Rio de Janeiro
Novembro, 2019

Transferência de dados entre Europa e Brasil:

Análise da Adequação da Legislação Brasileira

autor
Mario Viola

revisores
Priscilla Silva
Christian Perrone
Giovana Carneiro

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

ITS
Instituto
de Tecnologia
& Sociedade
do Rio

Sumário

Sumário interativo: clique para redirecionamento

Resumo Executivo

O foco de análise deste relatório é apresentar um exame comparativo entre entre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD) e o *General Data Protection Regulatio*n (GDPR)", de modo a avaliar se a legislação nacional assegura aos dados pessoais um grau de proteção compatível com o que é preconizado pela norma europeia e se tal compatibilidade seria, portanto, suficiente para autorizar a livre circulação de dados entre o Brasil e a União Europeia. Essa análise busca verificar se o novo marco legal brasileiro permite que o país seja reconhecido como um país apto a receber dados pessoais oriundos do bloco Europeu sem a necessidade de adoção de salvaguardas adicionais, já que caso o país de destino dos dados não seja reconhecido como detentor de um nível adequado de proteção de dados na forma como estabelece o GDPR, salvaguardas adicionais são exigidas pela referida norma, tais como: *i) regras vinculativas aplicáveis a empresas, ii) uso de cláusulas contratuais padrão aprovadas pela Comissão Europeia; iii) Código de Conduta aprovado também na forma do GDPR; ou iv) a utilização de algum processo de certificação igualmente aprovado na forma do GDPR*[1]. A exigência de salvaguardas adicionais acaba por gerar custos adicionais para países não considerados adequados em relação àqueles que já possuem esta qualificação. Assim, se torna essencial compreender se a LGPD apresenta ou não normas suficientemente protetivas para assegurar que o Brasil seja considerado um local seguro em termos de proteção de dados pessoais e possa integrar o ecossistema de transferência de dados com os países europeus.

A questão é de suma importância, pois estima-se que as exportações brasileiras para o bloco tenham somado US$ 42 bilhões no último ano (2018)[2], para as quais o fluxo de dados pessoais é quase pressuposto. Assegurar um ecossistema de proteção de dados pessoais efetivo e saudável no Brasil tem consequência direta na esfera política, social, econômica do país além do impacto positivo na perspectiva internacional, num momento em que o país busca ingressar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

O Relatório apresenta como se dá o procedimento de decisão de adequação à luz do GDPR, bem como possíveis entraves no caso brasileiro, comparando-o com sistemas semelhantes que têm demonstrado resultados positivos: Argentina e Uruguai. Por fim, analisa diferentes caminhos para que seja reconhecido, no Brasil, um grau adequado de proteção de dados pessoais, garantindo, assim, um ambiente seguro para o fluxo internacional desses dados, destacando-se a importância de uma Autoridade Nacional de Proteção de Dados (ANPD) independente.

1. Introdução

A discussão sobre proteção de dados pessoais ganhou muita relevância nas últimas décadas, principalmente a partir das impactantes transformações advindas dos avanços tecnológicos, que trouxeram como consequência o imediatismo na transmissão de informações e o aumento no volume de dados em circulação. Para dimensionar a grandeza do que vem ocorrendo, basta mencionar as projeções que indicam que só no ano de 2022 o volume global de tráfego de dados na Internet poderá superar a soma dos últimos trinta anos[3].

Como bem pontuado pelo Senador Eduardo Gomes na justificação da proposta de emenda à Constituição para incluir a proteção de dados pessoais no rol de direitos fundamentais, *"o avanço da tecnologia, por um lado, oportuniza racionalização de negócios e da própria atividade econômica: pode gerar empregabilidade, prosperidade e maior qualidade de vida. Por outro lado, se mal utilizada ou se utilizada sem um filtro prévio moral e ético, pode causar prejuízos incomensuráveis aos cidadãos e à própria sociedade, dando margem, inclusive, à concentração de mercados."*[4]

Isso tornou imperativo o estabelecimento – em alguns casos o aperfeiçoamento – de um regramento legal sobre a matéria, não só com a finalidade de proteger a intimidade e a privacidade das pessoas naturais titulares dos dados, o que por si só já justificaria a medida[I], mas, também, para estipular critérios transparentes no uso dessas informações na exploração de atividades econômicas, uma vez que a informação se tornou um ativo imprescindível da nova ordem econômica vigente[5].

No caso da União Europeia, que contava desde o ano de 1995 com a Diretiva nº 95/46/CE do Parlamento Europeu e do Conselho da União Euro peia dispondo sobre a proteção de dados pessoais, houve a necessidade de aperfeiçoamento dessa normatização, pois embora reconhecidos como ainda apropriados os objetivos e os princípios nela contidos, vislumbrou-se a necessidade de uniformização das regras que deveriam viger dentro do bloco.[II]

I. "(...) tanto a privacidade quanto a inviolabilidade de sigilo de dados, inseridas no art. 5º da Constituição Federal, são uma peça fundante da própria cidadania, ao lado de outros direitos fundamentais ali expressos. O sigilo, nesse sentido, tem a ver com a segurança do cidadão, princípio cujo conteúdo valorativo diz respeito à exclusão do arbítrio, não só de parte da sociedade como sobretudo do Estado que só pode agir submisso à ordem normativa que o constitui. Nestes termos, a cidadania, exigência do princípio republicano, que a reclama como um a espécie de fundamento primeiro da vida política e, por conseqüência, do Estado, antecede o Estado, não sendo por ele instituída. É ela que constitui a distinção entre o público e o privado, sob pena de perversão da soberania popular (CF., art. Iº, parágrafo único). As competências estabelecidas e atribuídas ao Estado devem, pois, estar submetidas ao reconhecimento do indivíduo com o cidadão, cuja dignidade se corporifica em direitos fundamentais." (In, FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado, p. 457.)

