Instituto de Referência em Internet e Sociedade

Policy Paper

Transferência Internacional de Dados no PL 5276/16

IRIS
Instituto de Referência em Internet e Sociedade

Instituto de Referência em Internet e Sociedade

Policy Paper

Transferência Internacional de Dados no PL 5276/16

Coordenação
Fabrício Bertini Pasquot Polido

Autores
Bruno Biazzatti
Bruno Tavares
Diego Machado
Lucas Anjos
Luíza Brandão
Matheus Rosa
Odélio Porto Júnior
Pedro Vilela
Tatiana Resende
Túlio Campos
Victor Vieira

Projeto gráfico
André Oliveira e Lucca Falbo

Capa
Freepik

Diagramação
André Oliveira

Produção Editorial
Instituto de Referência em Internet e Sociedade

Revisão
Lucas Costa dos Anjos

Finalização
André Oliveira

Como citar em ABNT
BIAZATTI, Bruno et al. Transferência Internacional de Dados no PL 5276/16. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2017. Disponível em: http://bit.ly/34YkcbZ. Acesso em: DD mmm. AAAA

SUMÁRIO

1. Sumário Executivo

O presente *policy paper* apresenta a contribuição do **Instituto de Referência em Internet e Sociedade - IRIS**, em parceria com **o Grupo de Estudos Internacionais em Internet, Inovação e Propriedade Intelectual – GNet** - da Universidade Federal de Minas Gerais (UFMG), sob a coordenação do Prof. Dr. Fabrício Bertini Pasquot Polido[1], para a discussão pública a respeito do Projeto de Lei nº 5276, sobre a proteção de dados pessoais no Brasil, ora em tramitação no Congresso Nacional, em regime de prioridade[2].

No ordenamento jurídico brasileiro, a proteção de dados pessoais é admitida como princípio relativo ao uso da Internet no Brasil, expressamente consagrado pela Lei nº 12.965, o Marco Civil da Internet. Reconhecido como legislação pioneira no mundo e exemplo do multissetorialismo que caracteriza a Governança da Internet[3], o Marco Civil estabeleceu, no artigo 3º, III, elaboração de lei específica para a proteção de dados. Nesse contexto, insere-se o PL 5276, enviado ao Congresso Nacional pela Presidência da República, no dia 13 de maio de 2016 e hoje aberto para procedimentos de consulta pública[4].

No âmbito do Poder Executivo, o então Anteprojeto de Lei sobre Proteção de Dados seguiu o modelo de consulta pública em que o Marco Civil foi baseado. O texto do Ministério da Justiça foi disponibilizado *online* e aberto a comentários de quaisquer usuários. Desse modo, tal qual no processo de elaboração do Marco Civil, viabilizou-se o debate entre múltiplos atores: membros da sociedade civil, academia, setores governamentais, regulatórios e empresas privadas[5].

De modo geral, o Projeto de Lei trata de temas como os direitos dos usuários e o tratamento, coleta e armazenamento de dados pessoais. Este estudo preliminar, contudo, concentrar-se-á na análise de questões materiais e procedimentais relativas ao Capítulo V, nomeadamente à **transferência internacional de dados e suas transações internacionais relacionadas**. O principal objetivo da presente intervenção é colaborar, científica e tecnicamente, para o processo legislativo envolvendo a elaboração de normas relacionadas à aplicação extraterritorial da lei brasileira e ao regime de proteção de dados pessoais, em particular aos impactos da discussão no Congresso Nacional sobre os atuais padrões de proteção em vigor.

O trabalho aqui desenvolvido, de forma independente e sem vinculação partidária no quadro congressual brasileiro, tem como premissa esclarecer ao público geral e aos parlamentares as questões legais e políticas decorrentes de relações jurídicas

1 Professor Adjunto de Direito Internacional da Faculdade de Direito da Universidade Federal de Minas Gerais – UFMG. Doutor em Direito Internacional pela Universidade de São Paulo. Pesquisador-Visitante no Instituto Max-Planck para Direito Internacional Privado e Comparado, Hamburgo. Membro da Associação Americana de Direito Internacional Privado. Fundador do Instituto de Referência em Internet e Sociedade-IRIS. Coordenador do Grupo de Estudos Internacionais de Internet, Inovação e Propriedade Intelectual-GNET, da Universidade Federal de Minas Gerais e do Projeto Governança Global da Internet e Sociedade do Conhecimento [Edital FAPEMIG-Demanda Universal 2015, Processo APQ-01604-15], do qual esse estudo também é produto de pesquisa derivado. E-mail: fpolido@ufmg.br. Contribuíram para este trabalho os pesquisadores Bruno Biazzatti, Bruno Tavares, Diego Machado, Lucas Anjos, Luíza Brandão, Matheus Rosa, Odélio Porto Júnior, Pedro Vilela, Tatiana Resende, Túlio Campos e Victor Vieira.

2 O processo legislativo pode ser acompanhado pelo link: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>.

3 Nesse sentido, ver SOUZA, Carlos Affonso Pereira; VIOLA, Mario; e LEMOS, Ronaldo. *Understanding Brazil's Internet Bill of Rights*. 1ª Ed. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2015. p.26.

4 Importante destacar que boa parte da análise aqui empreendida também se relaciona, quanto ao conteúdo, ao PL 4060/2012, de autoria do Dep. Milton Monti (PR/SP), de relativamente ao "tratamento de dados pessoais". O PL 4060/2012 encontra-se apensado ao PL 5276/2016 (conforme status do processo legislativo em agosto de 2016).

5 Cf. SOUZA, Carlos Affonso Pereira; VIOLA, Mario; e LEMOS, Ronaldo. *Understanding Brazil's Internet Bill of Rights.* p.37.

transfronteiriças envolvendo usuários de internet e a gestão de seus dados pessoais em escala global. A princípio, esta análise pode aparentar tratar de uma pequena parcela dentro do regime legal doméstico objetivado pelo PL 5276/2016. No entato, a convergência de temas relacionados ao fluxo e à transferência internacional de dados é muito sensível é muito sensível no cenário internacional e integra as discussões sobre jurisdição e governança da Internet[6].

A importância social e econômica da transferência internacional é reconhecida pelo volume de dados que circulam entre diferentes países, em todo o mundo[7]. Empresas multinacionais realizam coleta, tratamento e armazenamento de dados em diferentes jurisdições e, de acordo com sua atividade, procuram, para tanto, as formas e localidades mais eficientes e menos onerosas para a realização de suas atividades econômicas[8].

O tema da transferência internacional de dados também envolve os direitos dos usuários que, no contexto da Internet, começaram a ser delineados no Brasil pelo Marco Civil da Internet. Nesse sentido, qualquer lei ou regulamento que trate da proteção de dados pessoais e de sua transferência internacional, deve considerar o grande volume de informações relativos a indivíduos, organizações e empresas, ou por ela geradas. E ainda mais significativos serão os efeitos da transferência internacional de dados de usuários de internet, em inevitável trânsito entre fronteiras, sobre os modelos e *standards* de sua proteção em cada jurisdição, especialmente no que concerne à privacidade e à transparência dos mecanismos utilizados para "coleta, armazenamento e tratamento dos dados".

Para os autores deste estudo, trata-se de um excelente momento legislativo para reflexão sobre os distintos interesses em jogo: de um lado, de empresas, governos no tratamento desses dados; de outro, dos indivíduos, usuários de internet e titulares relativamente à proteção de informações pessoais que circulam entre distintos territórios, para além das fronteiras territoriais brasileiras.

Algumas perguntas devem ser assim formuladas: 1) Em que medida a regulamentação legal proposta para a transferência internacional de dados, desde a perspectiva brasileira no Projeto de Lei, compatibiliza-se com os padrões normativos e salvaguardas já estabelecidos pelo Marco Civil da Internet quanto aos direitos de usuários e as liberdades civis nas redes digitais? 2) Quais os limites técnicos, materiais e procedimentais impostos ao Poder Legislativo - em linha com as competências asseguradas pela Constituição de 1988, a legislação brasileira e normas internacionais aplicáveis - para a regulamentação desse tema em nível doméstico?

Este *policy paper* busca comentar, criticamente, o atual estado do Projeto de Lei, relacionando-o com aportes de especialistas e visões comparadas, para, ao final, oferecer recomendações de alterações quanto aos modelos adotados pela atual versão do texto.

6 A esse respeito, cf. apresentações reunidas nos Anais do I Seminário "Governança das Redes e o Marco Civil da Internet", sediado pela Universidade Federal de Minas Gerais em maio de 2015, organizadas por POLIDO, Fabrício B.P. e ROSINA, Monica S.G, *Governança das Redes e o Marco Civil da Internet: Liberdades, Privacidade e Democracia*. Belo Horizonte: Faculdade de Direito da UFMG, 2015. Disponível em: < http://www.direito.ufmg.br/gnet/ebooks/grmcivil.pdf>. Acesso em 15/07/2016.

7 KUNER, Christopher. Regulation of transborder data flows under data protection and privacy law: past, present, and future. *TILT Law & Technology Working Paper*, n. 016, 2010.p. 34-35.

