modo que a conformidade com a legislação aplicável à proteção de dados pessoais é uma responsabilidade do controlador e do operador, e não do Encarregado¹⁵.

Contudo, é evidente que quando houver dolo no agir do Encarregado, este poderá responder perante o empregador e até mesmo em face de terceiros.

Por fim, cabe destacar que a LGPD não veda a contratação de um Encarregado terceirizado, popularmente conhecido na Europa como *DPO as a service*, onde novamente todas as recomendações anteriores se aplicam, em especial a garantia da ausência de conflito de interesses.

¹⁴ BRUNO, Marcos Gomes da Silva. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019. P. 315.

¹⁵ Idem.

3.3. Autoridade Nacional de Proteção de Dados – ANPD.

Igualmente importante a existência de leis e regulamentações, imprescindível saber a maneira institucional pela qual as normativas se farão respeitadas e aplicadas. Para esse fim, restou aprovada a Autoridade Nacional de Proteção de Dados – ANPD.

Não existe qualquer órgão de proteção de dados no Brasil. Contudo, países europeus, como França, Alemanha e Reino Unido, possuem modelos já consolidados, que se mostram essenciais para garantir a harmonia na interpretação das leis que versam sobre dados pessoais e sua efetiva aplicação.

O presente cenário é de assimetria informacional, o qual exige que sejam estabelecidos órgãos que visem promover o equilíbrio na relação entre os titulares dos dados e os agentes, bem como fomentem uma cultura mais informada e centrada na proteção de dados e na Segurança da Informação.

Acerca da importância da ANPD, destaca-se, desde já, que ela pode estabelecer regulamentos específicos para setores que lidam com grandes volumes de dados, inclusive sensíveis, e proporcionar flexibilizações pontuais, a depender do poderio e da estrutura dos responsáveis pelo tratamento, visando, em contrapartida, estimular a inovação e novos modelos de negócios. A mais: será órgão competente para regular diversas disposições legais e desenhar com maior precisão os deveres dos agentes, como, por exemplo, a base legal do interesse legítimo e o relatório de impacto.

O que, de fato, podemos esperar da futura Autoridade Nacional de Proteção de Dados Brasileira? a) Especialização, consistência decisória e aprofundamento temático; b) Corpo técnico, multidisciplinar e intimamente afeto à temática; c) Independência funcional e autonomias administrativa, financeira e decisória; e d) Compromisso em promover a educação, a conscientização e a transparência no tratamento de dados, solicitando sugestões de melhoria e colaborando amplamente com as mais diversas partes interessadas, tratando os regulados como parceiros e não adversários.

O rol de competências da ANPD está delineado no art. 55-J, da LGPD:

Art. 55-J. Compete à ANPD:

I - zelar pela proteção dos dados pessoais, nos termos da legislação;

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a

natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;

XII - elaborar relatórios de gestão anuais acerca de suas atividades;

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da [Lei nº 10.741, de 1º de outubro de 2003 \(Estatuto do Idoso\)](#);

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

Como podemos perceber, o rol das atividades da Autoridade é bastante amplo. Contudo, até o presente momento (janeiro/2020) não houve qualquer movimentação significativa para sua real estruturação e funcionamento.

A aplicação das sanções previstas na LGPD compete exclusivamente à ANPD e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades e órgãos da administração pública.

A atribuição sancionatória é a mais tradicional de uma autoridade reguladora. Tal como bem definido na LGPD, em especial no Capítulo VIII (arts. 52-54), suas atribuições seriam receber e apurar denúncias, realizar o trabalho de fiscalização reativa e proativa de conformidade com a Lei, advertir organizações com requisições e prazos para conformidade, aplicar multas e requisitar o bloqueio ou eliminação dos dados pessoais da infração.

De acordo com o art. 52, os agentes de tratamento, em razão das infrações cometidas às normas previstas na LGPD, ficarão sujeitos às seguintes sanções administrativas:

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:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

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;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Claro que a aplicação das sanções não poderá ser de ofício, dependendo de procedimento administrativo que possibilite ampla defesa, e serão, também, aplicadas de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os parâmetros estabelecidos em lei, sendo importante destacar que as sanções estão previstas em rol taxativo e não exemplificativo.

Resumidamente, as condições regulatórias traçadas pela ANPD terão influência direta na maneira como as empresas brasileiras consomem serviços especializados e se diversificam, na forma como se inserem nas cadeias globais de valor

IMPACTA

e até nas exportações de serviços. Por isso, é muito importante que a futura ANPD tenha canais de diálogo permanente com as pastas responsáveis pelo desenvolvimento econômico e pela estratégia de transformação digital brasileira.