II. "Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que *(cont.)*

Assim, em 15 de abril de 2016 foi aprovado o *General Data Protection Regulation* (GDPR), que revogou a Diretiva mencionada e criou uma robusta regulamentação aplicável dentro de todo o bloco europeu, com observância obrigatória por todos os Estados-Membros[III], sem necessidade de internalização em cada um deles[IV].

O Brasil, por sua vez, até então ainda não possuía uma legislação tratando especificamente da proteção de dados pessoais. Os dispositivos que versavam sobre o assunto estavam contidos em legislações esparsas e sem uma sistematização que seria recomendada em razão da importância e complexidade da matéria.

Essa lacuna, porém, restou recentemente superada, quando em 2018 – mesmo ano em que o GDPR entrou em vigor – foi aprovada a Lei nº 13.709, instituindo a Lei Geral de Proteção de Dados (LGPD), após análise de diferentes projetos e discussões no Congresso Nacional.

A legislação nacional, com inegável inspiração no modelo europeu, passou a conferir ao país um admirável arcabouço legal sobre proteção de dados pessoais, o que significa dizer que, a partir da entrada em vigor da LGPD, prevista para ocorrer em agosto de 2020, haverá no Brasil um consistente grau de tutela de nossas informações pessoais.

Tanto é verdade que no que toca às transferências internacionais de dados a lei brasileira acabou por conceber mecanismos de salvaguarda semelhantes àqueles adotados pelo GDPR para assegurar aos dados pessoais proteção para além dos limites de seus respectivos territórios.

Assim, o GDPR e a LGPD fixam rígidas regras para que os dados pessoais coletados em seus territórios possam circular internacionalmente, exigindo, cada qual com as suas particularidades, o cumprimento de determinados requisitos, vinculados à manutenção da proteção dessas informações no país estrangeiro, como condicionante para que seja autorizado o seu fluxo transfronteiriço.

---

subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrônica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades econômicas a nível da União, distorcer a concorrência e impedir as Autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE." (Considerando nº 9 do GDPR)

III. Isso não significa dizer que os Estados-Membros não poderão estipular em seus âmbitos internos regras próprias sobre a proteção de dados pessoais, apenas não poderão conferir proteção em grau menor do que o previsto no GDPR.

IV. Importante, destacar, contudo, que o GDPR deixou algum espaço para que os Estados-Membros regulassem alguns temas específicos de modo diferenciado por meio de legislação nacional.

Reside exatamente nesse ponto o foco de análise deste relatório, que pretende apresentar um exame da adequação da LGPD aos padrões exigidos pelo GDPR, de modo a avaliar se a legislação nacional assegura aos dados pessoais um grau de proteção compatível com o que é preconizado pela norma europeia e se tal compatibilidade seria, portanto, suficiente para autorizar a livre circulação de dados entre o Brasil e a União Europeia.

A questão da transferência internacional de dados entre Brasil e União Europeia é de suma importância, pois estima-se que as exportações brasileiras para o bloco tenham somado US$ 42 bilhões no último ano (2018), para as quais o fluxo de dados pessoais é quase pressuposto. Assegurar um ecossistema de proteção de dados pessoais efetivo e saudável no Brasil tem consequência direta na esfera política, social, econômica do país além do impacto positivo na perspectiva internacional, num momento em que o país busca ingressar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

2. Transferência Internacional de Dados entre o Brasil e União Européia: Relevância Social e Econômica

É evidente que a circulação de dados pessoais entre Brasil e União Europeia já ocorre hoje em dia, ainda que não exista a "livre circulação" decorrente de processo de adequação. Entretanto, para que de dados pessoais oriundos da União Europeia possam ser transferidos para o Brasil, o GDPR — e mesmo anterior Diretiva Europeia 46 de 1995 — exige que sejam colocadas em prática garantias adicionais com vistas a assegurar um adequada proteção dos dados pessoais nas transferências que forem realizadas. Essas salvaguardas estão previstas no artigo 46 do GDPR e compreendem:

Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos;

a. Regras vinculativas aplicáveis às empresas;
b. Cláusulas-tipo de proteção de dados adotadas pela Comissão;
c. Cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão;
d. Adoção de um código de conduta acompanhado compromissos vinculativos e força executiva pelos controladores ou subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas;
e. Um procedimento de certificação igualmente aprovado nos termos do GDPR, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas.