8 WEBER, Rolf H. Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law,* p. 117 - 130, 2013. p.118

2. Relevância da discussão e metodologia de análise

A proposta de análise fornecida neste *policy paper* é desvinculada de qualquer interesse partidário, ou setorial, e se funda em duas premissas. A primeira é centrada na tentativa de esclarecer, aos parlamentares brasileiros, a importância, a sensibilidade e a vanguarda do tema da transferência internacional de dados de usuários de internet. A segunda diz respeito à necessidade de confronto (e encontro) entre os dispositivos da Lei nº 12.965/14 (Marco Civil da Internet) e do Projeto de Lei nº 5276/2016 que tocam, direta ou indiretamente, aspectos materiais e procedimentais da transferência internacional de dados.

a. Marco Civil da Internet - Artigo 11

> *Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.*
>
> § 1º *O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.*
>
> § 2º *O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.*
>
> § 3º *Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.*
>
> § 4º *Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.*

Enquanto tramita o Projeto de Lei nº 5276/2016 em regime de prioridade no Congresso Nacional, o Marco Civil da Internet apresenta-se como única lei infraconstitucional no Brasil estabelecendo dispositivos que tratam especificamente de dados pessoais nas redes. Na visão deste estudo, o Artigo 11 do Marco Civil relaciona-se a quatro aspectos relacionados à privacidade e à proteção de dados em casos de transferência internacional:

1) A **imperatividade das leis brasileiras** incidentes sobre quaisquer atos relacionados à transferência internacional de dados, nas situações em que pelo menos um deles se materialize, ou produza efeitos em território nacional, portanto conectado ou vinculado ao ordenamento brasileiro ("*qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional*"); aqui, poderíamos conceber um teste de "*compliance*" com as leis brasileiras;

2) Observância e respeito (*"enforcement"*) dos "*direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros"* por parte de provedores de conexão e de aplicações de internet;

3) Análise de condutas de empresas sediadas no estrangeiro relativamente à observância das leis brasileiras quando oferecem seus serviços de internet com contatos território nacional, mesmo que não possuam filial, ou subsidiária, sediada no Brasil (o que poderíamos de chamar de "*compliance digital*" ao direito brasileiro);

4) As expectativas legais e institucionais direcionadas a empresas, brasileiras ou estrangeiras, envolvidas com atividades relacionadas à coleta de dados, quanto à garantia de acesso, pelos usuários/clientes, a seus próprios dados pessoais armazenados no estrangeiro.

Com base na estrutura e alcance das regras contidas no Artigo 11 do Marco Civil, é importante analisar alguns elementos e funções do regime de proteção de dados pessoais em ambientes digitais, cotejando-os com as normas internacionais e internas de alguns países em visão comparada.

A Proteção de Dados em Escala Global e a Transferência Internacional de Dados

Em 1980, o Comitê de Ministros da *OCDE - Organização para a Cooperação e Desenvolvimento Económico* - publicou as "Diretrizes sobre Proteção da Privacidade e o Fluxo Transnacional de Informações Pessoais"[9], estabelecendo princípios básicos sobre proteção de dados e sobre a mobilidade de informações entre países com leis e regulamentos em conformidade com esses princípios.

As Diretrizes da OCDE de 1980, enquanto instrumentos não vinculantes (tendo um caráter de *soft law*, assim como outros instrumentos similares), não obrigam os Estados Membros, mas são suscetíveis a distintas modalidades de implementação ou internalização nos ordenamentos domésticos[10]. Durante a mesma década de publicação das Diretrizes da OCDE, contudo, os países parecem não ter recebido incentivos para adoção de leis e regulamentos internos para disciplinar a proteção de dados e aspectos da privacidade nos sistemas de comunicação então emergentes[11].

Pode-se dizer que a Diretiva 95/46/EC da União Europeia[12], de 1995, representou a primeira normativa de caráter supranacional referente à privacidade e a proteção de dados. Como consta no Artigo 1º, os Estados Membros da UE devem assegurar em suas legislações domésticas, seguindo os parâmetros da Diretiva, a proteção das liberdades e direitos fundamentais, especialmente à privacidade, no que tange aos dados pessoais.

9 OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Disponível em: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part3>. Acesso em 31 de maio de 2016.

10 Vale destacar, aqui, que o Brasil não é Membro da OCDE. No entanto, ele participa da organização na condição de parceiro convidado/observador. Em 2007, o Conselho da OCDE convidou a Secretaria a fortalecer as relações de cooperação com Brasil, Índia, República da China e África do Sul a partir dos programas de engajamento aperfeiçoado, com o que vem estimulando reformas estruturais e legais nos países. Na América Latina, somente Chile e México são Membros da OCDE.

11 Sobre as dificuldades de alcançar consenso sobre as leis de proteção de dados entre as décadas de 1970 e 1980 e múltiplos interesses dos segmentos da indústria de informática e comunicações, durante as negociações travadas na OCDE e nas Comunidade Econômicas Europeias, especificamente, ver COLE, Patrick E. "New Challenges to the US Multinational Corporation in the European Economic Community: Data Protection Laws", in *New York Univeirsity Journal of Int'l Law & Policy*, vol. 17, 1984, p. 893 e ss.

12 PARLAMENTO EUROPEU E CONSELHO, *Diretiva 95/46/CE*, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: < http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em 30 de maio de 2016. Vale observar, como será examinado, que a Diretiva foi revogada pelo Regulamento UE nº 2016/679, de 27 de abril de 2016.

A Diretiva UE nº 94/49 resultou de uma ofensiva das Comunidades Europeias, na década de 1990, para agressivamente regulamentar a proteção de dados pessoais[13], diferenciando-se da estratégia legislativa nos Estados Unidos da América de total absenteísmo nessa matéria. Ali, como sistematicamente observado pela literatura, imperou uma racionalidade liberal sobre o regime de tratamento dos dados por parte de empresas e associações, caracterizado por autorregulacão, sem interferência governamental, relegada a salvaguardas contratuais suscetíveis a barganha entre agentes econômicos e usuários[14].

Seria possível dizer que a Diretiva 94/46/EC, de 1995, da União Europeia, representou a primeira legislação supranacional a respeito de privacidade e proteção de dados. De acordo com seu artigo 1º, Estados Membros deveriam assegurar, em suas legislações domésticas e seguindo os parâmetros da Diretiva, a proteção de direitos e liberdades fundamentais, especialmente a privacidade de dados pessoais. Para fins de contextualização, a Diretiva 94/49 resultou de uma ofensiva pelas Comunidades Europeias nos anos 1990 para regular, de forma agressiva, a proteção de dados pessoais[15], o que difere da estratégia legislativa nos Estados Unidos, devido ao aparente absenteísmo nesse setor. O instrumento europeu inspirou-se em uma racionalidade liberal acerca da segurança jurídica para o tratamento e processamento de dados por companhias e associações, caracterizada pela autorregulação, sem interferência do governo. Além disso, a Diretiva previa um regime de segurança contratual sucetível a negociações entre agentes econômicos e usuários[16].

Em seu artigo 4º, a Diretiva 94/46 já oferecia uma solução para o "Direito Nacional Aplicável", prevendo, basicamente, que aqueles responsáveis pelo tratamento de dados pessoais dentro dos limites da União Europeia, mesmo que estrangeiros, deveriam se adequar à legislação dos Membros do bloco[17].

O próprio Marco Civil, seguindo essa racionalidade e o debate contemporâneo existente na Europa, introduziu uma regra muito semelhante no direito brasileiro, mantendo certo paralelismo com a fórmula empregada pela Diretiva Europeia. Isso porque, segundo a regra do artigo 11 do Marco Civil, empresas – nacionais ou estrangeiras - fornecedoras de serviço envolvendo coleta e tratamento de dados no Brasil devem respeitar a legislação local, em exata medida de observância (*"enforcement"*).

Entre 2008 e 2015, a União Europeia dedicou-se a atualizar a normativa comunitária, com o que o Parlamento e o Conselho chegaram ao importante **Regulamento nº 2016/679, de 27 de abril de 2016**, relativo à proteção de dados pessoais ("Regulamento da União Europeia sobre Proteção de Dados Pessoais"), e diretamente aplicável aos

13 Para comentários críticos sobre a Diretiva 95/46, em distintas perspectivas, cf. FROMHOLZ, Julia "The European Union data privacy directive", in *Berkeley technology law journal* vol.15, 2000, p. 461-484; WESTIN, Alan F. "Social and political dimensions of privacy." *Journal of social issues* vol 59, n.2, 2003, p. 431-453 e BIRNHACK, Michael D. "The EU data protection directive: an engine of a global regime", in: *Computer Law & Security Review,* vol. 24, n.6, 2008, p.508-520.

14 A esse respeito, Julia FROMHOLZ, Op.cit., p. 461-484, pp.462, observa: *"In the European Union , governments have moved aggressively to regulate the use of personal data. In the United States, on the other hand, the government has largely refrained from such regulation, instead allowing companies and associations to regulate themselves, save for a small number of narrowly drawn regulations targeting specific industries*".

15 Para uma análise crítica sobre a Directive 95/46, com a contraposição de diferentes perspectivas, veja FROMHOLZ, Julia "The European Union data privacy directive", in *Berkeley technology law journal* vol.15, 2000, p. 461-484; WESTIN, Alan F. "Social and political dimensions of privacy." *Journal of social issues* vol 59, n.2, 2003, p. 431-453 e BIRNHACK, Michael D. "The EU data protection directive: an engine of a global regime", in: *Computer Law & Security Review,* vol. 24, n.6, 2008, p.508-520.

16 A esse respeito, Julia FROMHOLZ, Op.cit., p. 461-484, p.462.

17 Importante destacar que, no sistema da União Europeia, as diretivas, ao contrário dos regulamentos que são diretamente aplicáveis, são destinadas para a aproximação e harmonização das leis nacionais. Da Diretiva da EU resultou um movimento de ajustamento das leis dos Membros criando regimes de proteção de dados, os quais variavam em certos aspectos. Apenas com a entrada em vigor do Regulamento 649 de 2016, um movimento de atualização a normativa europeia se completa.

sistemas jurídicos dos Membros a partir de 25 de maio de 2018[18]. Além de dispositivos sobre direitos de usuários aos seus dados pessoais, o Regulamento recém-promulgado prevê um bloco de regras sobre transferência de dados para "países terceiros" e organizações internacionais, estabelecendo mandato para a Comissão Europeia para monitorar o grau de proteção dado por determinado estado, território ou setor de processamento no estrangeiro para dados pessoais de usuários sediados em países da União Europeia. A medida de apreciação desse grau de proteção pode ser estabelecida, inclusive, segundo critérios objetivos, como salvaguardas (condições gerais de contratação, cláusulas de proteção de dados e regras empresariais vinculantes).

Nas justificativas de adoção do Regulamento, encontram-se expressas as preocupações e expectativas das instituições da UE quanto ao regime da transferência de dados, e que são muito significativos para o contexto brasileiro:

> "(101) 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 são transferidos da União para controladores, processadores, 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 mediante plena observação deste 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.
>
> (102) O presente regulamento não prejudica os acordos internacionais celebrados entre a União Europeia e países terceiros que regulem a transferência de dados pessoais, incluindo as garantias adequadas em benefício dos titulares dos dados. Os Estados-Membros poderão celebrar acordos internacionais que impliquem a transferência de dados pessoais para países terceiros ou organizações internacionais, desde que tais acordos não afetem o presente regulamento ou quaisquer outras disposições do direito da União e prevejam um nível adequado de proteção dos direitos fundamentais dos titulares dos dados.
>
> (103) 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"[19].

Com relação à disciplina das condutas de empresas – nacionais e estrangeiras – com atividades relacionadas à coleta de dados dos clientes, o Marco Civil da Internet foi, em seu artigo 11, § 3º, fortemente inspirado pela revogada Diretiva nº 94/46, tendo ambos aderido aos preceitos do direito de informação, pois pressupõem garantias aos usuários/clientes em relação ao acesso a seus próprios dados pessoais.

A Diretiva 94/46 estabelece, em seus artigos 10, 11 e 12, que aqueles que detêm dados pessoais, independente da forma como os tenham colhido, devem dispor

18 REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em:

19 Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>. Último acesso em 24.08.2016.

de mecanismos para que os indivíduos tenham acesso a tais dados, além de base para identificação do responsável pelo tratamento e finalidade da coleta de dados. É importante ressaltar, ainda, que a Diretiva 94/46/EC não estabelece como se processará a informação, deixando essa matéria a cargo da discricionariedade legal e administrativa dos Membros.

O surgimento de legislações estrangeiras para proteção de dados pessoais é recente, ainda que a preocupação provocada pelo tema remonte à década de 1970 nas Comunidades Europeias e OCDE. No plano do direito internacional, especificamente, ainda não existem tratados e convenções multilaterais sobre o tema.

A Organização dos Estados Americanos, de que o Brasil é Membro, tem se dedicado a explorar as questões normativas relativa à proteção de dados desde 1996, com mandato que prevê a elaboração de "estudo comparativo sobre os distintos regimes jurídicos, políticas e mecanismos de aplicação da proteção dos dados pessoais, incluindo legislação doméstica e autorregulacão, com vistas a explorar a possibilidade de um quadro normativo regional"[20]. Nesse mesmo sentido, o Departamento de Direito Internacional da OEA preparou o "Projeto de Princípios e Recomendações Preliminares sobre Proteção de Dados Pessoais", em que fica evidente a preocupação da organização de proteção do fluxo de informações e dados pessoais nas Américas[21].

No contexto latino-americano, a Argentina definiu normas de proteção de dados pessoais na Lei 25.326, de 2000[22]. Em seu artigo 44, a referida lei estabelece que, na hipótese de dados pessoais localizados em território argentino, os princípios gerais relativos à proteção, os direitos dos titulares dos dados, usuários e responsáveis por arquivos, registros e bancos de dados, bem como as sanções aplicadas, observarão exclusivamente o direito argentino. Nesse sentido, a fórmula empregada pela Lei 25.236 aproxima-se do Marco Civil, pois ela se baseia na aplicação imediata das normas argentinas para a proteção de dados pessoais que estiverem armazenados ou gerenciados em território argentino. Sob a perspectiva da técnica do direito internacional privado, ambas as soluções, aparentemente, estão baseadas na regra do conflito unilateral, segundo a qual o único direito aplicável, em termos de **respeito e observância da lei para todos os tipos de transações envolvendo dados**, é a **lei do foro** (*lex fori*).

A diferença, contudo, parece estar na aplicação extraterritorial das leis domésticas. O Marco Civil, em seu artigo 11, caput, expressamente autoriza a aplicação das leis brasileiras para regular atos de *"coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet"*, quando pelo menos um elemento de conexão com o ordenamento brasileiro seja identificado, em contato com o "território nacional".

Ainda no direito argentino, as formas pelas quais empresas estrangeiras realizam transferência internacional de dados é disciplinada pelo artigo 12 da Lei 25.326, que guarda semelhança com a revogada Diretiva 95/46/EC da União Europeia, uma vez que proíbe a transferência de dados pessoais de qualquer tipo com países ou órgão internacionais que não apresentam níveis de proteção adequados. Além disso, o dispositivo,

20 Cf. Resolução da Assembleia Geral nº 2661 da OEA (AG/RES. 2661, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES (Aprobada en la cuarta sesión plenaria , celebrada el 7 de junio de 2011), Disponível em: <http://www.oas.org/dil/esp/AG-RES_2661_XLI-O-11_esp.pdf>. Acesso em 15/07/16.

21 CP/CAJP-2921/10, *Proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos Personales*, 17 octobre de 2011. Disponível em: <http://www.oas.org/dil/esp/CP-CAJP-2921-10_rev1_corr1_esp.pdf>. Acesso em 15/07/16.

22 ARGENTINA. *Lei n. 25.326*, de 30 de outubro de 2000. Disponível em: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>. Acesso em 30 de maio de 2016.

assim como a Diretiva Europeia, também apresenta exceções em casos de cooperação jurídica internacional (administrativa e judicial), intercâmbio de dados médicos, transações bancárias, transferências que respeitem tratados do qual a Argentina faz parte, além de transferências de dados cujo objetivo é auxiliar na luta contra o crime organizado, o terrorismo e o narcotráfico.

Essa abordagem sobre a transferência internacional de dados, no direito argentino, parece consistente com os Princípios da OEA de 2011 sobre Proteção de Dados Pessoais, e se mostra elucidativa quanto à experiência brasileira de regulamentação por meio de lei específica. O Princípio 8º da OEA oferece **guia** para **elaboração e interpretação de normas relativas à proteção de dados** no contexto da transferência internacional. Para o propósito de análise do PL, ora em tramitação no Congresso Nacional, e seu confronto com a Constituição de 1988 e os princípios consagrados pelo Marco Civil sobre o uso da Internet no Brasil, é importante compreender o escopo e o alcance do Princípio 8º da OEA, bem como suas diretrizes aos legisladores e tribunais nacionais:

a) **natureza subsidiária das transferências internacionais de dados pessoais**: segundo o Princípio, elas devem apenas ser realizadas nas hipóteses de o exportador de dados assumir a responsabilidade subjetiva e objetiva pela proteção dos dados, ou quando o Estado da localização ou destino dos dados transferidos fornecer, minimamente, o mesmo padrão de proteção dos dados pessoais conferido pelos Princípios da OEA;

b) **obrigatoriedade de proteção material e procedimental dos dados pessoai**s, nos termos do item anterior, deve ser atendida pelo país de origem e país destino dos dados: países de trânsito dos dados (países pelos quais os dados passam, trafegam) não são obrigados a conferir proteção nesses moldes;

c) **a "proteção mínima" dos dados** é verificada a partir dos seguintes fatores: (i) a natureza dos dados; (ii) o país de origem; (iii) o país de recepção ou destino dos dados; (iv) finalidade do processamento dos dados transferidos: (v) existência e vigência das medidas de segurança para a transferência e tratamento de dados pessoais.