Essas garantias adicionais, evidentemente, acabam por aumentar os custos e criar entraves para a circulação de dados entre a União Europeia e o Brasil, podendo impactar, inclusive, serviços que poderiam ser prestados por empresas brasileiras a empresas da União Europeia, já que o custo da transferência de dados para o Brasil, por conta da necessidade de adoção de arranjos contratuais ou mesmo submissão a processos de certificação por parte da empresa brasileira, acabam por deixar tais empresas menos atrativas, do ponto de vista da proteção de dados pessoais, que empresas situadas em países que já contam com o reconhecimento do Comissão Europeia como sendo possuidores de um nível adequado de proteção de dados pessoais, o que é o caso de países vizinhos ao Brasil (Argentina e Uruguai), cuja experiência será igualmente objeto de análise neste relatório.

O objetivo deste relatório, portanto, é analisar se a LGPD dispõe de mecanismos protetivos equivalentes aos estatuídos pelo regulamento europeu, o que poderá outorgar ao Brasil, à luz dos critérios contidos no GDPR, autorização para receber dados pessoais procedentes da União Europeia, sem que haja necessidade de o controlador responsável pelo tratamento dos dados ter que oferecer garantias contratuais, equiparando o país, para fins de circulação de dados pessoais, aos países do próprio bloco econômico e àqueles países terceiros que já contam com o status de adequado[V].

Não se trata, evidentemente, de submeter a legislação brasileira a qualquer tipo de crivo de conveniência externa, o que atentaria inclusive contra a soberania nacional. Um dos propósitos deste relatório é identificar se a legislação nacional, que vigerá independentemente de chancela de entes internacionais, é adequada, segundo a ótica do regulamento da União Europeia, para conferir ao Brasil o reconhecimento de ser um destino seguro para que seja realizado o tratamento de dados pessoais procedentes do bloco europeu.

V. "Na falta de uma decisão sobre o nível de proteção adequado, o responsável pelo tratamento ou o subcontratante deverá adotar as medidas necessárias para colmatar a insuficiência da proteção de dados no país terceiro dando para tal garantias adequadas ao titular dos dados. Tais garantias adequadas podem consistir no recurso a regras vinculativas aplicáveis às empresas, cláusulas-tipo de proteção de dados adotadas pela Comissão, cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo, ou cláusulas contratuais autorizadas por esta Autoridade. Essas medidas deverão assegurar o cumprimento dos requisitos relativos à proteção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento no território da União, incluindo a existência de direitos do titular de dados e de medidas jurídicas corretivas eficazes, nomeadamente o direito de recurso administrativo ou judicial e de exigir indenização, quer no território da União quer num país terceiro. Deverão estar relacionadas, em especial, com o respeito pelos princípios gerais relativos ao tratamento de dados pessoais e pelos princípios de proteção de dados desde a conceção e por defeito. Também podem ser efetuadas transferências por Autoridades ou organismos públicos para Autoridades ou organismos públicos em países terceiros ou para organizações internacionais que tenham deveres e funções correspondentes, nomeadamente com base em disposições a inserir no regime administrativo, como seja um memorando de entendimento, que prevejam a existência de direitos efetivos e oponíveis dos titulares dos dados. Deverá ser obtida a autorização da Autoridade de controlo competente quando as garantias previstas em regimes administrativos não forem juridicamente vinculativas." (Considerando nº 108 do GDPR)
"Não tendo sido tomada qualquer decisão nos termos do artigo 45º, nº 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes." (art. 46º, 1, do GDPR)

Pudessem os dados ser livremente transferidos da União Europeia para o exterior, sem a incidência de qualquer regra restritiva, certamente haveria a burla ao GDPR, pois bastaria que os dados fossem tratados em um país não integrante do bloco para que fosse possível fugir da incidência das regras protetivas nele previstas, fazendo com que se tornassem totalmente inócuas as garantias concedidas aos titulares dos dados.

Como a União Europeia reconhece a proteção dos dados pessoais como um direito fundamental da pessoa humana[VI], exige, como contrapartida à autorização da transferência dos dados pessoais para um país terceiro, que haja respeito a esse direito. É necessário que os dados pessoais permaneçam protegidos, considerando um nível de proteção simétrico ao estatuído pelo GDPR.

O país estrangeiro ou organismo internacional que pretender receber dados pessoais oriundos da União Europeia deverá demonstrar ser capaz de assegurar um nível de proteção reputado adequado, caso contrário aqueles entes públicos ou empresas que pretenderem transferir dados para o Brasil deverão demonstrar no caso concreto a adoção de uma das medidas de garantia previstas no artigo 46 do GPDR e já citados neste relatório.

O tema é importante porque o fluxo transfronteiriço de informações reflete na esfera política, social e é essencial para o desenvolvimento de diversas atividades econômicas, principalmente em razão do crescente número de empresas com atuação global, que necessitam da constante troca de informações para subsidiar a gestão eficaz de seus negócios[VII].