O Princípio 8º da OEA ressalva a possibilidade de realização de transferência internacional de dados ainda nos casos de o país de recepção ou destino não oferecer o mesmo nível de proteção que aquele assegurado pela normativa de seu país de origem. No entanto, essa transferência está sujeita a certas condições de processamento legal e justo, como forma de salvaguardar:

a) **obrigações de prestação de contas ("*accountability*") sobre os dados transferidos e armazenados**: incidentes na hipótese de as leis locais não preverem proteção aos dados importados e como imposição ao exportador – empresa responsável pela transferência - de assegurar a proteção de dados independentemente de sua localização geográfica (sede, domicílio) e possibilidade de oferecer provas suficientes da proteção quando lhe for requerido.

b) **garantia de proteção materializada por relação contratual entre partes**: essa condição sugere que os dados pessoais podem ser transferidos para um país receptor que não outorgue, minimamente, o mesmo padrão de proteção dos dados pessoais que aquele oferecido pelos Princípios, desde que exista cláusula contratual obrigando o exportador a conferir o mesmo nível de proteção dos dados.

c) **existência de leis permitindo a transferência internacional**: uma lei nacional pode permitir a transferência de dados pessoais a um terceiro Estado que não outorgue o mesmo padrão de proteção que aquele dos Princípios, se: i) a transferência de dados é necessária e em benefício da pessoa (titular dos dados) em uma relação contratual; ii) a transferência é necessária para proteção de interesses vitais, como o de evitar um dano substancial ou morte da pessoa ou de terceiros; ou iv) o exportador dos dados se responsabilizar pela proteção dos mesmos[23];

d) **consentimento**: pode-se admitir a transferência de dados pessoais a um país receptor que não outorgue o mesmo padrão de proteção, na hipótese de a pessoa afetada consentir inequivocamente quanto à transferência;

e) **inovação tecnológica**: as normas que regem a transferências de dados e informação entre países devem refletir a realidade manifesta no uso da Internet, além do dever de tomar em conta o fato de que as restrições à transferência de dados possa limitar a inovação tecnológica e o desenvolvimento econômica.

Há certo dissenso, entre os Membros da OEA, sobre os métodos de regulação de transferências internacionais, especificamente quanto à determinação de um conceito tão aberto como o da **proteção equivalente no país beneficiário**. Parecem existir dificuldades técnicas e normativas de implementação na prática e elas também foram objeto dos trabalhos de revisão da normativa europeia sobre proteção de dados, os quais resultaram no Regulamento UE n. 679 de 2016[24]. Por outro lado, os Princípios da OEA reconhecem que dados pessoais devam ser objeto de proteção no quadro das transferências internacionais, mas os Membros devem contar com certo grau de flexibilidade quanto às formas de proteção de alcançá-la[25]. Esse seria o caso das escolhas legislativas feitas em relação ao projeto de lei em discussão no Brasil.

Feito o exame preliminar sobre a situação da transferência internacional de dados e a proteção dos dados pessoais nos plano internacional e regional, é possível estabelecer uma **primeira conclusão de análise**:

Qualquer opção feita pelo legislador brasileiro deve ser, necessariamente, testada à luz de um princípio de conformidade do direito brasileiro às normas e diretrizes internacionais regulando o tema (a exemplo do Princípio 8º da OEA de 2011), além de experiências nacionais comparadas e regionais (como o caso da União Europeia).

Por que essa conclusão é relevante para o contexto em comento? Para os autores deste estudo, qualquer solução para regular os regimes legais envolvidos na transferência internacional de dados, desde uma perspectiva nacional/doméstica, não poderia prejudicar o entendimento sobre os padrões atualmente adotados sobre o tratamento dos dados pessoais. Ainda que os países não tenham, multilateralmente, alcançado consenso sobre as formas de proteção dos dados pessoais, por meio de tratados e convenções, ou sobre os mecanismos para assegurar, legal e contratualmente, padrões mínimos de segurança e privacidade no fluxo transfronteiriço de dados, os signatários da presente opinião entendem que os patamares mínimos já delineados devem ser re-

23 O Princípio 8º admite o caráter alternativo das condições para o caso de existência de leis permitindo transferência para um país (destino) que não outorgue mesmos padrões de proteção que aquele da normativa interamericana.

24 Processo que culminou na aprovação da *General Data Protection Regulation 2016/679.*

25 Cf. Artigo 8º dos Princípios de 2011.

speitados e rediscutidos, sempre em favor de um princípio que endosse um direito de acesso, pelos usuários, aos seus dados pessoais.

É justamente na interpretação favorável desse direito de acesso, também estampado no Marco Civil da Internet, que deve o legislador simular ou projetar os reflexos ou impactos sociais da futura lei objetivada, em benefício de uma harmonização que se projete globalmente.

b. Projeto de Lei Nº 5.276 - Capítulo V: "Transferência Internacional de Dados"

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

I - para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao desta Lei;

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

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

IV - quando o órgão competente autorizar a transferência;

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

VI - quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do art. 24.

VII - quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos.

Parágrafo único. O nível de proteção de dados do país será avaliado pelo órgão competente, que levará em conta:

I - normas gerais e setoriais da legislação em vigor no país de destino;

II - natureza dos dados;

III - observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

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

V - outras circunstâncias específicas relativas à transferência.

O artigo 33 do PL 5276 define as hipóteses em que a transferência internacional será permitida no Brasil. A seguir, apresenta-se a análise dos incisos que, caso sejam assim aprovados, representarão as possibilidades para a transmissão internacional de dados envolvendo partes relacionadas ao território brasileiro e a outros fatores de conexão:

I - para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao desta Lei;

O inciso I do artigo 33 inspira-se no critério geográfico definido na agora revogada Diretiva Europeia 95/46, de 1995[26], para a autorização à transferência internacional de dados. O modelo da antiga Diretiva leva em consideração os riscos potenciais a que os dados estarão submetidos nos países para os quais serão transferidos e, por isso, baseia-se na comparação entre os padrões domésticos de proteção[27].

A equiparação deve considerar o sistema de proteção de dados pessoais de cada país, conforme os parâmetros delineados no parágrafo único do artigo 33. De modo geral, o modelo geográfico concentra os critérios de equivalência e adequação que autorizam a transferência internacional no nível de proteção que cada país, em sua legislação doméstica e compromissos internacionais que assume, define para dados pessoais coletados, tratados e armazenados em seu território.

O modelo geográfico adotado em 1995 aplica-se ao sistema comunitário europeu, pois promove a harmonização das legislações nacionais a fim de garantir padrões de proteção equivalentes e, por consequência, viabilizar a transferência internacional de dados entre países do bloco e incentivá-la em detrimento de transferência a terceiros. O contexto de aplicação da Diretiva 95/46 não equivale à realidade brasileira e, portanto, a regra do inciso I do artigo 33 não deve ser automaticamente implantada no ordenamento doméstico, mas adaptada a uma conjuntura que não corresponde a de um direito comunitário.

A Diretiva Europeia, apesar de ter sido pioneira na definição das regras que disciplinam a transferência transnacional de dados pessoais, não está livre de críticas. O critério geográfico adotado – e que é reproduzido pelo artigo 33, I do PL 5276 - gera, como se verificou ao longo do tempo, diferentes níveis de "adequação de proteção" entre os países e, a despeito das outras hipóteses previstas pelo próprio sistema, tem por efeito a limitação dos processos de transferência internacional de dados[28]. Isso porque a comparação é estática e analisa apenas os padrões estatais de proteção, sem considerar, por exemplo, as providências da iniciativa privada para a proteção dos dados transferidos em nível internacional.

A exigência de proteção equivalente tem, ainda, como reflexo de sua rigidez, dúvidas acerca de sua eficácia[29]. Nesse sentido, a dificuldade de harmonização legislativa entre países diferentes, que não necessariamente pertençam à mesma comunidade, como os europeus, e a burocracia que caracteriza o procedimento de autorização de transferência transnacional podem gerar transferências ilegais, cujo controle, pelo volume,

26 O artigo 25 (1) da Diretiva Europeia 95/49 dispõe que: "Os Estados-membros estabelecerão que a transferência para um país terceiro de dados pessoais objeto de tratamento, ou que se destinem a ser objeto de tratamento após a sua transferência, só pode realizar-se se, sob reserva da observância das disposições nacionais adotadas nos termos das outras disposições da presente diretiva, o país terceiro em questão assegurar um *nível de proteção adequado.*" Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&qid=1465326802683&from=en>. Acesso em 07/06/2016.

27 WEBER observa que a comparação estabelecida no modelo geográfico manifesta-se pela qualificação dos níveis de proteção do país destinatário como "adequado", "similar"ou "igual". Cf.: WEBER, Op. cit., p.122. O PL utiliza a expressão "equiparável", que também revela a opção pelo modelo geográfico.

28 A recomendação, no plano internacional, é a de que a transferência seja a menos restrita possível, ainda que sejam definidos parâmetros de segurança e proteção de dados em cada país. Nesse sentido, manifesta-se a Organização para a Cooperação e Desenvolvimento Econômico, na Recomendação sobre Proteção da Privacidade e Transferência Internacional de Dados Pessoais, de 1980. O texto da Recomendação pode ser acessado em: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part3>. Acesso em 31 de maio de 2016.

29 KUNER, Christopher. Regulation of transborder data flows under data protection and privacy law: past, present, and future. *TILT Law & Technology Working Paper*, n. 016, 2010. p.28.

procedimento e destinação dos dados, podem não ser fiscalizadas ou coibidas pelos Estados que adotam o modelo geográfico. Observa-se, na União Europeia, autorizações às transferências em números significativamente inferiores e não correspondentes às transações econômicas e tecnológicas que os países europeus estabelecem com outros ao redor do mundo.[30]

A opção do legislador pela regra do artigo 33, I, baseada no artigo 25 (I) da Diretiva também deve considerar que o critério é custoso, tanto para o Estado, que deve manter estrutura de autorizações de transferência e fiscalização das operações transnacionais para garantir sua eficácia, quanto para os agentes econômicos que deverão requerer a permissão para transferir os dados. Assim, a experiência europeia revela que um sistema baseado na proteção equivalente e em autorizações recebidas, analisadas e proferidas por autoridade estatal implica em custos e dispêndio de tempo incompatível com a celeridade que caracteriza as operações da rede mundial de computadores.

> *II - quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;*

O artigo 33, inciso II rege a transferência internacional de informações para fins de investigações sendo conduzidas em outros Estados. O tópico é de grande relevância na atualidade e tem ensejado grande discussão nos fóruns internacionais. Por exemplo, durante o XII Congresso das Nações Unidas sobre a Prevenção ao Crime e Justiça Criminal, realizado em Salvador, em abril de 2010, adotou-se a *Declaração de Salvador sobre as Estratégias Abrangentes para os Desafios Globais: Prevenção de Crime e Sistemas de Justiça Criminal e seu Desenvolvimento num Mundo em Mudança*[31].

O parágrafo 15 dessa Declaração afirma que "[o]s Estados-Membros [da ONU] são incentivados a reforçar a cooperação internacional [no combate à fraude econômica e aos crimes de falsidade ideológica], incluindo por meio do intercâmbio de informações e práticas relevantes, bem como através de assistência técnica e jurídica".

Debates e avanços quanto à transferência de dados no contexto de investigações criminais também têm ocorrido entre a União Europeia (UE) e os Estados Unidos. Nesse sentido, essas duas entidades assinaram, em 2015, um *Umbrella Agreement*[32] a fim de estabelecer um conjunto unificado e abrangente de regras de proteção de dados a serem aplicadas às transferências transatlânticas de informações no âmbito da cooperação em assuntos criminais. A segurança dos dados é questão tão relevante aos europeus que a UE condicionou a sua assinatura ao Acordo de 2015 à adoção do *Judicial Redress Act*[33], pelo Congresso norte americano. De forma pioneira, essa lei estabelece um tratamento igualitário entre cidadãos dos Estados Unidos e da UE diante do *1974 U.S. Privacy Act*. O

Judicial Redress Act foi promulgado pelo Congresso Congresso norte americano em 10 de

30 Nesse sentido, KUNER, Op. cit., p. 28: "O fato de algumas das maiores economias no mundo (como China e Japão) não terem sido protagonistas de uma decisão formal da UE acerca de adequação significa que deve haver substancial desobediência, pelo menos no que tange à transferência de dados da EU para esses países." Tradução livre de: "The fact that some of the largest economies in the world (such as China and Japan) have not been the subject of a formal EU adequacy decision means that there must be substantial non-compliance at least with regard to data flows from the EU to those countries."

31 ONU, *Declaração de Salvador sobre as Estratégias Abrangentes para os Desafios Globais: Prevenção de Crime e Sistemas de Justiça Criminal e seu Desenvolvimento num Mundo em Mudança*. 2010. Disponível em: <http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/In-session/ACONF.213L6_Rev.2/V10529061A_CONF213_L6_REV2_S.pdf>. Acesso em 01 de junho de 2016.

32 EUA-UE,*Umbrella Agreement*. 2015. Disponível em: <http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm>. Acesso em 15 de junho de 2016.

33 EUA, *Judicial Redress Act,* 2015. Disponível em: <https://www.congress.gov/bill/114th-congress/house-bill/1428>. Acesso em 15 de junho de 2016.

fevereiro de 2016 e foi sancionado pelo Presidente Barack Obama em 24 de fevereiro desse ano[34].

Em relatório elaborado em Fevereiro pela Comissão Europeia[35], atestou-se que o *Umbrella Agreement* de 2015 é muito importante, porque estabelece padrões de processamento de dados, limitações ao uso das informações transferidas e o respeito aos direitos individuais. Um dos direitos garantidos é o acesso à justiça, de forma a permitir que os indivíduos contestem, perante autoridades judiciais, as decisões negando-lhes o acesso aos dados ou o direito de retificar informações incorretas. O direito ao recurso judicial também lhes permitirá exigir reparação por qualquer divulgação ilícita de informações[36].

Nesse contexto, o inciso II do artigo 33 encontra-se em harmonia com a tendência internacional de favorecer a cooperação jurídica entre diferentes países, garantindo a autorização para a transferência internacional de dados quando ela se dedique a esse propósito. Tendo em vista potenciais conflitos com as provisões existentes no Marco Civil da Internet e no Código de Processo Civil de 2015 (em particular o artigo 26, sobre os princípios acerca da cooperação internacional em litígios cíveis[37]). Seria recomendável que legisladores brasileiros incluíssem uma cláusula de salvaguarda no Projeto de Lei para garantias procedimentais e o devido processo legal, no que diz respeito à cooperação internacional na transferência de dados.

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

O inciso III autoriza o envio de dados para o exterior, a fim de proteger a vida ou a incolumidade física do titular ou de terceiros, ainda que o nível de proteção de dados do local de destino seja inferior ao brasileiro. Trata-se de dispositivo que visa tutelar diretamente a pessoa humana. Um exemplo que ilustra a importância desse inciso seria a transferência dos registros médicos, por autoridade de saúde brasileira, para um país onde um indivíduo sofreu um acidente ou adoeceu e seu histórico médico se faz necessário para decidir o tratamento clínico adequado. Sem esses dados, a vida do indivíduo estaria em sério risco. São dois os propósitos dessa provisão: primeiramente, ela atende a situações urgentes que demandam o tratamento excepcional do trânsito de dados pessoais; além disso, ela se refere a procedimentos expeditados e espontâneos de cooperação envolvendo a transferência de dados, particularmente em que pessoas físicas e jurídicas estão envolvidas em intensa mobilidade internacional.

A previsão do artigo 33, inciso III, também se encontra presente na Diretiva da União Europeia no. 2016/680, adotada em 27 de abril de 2016[38]. Nos termos do seu artigo 38, §1º, alínea "a", é possível transferir dados pessoais para um Estado que não

34 COMISSÃO EUROPEIA, *Transatlantic Data Flows: Restoring Trust through Strong Safeguards*,117 final, Brussels, 29 February 2016, Disponível em: <http://europa.eu/rapid/press-release_IP-16-433_en.htm>. Acesso em 15 de junho de 2016. p.11.

35 Idem.

36 Ibidem. p.12.

37 Art. 26. A cooperação jurídica internacional será regida por tratado de que o Brasil faz parte e observará: I - o respeito às garantias do devido processo legal no Estado requerente; II - a igualdade de tratamento entre nacionais e estrangeiros, residentes ou não no Brasil, em relação ao acesso à justiça e à tramitação dos processos, assegurando-se assistência judiciária aos necessitados; III - a publicidade processual, exceto nas hipóteses de sigilo previstas na legislação brasileira ou na do Estado requerente; IV - a existência de autoridade central para recepção e transmissão dos pedidos de cooperação; V - a espontaneidade na transmissão de informações a autoridades estrangeiras".

38 PARLAMENTO EUROPEU E CONSELHO, *Direita 2016/680*,de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L0680&from=PT>. Acesso em 15 de junho de 2016.

assegure um nível de proteção adequado quando essa transferência for necessária "[p]ara proteger os interesses vitais do titular dos dados ou de outra pessoa". A Diretiva da União Europeia no. 95/46/CE possui regime jurídico similar, pois em seu artigo 26º, §1º, alínea "e" autoriza a transferência internacional de dados quando "[...] necessária para proteger os interesses vitais da pessoa em causa".

Nota-se que as diretivas da União Europeia não especificam o que seriam os interesses vitais que justificam as transferências de dados. Em sentido contrário, o legislador brasileiro já determina, no próprio texto legal, que as transferências só podem ocorrer, com fulcro no artigo 33, inciso III, para proteger a vida e a integridade física do titular ou de terceiro. Segundo interpretação dada pela Unidade de Proteção de Dados do Diretório Geral da União Europeia para Justiça, Liberdade e Segurança, a expressão "interesses vitais", presente nas duas diretivas da União Europeia acima, diz respeito a emergências médicas sérias. [39] Assim, não parece haver divergência considerável entre o regime legal europeu e o brasileiro, no que diz respeito à regra sobre a transferência de dados para o propósito de proteção da vida e da integridade física de seu titular, ou de um terceiro.

A Irlanda, por sua vez, pelo Ato de Proteção de Dados de 2003 (*Data Protection Act 2003*)[40] expressamente autoriza a transferência internacional de dados para proteger não apenas a vida, mas também o patrimônio. Segundo o artigo 11, §4º, alínea "a" do referido Ato, transferências de dados para Estados sem um nível de proteção apropriado poderão ocorrer, desde que elas sejam necessárias "[...] para evitar ferimentos ou outros danos à saúde da pessoa interessada ou grave perda ou dano à sua propriedade ou para proteger os seus interesses vitais, e informar a pessoa interessada ou buscar o seu consentimento para a realização da transferência de dados seja susceptível de prejudicar os seus interesses vitais[41]".