O próprio Considerando nº 101 do GDPR reconhece que *"a circulação de dados pessoais, com origem e destino quer a países não pertencentes à União quer a organizações internacionais, é necessária ao desenvolvimento do comércio e da cooperação internacionais[VIII]"*. Uma restrição absoluta à

VI. "Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito." (art. 8ª, 1, da Carta dos Direitos Fundamentais da União Europeia)

VII. *"Transborder data flows have become increasingly important in economic, political, and social terms over the thirty years since the adoption, in 1980, of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. A fundamental change in the business and technological environment for data processing is also taking place, driven by developments such as the increased globalisation of the world economy; the growing economic importance of data processing; the ubiquity of data transfers over the Internet; greater direct involvement of individuals in transborder data flows; the changing role of geography; and growing risks to the privacy of individuals. Despite these fundamental changes in the data processing landscape, and the growth in the regulation of transborder data flows in numerous countries, there has been little attempt so far to conduct a systematic inventory of such regulation at a global level; to examine the policies underlying it; and to consider whether those policies need to be re-evaluated."* (Kuner, C. (2011), "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", OECD Digital Economy Papers, No. 187, OECD Publishing). Disponível em http://www.kuner.com/my-publications-and-writing/untitled/kuner-oecd-tbdf-paper.pdf

VIII. "A circulação de dados pessoais, com origem e destino quer a países não pertencentes à União quer a organizações internacionais, é necessária ao desenvolvimento do comércio e da cooperação internacionais. O aumento dessa circulação criou novos desafios e novas preocupações em relação à proteção dos dados pessoais. Todavia, quando os dados pessoais *(cont.)*

circulação de informações poderia resultar na impossibilidade de concretização de diversos negócios, inviabilizando, inclusive, o cumprimento de tratados de cooperação internacional.

Mas, se por um lado deve ser compreendida a imperiosa necessidade de circulação internacional dos dados pessoais como um pressuposto de existência de uma economia que se apresenta cada dia mais globalizada, por outro é preciso reconhecer que assegurar um adequado grau de proteção a esses dados que serão objeto de transferência internacional é uma preocupação justificável e que existe antes mesmo das disposições do GDPR e da LGPD.

Desde 1980 a OCDE já havia publicado as suas diretrizes relativas à política internacional sobre a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais[6], o que demonstra que a preocupação com a proteção dos dados pessoais é algo que não reprime, ao revés, fomenta, o desenvolvimento de um ambiente econômico saudável.

Nesse sentido, é inegável o relevo da questão, pois eventual reconhecimento de que a LGPD garante ao Brasil um grau de proteção aos dados pessoais equivalente ao estatuído pelo GDPR, permitirá que haja o livre fluxo de dados com a União Europeia, com potencial impacto econômico positivo, já que a economia relacionada ao mercado de dados deverá representar 5,4% do PIB da União Europeia até o ano de 2025[7].

E a relevância do assunto poderá ser ainda maior caso venha a prosperar o recém anunciado Acordo de Associação Mercosul — União Europeia, que é baseado no *"diálogo político, cooperação e livre comércio"*[8].Ou seja, o fluxo de dados pessoais entre empresas e até mesmo entre os governos do Brasil e dos países da União Europeia será fundamental para permitir um pleno aproveitamento da abertura comercial que se avizinha.

Entretanto, mesmo o eventual (mas indesejado) insucesso na concretização do acordo entre o Bloco Sul-Americano e o Europeu não retirará do tema a importância que ele tem. Frisa-se as exportações brasileiras para a União Europeia somaram US$ 42 bilhões no último ano (2018), o que indica se tratar de um mercado proeminente, a merecer a devida atenção.

---

são transferidos da União para responsáveis pelo tratamento, para subcontratantes ou para outros destinatários em países terceiros ou para organizações internacionais, o nível de proteção das pessoas singulares assegurado na União pelo presente regulamento deverá continuar a ser garantido, inclusive nos casos de posterior transferência de dados pessoais do país terceiro ou da organização internacional em causa para responsáveis pelo tratamento, subcontratantes desse país terceiro ou de outro, ou para uma organização internacional. Em todo o caso, as transferências para países terceiros e organizações internacionais só podem ser efetuadas no pleno respeito pelo presente regulamento. Só poderão ser realizadas transferências se, sob reserva das demais disposições do presente regulamento, as condições constantes das disposições do presente regulamento relativas a transferências de dados pessoais para países terceiros e organizações internacionais forem cumpridas pelo responsável pelo tratamento ou subcontratante." (Considerando 101 do GDPR).

Os ganhos econômicos, todavia, não podem e não devem ser enxergados como o elemento principal dessa equação. Os benefícios de um ambiente seguro para o tratamento de dados pessoais significam a proteção do próprio ser humano, visto que *"a tutela jurídica da intimidade (e, também, da privacidade) constitui — qualquer que seja a dimensão em que se projete — uma das expressões mais significativas em que se pluralizam os direitos da personalidade"*[9].

Logo, obter o reconhecimento de adequação da LGPD ao GDPR é medida que poderá resultar em ganhos econômicos e sociais que não podem ser desprezados.

3. Decisão de Adequação: Equivalência do Grau de Proteção

A decisão de adequação, segundo o que se extrai da leitura do considerando nº 103 do GDPR[IX] e do seu artigo 45º, 1[X], nada mais é do que o reconhecimento pela Comissão da União Europeia de que um país terceiro ou organismo internacional assegura aos dados pessoais um nível de proteção compatível com aquele que é conferido pelo regulamento europeu.