A França, por outro lado, possui regime legal similar àquele que o Brasil pretende implementar. O artigo 6º, §2º, alínea "e" da Lei Federal de Proteção de Dados (*Loi Fédérale sur la Protection des Données*)[42] indica que as transferências de dados podem ocorrer quando "[...] necessári[as] para proteger a vida ou a integridade física da pessoa em causa". [43] Percebe-se que o texto legal desse dispositivo se assemelha muito ao inciso III do artigo 33.

Assim, o artigo 33, inciso III deve ser compreendido como um dispositivo necessário, cuja finalidade é proteger a vida e a integridade de brasileiros que se encontram em situação de perigo no exterior. Além disso, ele se alinha com instrumentos normativos estrangeiros e internacionais, em especial com as diretivas da União Europeia.

IV - quando o órgão competente autorizar a transferência;

Os casos de transferência internacional de dados que terão necessidade de uma

39 Directorate-General for Justice, Freedom and Security/Data Protection Unit. "*Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries*", p.53. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf>. Acesso em 02 de junho de 2016.

40 IRLANDA. *Data Protection Act*, 2003. Disponível em: <https://dataprotection.ie/viewdoc.asp?DocID=1467&ad=1>. Acesso em 15 de junho de 2016.

41 O texto original em inglês é: "*The transfer is necessary in order to prevent injury or other damage to the health of the data subject or serious loss or damage to property of the data subject or otherwise to protect his or her vital interests, and informing the data subject of, or seeking his or her consent to, the transfer is likely to damage his or her vital interests*".

42 FRANÇA. *Loi Fédérale sur la Protection des Données.* 1992. Disponível em: <https://www.admin.ch/opc/fr/classified-compilation/19920153/201401010000/235.1.pdf>. Acesso em 15 de junho de 2016.

43 O texto original em francês é: "la communication est, en l'espèce, nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée".

autorização prévia do órgão competente estão elencados no artigo 34 do PL nº 5.276. No mesmo dispositivo, encontram-se descritos os critérios para a autorização pelo ente competente.

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

O inciso V do artigo 33 afirma que o Brasil deverá transferir dados para outro Estado quando uma obrigação nesse sentido for contraída via tratado de cooperação internacional. Relevante destacar que, segundo o Supremo Tribunal Federal (STF), tratados possuem, como regra geral, o valor de lei ordinária no ordenamento jurídico pátrio. Apenas tratados sobre direitos humanos gozam de um regime jurídico específico[44]. Diante disso, os tratados de cooperação internacional ratificados pelo Brasil, em linhas gerais, possuem o valor de lei ordinária.

No cenário internacional referente às obrigações assumidas pelo Brasil, dois relevantes tratados impõem ao país o dever de transferir dados a outros Estados. O primeiro deles é a *Convenção das Nações Unidas contra o Crime Organizado Transnacional*[45]. O seu artigo 18, que regula a assistência judiciária recíproca, determina que "[o]s Estados Partes prestarão reciprocamente toda a assistência judiciária possível nas investigações, nos processos e em outros atos judiciais relativos às infrações previstas pela presente Convenção [...]". O artigo 18, § 3º expressamente menciona que essa cooperação judiciária recíproca pode ser solicitada para fornecer informações, elementos de prova e originais ou cópias autenticadas de documentos, incluindo documentos administrativos, bancários, financeiros ou comerciais e documentos de empresas.

Além disso, o artigo 18, § 2º aponta que a transferência de dados também deverá ocorrer quando o investigado ou processado for uma pessoa jurídica. Contudo, esse dispositivo determina que o envio de informações de pessoas coletivas só terá lugar na medida do que for permitido pelas "[...] leis, tratados, acordos e protocolos pertinentes do Estado Parte requerido [...]". Assim, a *Convenção das Nações Unidas contra o Crime Organizado Transnacional* expressamente permitiu que os Estados partes limitem a obrigação de fornecer dados de pessoas jurídicas, seja por meio de outro tratado ou por meio da promulgação de leis internas.

Por fim, o artigo 18, § 4º da Convenção apresenta a prerrogativa (não uma obrigação) aos Estados partes de transferir informações não solicitadas quando acreditarem que esses dados ajudarão na condução de investigações e processos penais em outros países. Segundo o dispositivo, sem prejuízo do seu direito interno, as autoridades competentes de um Estado Parte poderão, sem pedido prévio, comunicar informações relativas a questões penais a uma autoridade competente de outro Estado Parte, se considerarem que estas informações poderão ajudar a empreender ou concluir com êxito investigações e processos penais ou conduzir este último Estado Parte a formular um pedido ao abrigo da presente Convenção.

44 Nos termos do artigo 5º, § 3º da Constituição Federal de 1988, tratados relativos a direitos humanos aprovados, em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros, serão equivalentes às emendas constitucionais. Além disso, em 3 de dezembro de 2008, no julgamento do RE 466.343-SP e do HC 87.585-TO, o STF, adotando a tese proposta pelo Ministro Gilmar Mendes, determinou que tratados sobre direitos humanos que não foram aprovados com o quorum qualificado do artigo 5º, 3º, da Constituição terão status supralegal, ou seja, estarão hierarquicamente abaixo das normas constitucionais e acima das outras normas infraconstitucionais.

45 ONU. *Convenção das Nações Unidas contra o Crime Organizado Transnacional,* 2000.Disponível em: <https://www.unodc.org/lpo-brazil/pt/crime/marco-legal.html>. Acesso em 15 de junho de 2016.
A Covenção foi assinada pelo Brasil em 12 de dezembro de 2000, ratificada em 29 de janeiro de 2004 e incorporada ao Direito brasileiro pelo Decreto n. 5.015, de 2004, ano em que passou a vigorar para o país. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm>. Acessso em 15 de junho de 2016.

Outro tratado importante é a *Convenção das Nações Unidas contra a Corrupção*[46]. Nos termos do seu artigo 46, § 1º, "[o]s Estados Partes prestar-se-ão a mais ampla assistência judicial recíproca relativa a investigações, processos e ações judiciais relacionados com os delitos compreendidos na presente Convenção".

De forma análoga à *Convenção contra o Crime Organizado Transnacional*, a *Convenção contra a Corrupção* também apresenta uma lista ilustrativa de possíveis pedidos de assistência judicial. Entre os tópicos da lista. estão a apresentação de documentos judiciais, informações e elementos de prova e a entrega de documentos originais ou cópias certificadas, incluindo documentação pública, bancária e financeira, assim como a documentação social ou comercial de sociedades mercantis.

Outra semelhança com a *Convenção contra o Crime Organizado Transnacional* diz respeito à prerrogativa de encaminhar informações não requeridas por outros Estados, quando se entender que tais dados são relevantes às investigações ou ações judiciais no exterior[47]. Também se afirma que a transferência de informações de pessoas jurídicas ocorrerá "[...] no maior grau possível conforme as leis, tratados, acordos e declarações pertinentes do Estado Parte requerido"[48].

Os tratados existentes dos quais o Brasil é parte signatária, seja no nível bilateral ou multilateral, serão, igualmente, de grande importância para determinar o escopo preciso da aplicação das provisões do artigo 33, inciso V, do Projeto de Lei. Em resumo, qualquer relação entre transferência de dados, conforme entendimento estrito pelo Direito de Internet, e a cooperação jurídica internacional por meio de tratados e convenções específicas demandará uma abordagem equilibrada para a interpretação e aplicação dessa provisão legal nos tribunais brasileiros.

> *VI - quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do art. 24.*

O presente dispositivo autoriza a transferência internacional de dados no âmbito das atividades e funções do poder público, desde que a devida publicidade seja dada à transferência de dados pessoais em questão. Trata-se de previsão que busca definir margem de liberdade ao agente público, que pode decidir pela necessidade da transferência de dados, em consonância com os dois determinantes estipulados pela regra - o contexto de implementação de uma política pública e o cumprimento de obrigações legais.

Numa perspectiva jurídica comparada, percebe-se que a autorização para a realização de transferências internacionais de dados à luz do interesse público é cautelosa e restritiva. Na Suíça, o envio de dados para países que não oferecem o mínimo de garantias poderá ocorrer apenas quando for "indispensável para a proteção de um interesse público preponderante"[49].

46 ONU. *Convenção das Nações Unidas contra a Corrupção*, 2000. Disponível em: <https://www.unodc.org/lpo-brazil/pt/corrupcao/convencao.html>. Acesso em 16 de junho de 2016.
O tratado foi assinado pelo Brasil em 9 de dezembro de 2003 e ratificado em 15 de janeiro de 2005. Só entrou em força face ao Brasil em 14 de dezembro de 2005, sendo incorporado em nosso ordenamento pelo Decreto n. 5.687, de 31 de janeiro de 2006. .Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Decreto/D5687.htm>. Acesso em 16 de junho de 2016.

47 *Convenção das Nações Unidas contra a Corrupção*, artigo 46(4): "Sem menosprezo à legislação interna, as autoridades competentes de um Estado Parte poderão, sem que se lhes solicite previamente, transmitir informação relativa a questões penais a uma autoridade competente de outro Estado Parte se crêem que essa informação poderia ajudar a autoridade a empreender ou concluir com êxito indagações e processos penais ou poderia dar lugar a uma petição formulada por este último Estado Parte de acordo com a presente Convenção".

48 *Convenção das Nações Unidas contra a Corrupção*, artigo 46(2).

49 SUIÇA. *Loi fédérale sur la protection des données*, 1992. Disponível em: <https://www.admin.ch/opc/fr/classified-compilation/19920153/201401010000/235.1.pdf>. Acesso em 16 de junho de 2016. Artigo 6(2)(f). O texto original em francês é: "indispensable soit à la

Já a Diretiva da União Europeia no. 2016/680 afirma que essas transferências serão possíveis "a fim de evitar uma imediata e séria ameaça à segurança pública de um Estado Membro [da União Europeia] ou país terceiro"[50]. Esses dois instrumentos assentam que as transferências de dados para locais não seguros, a fim de proteger o interesse público, são medidas excepcionais.

Os Estados da América Latina também adotaram instrumentos legais restritivos nesse aspecto. A lei uruguaia permite a transferência quando "[...] seja necessária ou legalmente exigida para a proteção de um interesse público importante[51]. A Colômbia autoriza as transferências quando sejam "[...] legalmente exigidas para a proteção do interesse público"[52]. A Argentina, por sua vez, não possui uma exceção referente à salvaguarda do interesse público prevista em sua Lei de Proteção dos Dados Pessoais[53].

O regime do artigo 33, VI, por outro lado, torna as transferências de dados para locais não seguros uma parte integrante do funcionalismo público. Na conjuntura desse dispositivo legal, essas transferências poderão ser executadas sempre que a atribuição legal de serviço público ou a execução de política pública assim demandar, observada a publicidade da transferência.

Na verdade, esse dispositivo deveria prever, de forma expressa, que a sua aplicabilidade estaria limitada a interesses públicos relevantes e para assegurar o direito de indivíduos a opô-los diante da Administração Pública e de tribunais domésticos. Do contrário, as autoridades públicas poderiam realizar envios em massa de dados pessoais para locais não seguros, ameaçando a própria efetividade do artigo 33, inciso I. A intenção do artigo 33, inciso VI, não poderia ser uma "carta branca", nem uma forma de favorecer de forma desigual órgãos governamentais brasileiros. Ele parece representar mais uma obsessão pelo empoderamento do serviço público no Brasil, com várias preocupações relacionadas à coleta, ao gerenciamento e à transferência de dados.

> *VII - quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos.*

O inciso VII do artigo 33 do PL 5.276 trata do *consentimento*, que deve ser considerado de modo coerente com outros dispositivos do Projeto que versam sobre a necessidade do consentimento para coleta e tratamento de dados pessoais. Nesse sentido, o artigo 7º, define entre as condições para o tratamento dos dados, no inciso I, o consentimento "livre, informado e inequívoco". As três características são reafirmadas no artigo 9º, segundo o qual o consentimento deve ser disponibilizado por escrito ou por qualquer outro meio que o certifique. Finalmente, existe a exigência de consentimento com o tratamento de dados pessoais sensíveis, que segundo o artigo 11, inciso I, fica vedado caso ele não seja "livre, inequívoco, informado, expresso e específico pelo titular".

Ao observar os adjetivos vinculados ao termo, com destaque a "inequívoco" e "informado", afirma-se a preocupação do PL com as características necessárias aos termos

sauvegarde d'un intérêt public prépondérant".

50 *Diretiva no. 2016/680* artigo 38(1)(c). O texto original em inglês é: "*for the prevention of an immediate and serious threat to public security of a Member State or a third country*".

51 URUGUAI. *Ley 18.331 (Protección de datos personales y acción de 'habeas data'")*, 2008. Disponível em: <http://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n%C2%B0-18331-de-11-de-agosto-de-2008.html>. Acesso em 16 de junho de 2016. Artigo 23(5)(d). O texto original em espanhol é: "la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante"

52 COLOMBIA. *Ley Estatutaria no. 1581*, 2012. Disponível em: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>.Acesso em 15 de junho de 2016. Artigo 26(f). O texto original em espanhol é: "legalmente exigidas para la salvaguardia del interés público".

53 ARGENTINA. *Lei n. 25.326*, de 30 de outubro de 2000. Disponível em: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>. Acesso em 30 de maio de 2016. Artigo 12.

do consentimento de uso de dados. A premissa básica é que, contanto que todas as circunstâncias de uso e tratamento dos dados sejam bem explicadas, o usuário possuirá condições suficientes para autorizar ou não a cessão de suas informações pessoais.

Nesse sentido, é possível relacionar as disposições do PL com o consentimento segundo o modelo nomeado como "*transparency and choice*" (também chamado de *notice and consent* ou *informed consent*). Nesse sistema, a transparência pela parte que procura os dados daria condições para uma escolha clara e válida pela outra que os cede. Desse modo, admite-se que, conquanto todas as informações concernentes ao destino dos dados sejam fornecidas de forma transparente ao usuário, ele poderá tomar decisões conscientes de engajamento na concessão de suas informações. Esse processo informativo conferiria maior controle ao indivíduo e, por isso, garantiria sua proteção contra o mal-uso dos dados. Cabe destacar, também, que o modelo opta, na maioria das vezes, por uma adesão "tudo ou nada" (*"take it or leave it"*) do usuário - ou ele concorda com a transferência de dados com todas as ressalvas postuladas, ou rejeita o serviço completamente[54].

Apesar da aparência de adequação, o modelo do *transparency and choice*, na prática, apresenta algumas falhas. Isso porque as informações sobre o tratamento de dados são entregues ao usuário da rede por meio de documentos como os "Termos e Condições de Uso" e "Políticas de Privacidade". Tratam-se de textos volumosos e detalhados, com disposição em termos técnicos e que circulam na oferta da maioria de serviços *online*, a exemplo das redes sociais. Por essa razão, não se pode aceitar que o usuário apreenda todas as condições às quais seus dados serão submetidos. Aqui, o requisito não poderia ser satisfeito por meios operacionais, devido à falta ou à insuficiência de informações a respeito do tratamento de dados.

Faticamente, os "termos de uso", "termos de prestação de serviços" e "política de privacidade" são ignorados por usuários, criando o que é chamado de "paradoxo da transparência". Nesse sentido, o usuário, apesar de ter acesso às informações, em razão da complexidade, extensão e detalhamento dos termos, opta por ignorar as condições a que seus dados estarão submetidos[55], de modo que aceitar o termo não significa necessária consentimento livre, informado e manifesto, como exigem os dispositivos do PL n. 5276.

O sistema de transparência adotado no Projeto de Lei replica-se no que tange à transferência internacional de dados. Além dos critérios genéricos do consentimento, devem ser explicitados o caráter internacional do fluxo de informações, bem como seus riscos. A Diretiva Europeia 95/46, da mesma forma, adota o modelo do *transparency and choice*, pois, conforme dispõe o artigo 2º, h), o consentimento fica entendido como "qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita quais dados pessoais que lhe dizem respeito serão objeto de tratamento.". A Diretiva, ainda, em seu artigo 26, admite transferências entre países que não possuem o mesmo nível de proteção adequada, desde que se verifique consentimento inequívoco[56].

54 NISSENBAUM, Helen. A Contextual Approach to Privacy Online. *Daedalus, the Journal of the American Academy of Arts & Sciences*, v. 140, n. 4, p. 32, 2011. p. 34-35.

55 GEPI - Grupo de Ensino e Pesquisa em Inovação, FGV São Paulo. Contribuição ao Anteprojeto de Proteção de Dados Pessoais. São Paulo, p. 4-15, 2015. p. 5-6.

56 PARLAMENTO EUROPEU E CONSELHO, *Diretiva 95/46/CE*, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: < http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em 30 de maio de 2016.

Finalmente, ressalta-se que o tratamento dispensado pelo Projeto de Lei às formas de consentimento deve ser compreendido de acordo com os parâmetros definidos pelo Marco Civil da Internet. O Direito brasileiro segue o princípio pelo qual a lei especial derroga a lei geral (*lex specialis derrogat legi generali*). Sob essa hierarquia, as normas do Marco Civil prevaleceriam em todos os casos envolvendo consentimento na internet, mesmo que haja casos em que o modelo proposto pela Lei de Proteção de Dados seria mais adequado (i.e., temas envolvendo a proteção de dados e o consentimento online).

O parâmetro que embasa o conceito de consentimento dos artigos 7 e 9 e que envolve o controle dos dados pelo usuário por meio da informação, visa reduzir a assimetria de informação e poder econômico entre o consumidor e a entidade que coleta, trata e transfere os dados. O regime estabelecido pelo PL n. 5276 deve ser aplicado também à Transferência Internacional de Dados, especificamente na hipótese do inciso VII, que a autoriza quando com ela o usuário concordar.