Essa decisão, contudo, não pode e não deve ser tomada com base em subjetivismo. O GDPR indica quais os critérios que devem ser observados para que seja adotada uma decisão de adequação. Ao fazer esse julgamento, a Comissão, por imposição contida no artigo 45º, 2, do Regulamento, deverá avaliar a presença dos seguintes elementos:

f. Estado de Direito: O primado do Estado de Direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência;

IX. "A Comissão pode decidir, com efeitos no conjunto da União, que um país terceiro, um território ou um setor determinado de um país terceiro, ou uma organização internacional, oferece um nível adequado de proteção de dados adequado, garantindo assim a segurança jurídica e a uniformidade ao nível da União relativamente ao país terceiro ou à organização internacional que seja considerado apto a assegurar tal nível de proteção. Nestes casos, podem realizar-se transferências de dados pessoais para esse país ou organização internacional sem que para tal seja necessária mais nenhuma autorização. A Comissão pode igualmente decidir, após enviar ao país terceiro ou organização internacional uma notificação e uma declaração completa dos motivos, revogar essa decisão." (Considerando 103 do GDPR)**7** Isso não significa dizer que os Estados-Membros não poderão estipular em seus âmbitos internos regras próprias sobre a proteção de dados pessoais, apenas não poderão conferir proteção em grau menor do que o previsto no GDPR.

X. "Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica." (art. 45º, 1, do GDPR)

g. Autoridade de Controle Independente: A existência e o efetivo funcionamento de uma ou mais autoridades de controle independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e,
h. Compromissos Internacionais: Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais.

O grupo de trabalho do artigo 29[XI], em parecer no qual dá diretrizes para o processo de verificação da adequação do nível de proteção de dados de um país terceiro, já com base no que dispõe o GDPR, estabelece a necessidade de verificação da presença dos seguintes princípios e mecanismos básicos relativos ao conteúdo e aos requisitos processuais/de execução em matéria de proteção de dados para que o "selo" da adequação seja concedido a determinado país[10]:

1. **Conceitos:** Devem existir conceitos e/ou princípios básicos em matéria de proteção de dados;
2. **Fundamento para o tratamento lícito e leal para fins legítimos:** Os dados devem ser tratados de forma lícita, leal e legítima;
3. **Princípio da limitação da finalidade:** os dados devem ser tratados com uma finalidade específica e, subsequentemente, utilizados apenas na medida em que essa utilização não seja incompatível com a finalidade do tratamento;
4. **Princípio da qualidade e proporcionalidade:** os dados devem ser exatos e, quando necessário, objeto de atualização, além de deverem ser adequados, pertinentes e não excessivos relativamente às finalidades para que são tratados;
5. **Princípio da conservação:** regra geral, os dados não devem ser conservados mais tempo do que o necessário;

XI. O Grupo de Trabalho do Artigo 29.º (GT Art. 29.º) é o grupo de trabalho composto por representantes de autoridades de proteção de dados pessoais de todos os estados membros da União Europeia, que cuidava da interpretação de todas as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de entrada em vigor do GDPR), quando foi substituído pelo Comité Europeu para a Proteção de Dados (CEPD).

6. **Princípio da segurança e da confidencialidade:** qualquer entidade que proceda ao tratamento de dados pessoais deve assegurar que os dados são tratados de modo a garantir a sua segurança;
7. **Princípio da transparência:** todos os titulares devem ser informados de todos os principais elementos do tratamento dos seus dados pessoais de forma clara, facilmente acessível, concisa, transparente e inteligível;
8. **Direito de acesso, retificação, apagamento e oposição:** o titular dos dados deve ter o direito de obter confirmação do eventual tratamento dos dados que lhe dizem respeito, bem como de aceder a esses dados, obter sua retificação quando estes estiverem incorretos ou incompletos ou seu apagamento quando seu tratamento deixar de ser necessário ou for ilícito. Podem ainda se opor a tratamento de dados por motivos legítimos imperiosos relacionados com a sua situação particular;
9. **Restrições relativas a transferências subsequentes:** outras transferências dos dados pessoais por parte do destinatário inicial da transferência de dados original só devem ser permitidas se o destinatário seguinte também estiver sujeito a normas (incluindo normas contratuais) que garantam um nível de proteção adequado e seguir as instruções pertinentes aquando do tratamento de dados em nome do responsável pelo tratamento dos dados;
10. **Categorias especiais de dados:** Devem existir salvaguardas específicas aplicáveis a categorias especiais de dados (p. ex. dados relativos à saúde, opção sexual, crença religiosa, dentre outros);
11. **Comercialização Direta:** se os dados forem tratados para efeitos de comercialização direta, o titular deve poder opor-se sem qualquer custo ao tratamento dos dados para essa finalidade, em qualquer momento;
12. **Decisões automatizadas e definição de perfis:** as decisões baseadas unicamente no tratamento automatizado (decisões individuais automatizadas), incluindo definição de perfis, que produzem efeitos jurídicos ou afetam significativamente o titular dos dados, só podem ser tomadas nas condições fixadas no quadro normativo do país terceiro;
13. **Autoridade de controle competente e independente:** Deve existir uma ou mais autoridades de controle independentes, responsáveis pelo seguimento e por assegurar e aplicar a conformidade com as disposições de proteção de dados e privacidade no país terceiro;
14. **Responsabilização:** o quadro de proteção de dados do país terceiro deve obrigar os responsáveis pelo tratamento dos dados e/ou aqueles que tratam dados pessoais em seu nome a cumprir esse mesmo quadro e conseguir comprovar esse cumprimento;

15. **Apoio e ajuda destinada aos titulares de dados no exercício dos seus direitos e mecanismos de reparação adequados:** as pessoas singulares devem ter acesso a vias de recurso para fazer valer os seus direitos rápida e eficazmente, e sem custos proibitivos, bem como assegurar a conformidade[XII]; Sem necessidade de se ater à análise pormenorizada de cada um dos elementos prescritos no regulamento europeu para respaldar uma decisão de adequação, pode-se dizer que o Brasil, considerando o regime que vigorará com a LGPD, de uma maneira geral, atenderá aos requisitos para obter o reconhecimento de adequação[11] . Apesar de existirem algumas particularidades na referida lei, especialmente no que diz respeito à autoridade de controle (Autoridade Nacional de Proteção de Dados – ANPD), que são passíveis de crítica, é inegável que sob a sua égide o Brasil terá um elevado grau de proteção aos dados pessoais, principalmente quando comparado com o cenário existente anteriormente, no qual eram praticamente ausentes as regras acerca do tema. Com a nova legislação, o Brasil ingressa num seleto grupo de países que confere à proteção de dados pessoais a importância devida.

Todavia, conforme destacado, no que toca ao funcionamento da ANPD a LGPD parece não estar plenamente em conformidade com os parâmetros descritos no GDPR, nem, tampouco, nos requisitos elencados pelo Grupo do Artigo 29, que exigem a existência e o funcionamento de uma Autoridade de controle independente, isso porque após o veto presidencial aos dispositivos da LGPD que dispunham sobre a criação da ANPD, o que se justificou na alegação de inconstitucionalidade por vício de iniciativa, a estrutura administrativa da ANPD voltou a ser prevista como órgão integrante da Presidência da República por meio da Medida Provisória nº 869/18, convertida na Lei nº 13.853/2019[12]. O fato de a ANPD estar vinculada à administração direta atrai críticas no sentido de que esse órgão responsável pelo controle e fiscalização do cumprimento da lei de proteção de dados no Brasil pode não possuir a independência que seria esperada.

XII. No citado documento o Grupo do Trabalho do Artigo 29 resume as Garantias essenciais em países terceiros a quatro pontos principais: 1) O tratamento deve basear-se em regras claras, precisas e acessíveis (base jurídica); 2) A necessidade e a proporcionalidade relativamente aos objetivos legítimos prosseguidos devem ser demonstradas; 3) O tratamento tem de estar sujeito a supervisão independente; 4) Devem existir meios de recurso eficazes ao dispor das pessoas singulares. (Grupo de Trabalho do Artigo 29. Op. cit.).

Há, entretanto, a possibilidade de haver a correção de rumo, a fim de que a ANPD se torne um órgão independente, sem uma subordinação direta à Presidência da República, como, a propósito, projeta o §1º do artigo 55-A da LGPD, que indica ser transitória a natureza jurídica do órgão, o qual poderá ser transformado em entidade da administração pública federal indireta, de maneira vinculada, mas não integrante da Presidência da República.

Além disso, a legislação brasileira também fixou algumas salvaguardas que podem assegurar uma atuação independente da ANPD.

À ANPD foi assegurada autonomia técnica e decisória (artigo 55-B), o seu Conselho Diretor será composto por membros com mandato (artigo 55-D, §3º), escolhidos e nomeados pelo Presidente da República após a aprovação do Senado (artigo 55-D, §1º), que só perderão seus cargos em hipótese de renúncia, condenação judicial transitada em julgado ou pena de demissão aplicada em processo administrativo disciplinar (artigo 55-E).

Assim, como se verá no tópico seguinte, essa possível desconformidade referente à independência da ANPD não deve ser vista como um empecilho intransponível para que o Brasil obtenha o reconhecimento de adequação e possa ser destino dos dados pessoais vindos da União Europeia (efetivação do chamado *compliance*).

4. Casos Semelhantes no Uruguai: Possibilidade de um Acordo Bilateral

O GDPR assenta a existência e o efetivo funcionamento de uma Autoridade de controle independente como um dos elementos para o reconhecimento da adequação do grau de proteção de dados pessoais oferecido pelo país estrangeiro.

A independência da Autoridade de controle não deve, porém, ser analisada sob a ótica puramente formal. O que é preciso é existir um órgão que seja de fato independente, que possa servir para o indivíduo como um guardião dos seus direitos concernentes à proteção dos seus dados pessoais, sendo um anteparo contra possíveis violações, ainda que praticadas pelo próprio Estado. Não basta a legislação conter previsão de uma Autoridade independente se ela não o for no plano fático.

Existem exemplos de Autoridades Nacionais de proteção de dados pessoais que adotam (ou adotaram) modelo similar ao previsto na LGPD e que ainda assim foram reconhecidas como independentes e não se revelaram empecilhos para que os sistemas de proteção de dados de seus países fossem reconhecidos como adequados pela Comissão da União Europeia para fins de transferências internacionais de dados pessoais. São os casos da Argentina e do Uruguai.

A Argentina foi o segundo país fora do continente europeu a obter uma decisão de adequação (depois do Canadá, que, por sua vez, só recebeu a adequação com relação às regras relativas às organizações comerciais) e o primeiro país da América Latina a obter tal qualificação[XII]. À época em que a decisão de adequação foi adotada pela Comissão Europeia a Autoridade de proteção de dados da Argentina era a *Dirección Nacional de Protección de Datos Personales*, órgão vinculado à estrutura do então *Ministerio de Justicia, Seguridad y Derechos Humanos*, situação essa que permaneceu até sua incorporação pela Agencia de *Acceso a la Información Pública*, em 2017. Apesar disso, a União Europeia jamais reviu sua decisão quanto à adequação da normativa Argentina, mesmo diante das críticas quanto à real independência da DNPDP[13].

XII. Os Estados Unidos também foram objeto de uma decisão de adequação no ano 2000, mas apenas com relação às empresas que aderissem ao programa criado pelo acordo sobre o «Porto Seguro» (Safe harbour Agreement em inglês). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32000D0520&from=en

O Uruguai, por sua vez, conseguiu o reconhecimento da Comissão da União Europeia em 2012, com a aprovação de sua lei de proteção de dados pessoais e a criação da *Unidad Reguladora y de Control de Datos Personales* – URCDP, órgão desconcentrado da *Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento* - AGESIC, criado pela Lei nº 18.331 de 2008, que lhe atribuiu autonomia técnica, mesma expressão utilizada pelo artigo 55-B da LGPD. Além disso, o Uruguai foi o primeiro país não membro do Conselho da Europa a ratificar a Convenção nº 108 de 1981 para a proteção dos indivíduos com relação ao processamento automático de dados pessoais, ratificação essa que ocorreu em de 10 de abril de 2013, ou seja, após a decisão de adequação da Comissão Europeia, que ocorreu em 21 de agosto de 2012. A Convenção nº 108 foi o primeiro instrumento internacional vinculante aos estados que a ratificarem, trazendo em seu texto os princípios fundamentais da proteção de dados pessoais, tendo sido a grande fonte de inspiração para a normativa de proteção de dados da União Europeia.

Esses exemplos apontam para a possibilidade de o Brasil ser reconhecido pela União Europeia como um país com adequado grau de proteção de dados, a despeito do que se referiu anteriormente sobre a ausência de expressa previsão normativa quanto à independência da ANPD. E essa conclusão deriva não apenas da experiência da Argentina e do Uruguai, mas, também, da interpretação do próprio regulamento europeu.

O GDPR abre, portanto, a possibilidade de que os compromissos internacionais assumidos pelo país terceiro, ou mesmo sua participação em sistemas multilaterais ou regionais seja levado em consideração na avaliação da adequação, conforme previsto em seu considerando 105. Isso torna possível que o Brasil assegure a independência da ANPD via assunção de compromissos internacionais.

Os tratados e acordos internacionais celebrados pelo Brasil – e incorporados ao nosso ordenamento jurídico – quando não versam sobre Direitos Humanos adquirem o *status* de lei ordinária, conforme entendimento consolidado pelo Supremo Tribunal Federal[14]. Assim, um acordo celebrado pelo Brasil com a União Europeia no sentido de assegurar a independência da Autoridade Nacional de proteção de dados pessoais, ainda que vinculada à Presidência da República, teria força de lei.

Já existe inclusive "precedente" na experiência europeia com vistas à adoção de uma decisão sobre adequação em situação semelhante, que ocorreu com os Estados Unidos, cuja adequação (parcial, cumpre registrar) foi reconhecida em decorrência de um acordo internacional celebrado entre

aquele país e a União Europeia, recentemente revisto e conhecido com *Privacy Shield* (escudo de privacidade), no qual o Governo Americano acordou criar garantias adicionais para o tratamento de dados de cidadãos europeus nas hipóteses tratadas pelo acordo[15].

Como se não bastasse, a LGPD também prevê, em seus artigos 33 e 34, uma decisão de adequação relativa a um país (ou países) estrangeiro(s) por parte da Autoridade Nacional, o que importa dizer que a celebração de um acordo internacional entre o Brasil e a UE com vistas ao reconhecimento de adequação mútua facilitaria muito o fluxo de dados pessoais entre o Brasil e os países membros daquele bloco econômico e vice-versa, resolvendo eventuais dificuldades relativas a decisões isoladas sobre adequação (que no caso do Brasil deveriam se referir a cada um dos 28 Estados Membros da UE, o que provavelmente levaria muito tempo para ser alcançado). Essa, aliás, foi a opção adotada recentemente nas negociações concluídas entre a UE e o Japão para um reconhecimento de adequação recíproca.[16]

Importante salientar - para concluir - que o GDPR determina, ainda, que a Comissão Europeia monitore regularmente o nível de proteção de dados do país terceiro e que, dependendo do caso, poderá revogar, alterar ou suspender sua decisão que reconheceu a adequação de tal país. Esse mecanismo serve a impedir que um país, uma vez alcançando o reconhecimento pela União Europeia, deixe de continuar a assegurar um nível de proteção adequado. Isso, no caso de eventual acordo para reconhecimento recíproco entre UE e Brasil, serviria como uma garantia não apenas para que a ANDP tivesse a necessária independência como, também, para que a proteção dos dados pessoais fosse aplicada efetivamente no país.

Assim, parece haver caminhos para que o Brasil obtenha o “selo” de adequação junto à União Europeia, e que também outorgue o seu reconhecimento de adequação ao bloco europeu, tornando possível e juridicamente mais seguro o ambiente para o fluxo de dados pessoais.

5. Conclusão

Como se demonstrou, a transferência internacional de dados pessoais é tema que merece bastante atenção, especialmente na atualidade, em que um mero armazenamento de dados na nuvem – desde que envolva um servidor localizado no exterior – pode ser suficiente para configurar uma transmissão transfronteiriça, a exigir o cumprimento de diversas obrigações. E o assunto deve ser tratado com responsabilidade por envolver não só relevantes questões de ordem econômica, mas, também, por estar associado a um direito fundamental.

Como referido neste relatório, eventual reconhecimento do Brasil, pela União Europeia, como um país que possui mecanismos que asseguram um adequado grau de proteção aos dados pessoais poderá representar ganhos econômicos e sociais de significativa monta, pelo que se mostra recomendável que se postule a obtenção de uma decisão de adequação junto à Comissão da União Europeia.

E a despeito da aparente desconformidade que se apontou na LGPD ante o seu equivalente europeu, a experiência com outros países, especialmente com a Argentina e o Uruguai, demonstra que a mera ausência de previsão de independência formal da ANPD na nossa legislação não deve ser vista como uma barreira intransponível para que o Brasil seja reconhecido pela União Europeia como um país com adequado sistema de proteção de dados pessoais.

Ademais, há a possibilidade de o Brasil negociar um acordo bilateral com a União Europeia, de modo a assumir compromissos que assegurem a efetiva independência da ANPD. A partir do que se infere dos exemplos dos acordos firmados com os Estados Unidos e o Japão com o bloco europeu, a assunção de compromisso internacional pode ser um meio eficaz para ajustar eventuais desconformidades entre as legislações, o que permitiria um recíproco reconhecimento de adequação da LGPD ao GDPR e vice e versa.

O que é importante é que seja alcançado o reconhecimento de adequação da legislação nacional, mesmo que subsidiado a partir de um acordo bilateral, a fim de que seja construído um ambiente para que pessoas, empresas e governos do Brasil e dos Países-Membros da União Europeia possam transmitir dados pessoais de maneira juridicamente segura, servindo como um indutor do desenvolvimento.

Referências

1
Ver art. 46 do GDPR. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&-from=PT

2
Dados do Ministério da Economia do Brasil, disponível em: http://www.mdic.gov.br/index.php/micro-e-pequenas-empresa/61-noticias/3777-exportacoes--em-2018-alcancam-o--maior-valor-dos-ultimos-5-anos

3
ÉPOCA NEGÓCIOS. Por que a inovação será essencial para o mundo manter a conectividade. Editora Globo, 2019. Disponível em https://epocanegocios.globo.com/Tecnologia/noticia/2019/08/por-que-inovacao-sera-essencial-para-o-mundo-manter-conectividade.html

4
Texto da PEC nº 17/2019 disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1564052658918&disposition=inline

5
Disponível em http://www.oecd.org/sti/ieconomy/15590254.pdf

6
Disponível em http://www.oecd.org/sti/ieconomy/15590254.pdf

7
Disponível em https://europa.eu/rapid/press-release_IP-19-2749_pt.html

8
Disponível em http://www.itamaraty.gov.br/images/2019/2019_07_03_-_Resumo_Acordo_Mercosul_UE.pdf

9
Trecho do voto vencido proferido pelo eminente Ministro CELSO DE MELLO, do SUPREMO TRIBUNAL FEDERAL, no julgamento do RE 601.314/SP.

10
Grupo de Trabalho do Artigo 29. Documento de referência relativo à adequação. Disponível em https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

11
Nesse sentido são os artigos 5º, 11, 18, 20, 31, 32, 42, 43, 44 e 45 e os Capítulos V e X, todos da LGPD.

12
Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. (dispositivo introduzido na LGPD através da Lei nº 13.853/2019)

13
Ver DELGADO, Lucrecio Rebollo; SALTOR, Carlos Eduardo. El derecho a la protección de datos en España y Argentina: Orígenes y regulación vigente. Dykinson: Madrid, 2013. p. 159. 60 Decreto n. 899/2017. Disponível em espanhol em: https://libros--revistas-derecho.vlex.es/source/derecho-a-la-proteccion-de-datos-en-espa-a-y--argentina-origenes-y-regulacion-vigente

14
Ver a título ilustrativo os acórdãos dos Recursos Extraordinários 80.004/SE e 636.331./RJ.

15
EU-U.S. Privacy Shield. Disponível em https://iapp.org/media/pdf/resource_center/eu_us_privacy_shield_full_text.pdf.pdf

16
Comissão Europeia. Comunicado de imprensa: Fluxos internacionais de dados: Comissão lança o procedimento de adoção da sua decisão de adequação sobre o Japão. 5 de setembro de 2018. Disponível em http://europa.eu/rapid/press-release_IP-18-5433_pt.html

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

Acesse nossas redes

itsrio.org