> *Parágrafo único. O nível de proteção de dados do país será avaliado pelo órgão competente, que levará em conta:*
>
> *I - normas gerais e setoriais da legislação em vigor no país de destino;*
>
> *II - natureza dos dados;*
>
> *III - observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;*
>
> *IV - adoção de medidas de segurança previstas em regulamento; e*
>
> *V - outras circunstâncias específicas relativas à transferência.*

O parágrafo único do artigo 33 também se assemelha com os critérios utilizados na Diretiva 95/46 para avaliação do nível de proteção de um país externo à Área Econômica Europeia. O critério de verificação das normas gerais e setoriais, de natureza dos dados e de adoção medidas de segurança, estão expressos, nos mesmos termos, também no artigo 25, nº 2 da Diretiva.[57]

A nova regulação, GDPR 2016/679, expande o número de critérios para certificação de adequação. Primeiramente, os atores sujeitos à verificação de adequação podem ser países terceiros, seus territórios ou regiões específicas e organizações internacionais, conforme o artigo 45, nº1, GDPR. A análise do artigo 45, nº 2, GDPR[58] é expandida para um conceito que considera qual o real Estado de Direito da localidade para onde se transferem os dados, bem como o grau de respeito aos direitos humanos e às liberdades fundamentais. Além disso, a Comissão Europeia buscará verificar qual a efetiva aplicação das normas protetivas, por meio da análise dos mecanismos judiciários e administrativos disponíveis ao titular dos dados e da análise jurisprudencial local.

As normas relacionadas à segurança pública e defesa nacional, em consonância com o grau de acesso das autoridades públicas a dados pessoais, passam a figurar como critério importante de verificação. Essa recente preocupação provavelmente foi influen-

57 Diretiva 95/46/EU, artigo 25, nº 2: "A adequação do nível de protecção oferecido por um país terceiro será apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projectados, os países de origem e de destino final, as regras de direito, gerais ou sectoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país." Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&qid=1466131624407&from=EN>. Acessado em: 20/06/2016

58 General Data Protection Regulation 2016/679, artigo 45. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN>. Acessado em: 20/06/2016

ciada pelos vazamentos de Edward Snowden sobre a vigilância realizada por diversos órgãos estatais do EUA, principalmente a *National Security Agency*, e de alguns países da Europa[59].Outra inovação foi a preocupação com que o país terceiro tenha autoridades de fiscalização independentes com meios aptos a efetivar a proteção dos dados pessoais dos titulares e que possam cooperar com as autoridades de controle europeias.

Por fim, serão considerados os compromissos internacionais assumidos pelo país terceiro ou organização internacional, bem como sua participação em sistemas multilaterais e regionais (participação do Brasil na OEA, por exemplo), os quais estão relacionados à proteção de dados pessoais.

A expansão dos critérios de avaliação da União Europeia para um decisão de adequação sobre o nível de proteção de dados pessoais demonstra o quão complexa é tal análise. A magnitude da mudança evidencia como restarão insuficientes os critérios da Diretiva 95/46, na qual se inspira fortemente o parágrafo único do artigo 33 do PL nº 5276.

> *Art. 34. A autorização referida no inciso IV do caput do art. 33 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular, apresentadas em cláusulas contratuais aprovadas pelo órgão competente para uma transferência específica, em cláusulas contratuais padrão ou em normas corporativas globais, nos termos do regulamento.*
>
> *§ 1º O órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos constantes em documentos que fundamentem a transferencia internacional de dados, que deverão observar os principios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária do cedente e do cessionário, independentemente de culpa.*
>
> *§ 2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação do órgão competente, obrigatórias para todas as empresas integrantes do grupo ou conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.*
>
> *§ 3º Na análise de cláusulas contratuais, documentos ou de normas corporativas globais submetidas à aprovação do órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.*
>
> *§ 4º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput serão, também, analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §1° e §2° do artigo 45.*

O caput do artigo 34 do PL n.5276 define as hipóteses que necessitam da autorização prévia a que se refere o artigo 33, IV. O critério geral para autorização da transferência internacional de dados pessoais, pelos responsáveis do tratamento, dar-se-á pela conformidade com os "princípios gerais de proteção e os direitos do titular", expressa por meio de (1) cláusulas contratuais ou (2) normas corporativas globais.

O modelo de autorização prévia do Projeto de Lei assemelha-se com as exceções ao critério da "proteção equivalente" para as transferências internacionais de dados pessoais a terceiros fora da Área Econômica Europeia (*European Economic Area*), estabelecidas no artigo 26, parágrafo 2, da antiga Diretiva 95/46/EU. No modelo europeu, o Estado membro pode autorizar a transferência para um país que não possui um nível

59 GREENWALD, Glenn. Sem Lugar para se Esconder: Edward Snowden, A Nsa e A Espionagem do Governo Americano. 1ª Edição. Editora Sextante, 28/04/2014. 288 páginas.

equivalente ao de proteção europeia quando o "controlador" garantir a "privacidade, os direitos fundamentais e as liberdades individuais" dos cidadãos objeto de tratamento, enfatizando, no texto legal, como um dos meios para a proteção, as "cláusulas contratuais".[60]

Ao longo dos anos 2000, a Comissão Europeia adotou adicionalmente o modelo de cláusulas contratuais padrão[61] e regras corporativas vinculantes (*binding corporate rules*)[62], as quais não estavam previstas no texto da Diretiva 95/46. Em 2016, o *General Data Protection Regulation* (GDPR) 2016/67 foi aprovado pelo Parlamento Europeu, com caráter uniformizador e manteve o mesmo modelo geral do critério da "proteção equivalente" da Diretiva 95/46. Caso o país terceiro, território especifíco, ou organização internacional, não se adeque ao mesmo nível de proteção europeu, ou ainda não tenha sido analisado sua adequação[63], a transferência pode ser realizada com base em outros parâmetros. O recurso às cláusulas contratuais padrão, às cláusulas específicas aprovadas pelos órgãos competentes e às normas corporativas vinculantes (*binding rules*)[64] foi mantido.

A nova regulação europeia, no artigo 46, chegou a expandir o número de exceções que permitem as transferências internacionais, como nos casos de (1) haver instrumentos juridicamente vinculantes entre as autoridades ou organismos públicos da Europa e o terceiro envolvido na transferência; (2) o responsável pelo tratamento ou pelos subcontratantes no país terceiro adote um código de conduta de caráter vinculativo juridicamente, previamente aprovado; e (3) criação de um procedimento de certificação a ser conferido aos responsáveis pelo tratamento ou pelos subcontratantes que se adequarem a determinados critérios. Essa política legislativa parece recorrer a um modelo parcialmente baseado na autonomia das partes, mas sujeito a algumas regras de ordem pública, sempre que autoridades ou organizações têm o poder de interferir com o conteúdo de cláusulas contratuais ou códigos corporativos (e.g. anteriormente à aprovação).

O artigo 34 do PL e seus parágrafos fazem referência a **um órgão competente pela supervisão de dados**, no entanto, **falta ao Projeto qualquer definição a respeito das premissas de sua estrutura e operações, o que pode resultar em incertezas e em menores graus de transparência para grandes *stakeholders* e, acima de tudo, para usuários de internet**. Também a Corte de Justiça Europeia discutiu, no caso *European Comission v. Austria*[65], a constituição de órgão independente como componente necessário ao sistema de proteção de dados. Segundo a Corte, para que operem de forma objetiva e imparcial, os órgãos necessitam de orçamento próprio, ainda que se

60 Diretiva 95/46/EU, artigo 26, nº 2: " 2.Sem prejuízo do nº 1, um Estado-membro pode autorizar uma transferência ou um conjunto de transferências de dados pessoais para um país terceiro que não assegura um nível de protecção adequado na acepção do nº 2 do artigo 25º, desde que o responsável pelo tratamento apresente garantias suficientes de protecção da vida privada e dos direitos e liberdades fundamentais das pessoas, assim como do exercício dos respectivos direitos; essas garantias podem, designadamente, resultar de cláusulas contratuais adequadas. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&qid=1466131624407&from=EN>. Acessado em: 17/06/2016

61 Decision 2001/497/EC; Decision 2004/915/EC; e Decision 2010/87/EU.

62 Overview on Binding Corporate Rules.Disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm>. Acessado em 17/06/2016

63 GDPR 2016/679/EP, artigo 45, nº 1: "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."Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN>. Acessado em: 17/06/2016

64 GDPR 2016/679/EP, artigos 46 e 47.

65 Tribunal de Justiça Europeu, Caso C614/10, European Commission v. Republic of Austria, julgamento em 16/10/2012, disponível em: <https://tinyurl.com/kvt388s>.

vinculem à estrutura do Estado[66].

Apesar da importância da atuação independente do órgão, o objetivo não é a sua separação total do Estado, mas sua autonomia, a fim de que sirva ao propósito de uma efetiva proteção aos dados a serem transferidos, resguardados os princípios gerais de proteção, que são delineados no artigo 6º do Projeto de Lei n. 5276. **Se a decisão do legislador brasileiro for a de prosseguir com esse modelo, deve ser feita previamente uma avaliação de oportunidade e de viabilidade. Essa decisão envolve, por exemplo, a opção de criar um órgão ou agência governamental independente com mandatos claros e definidos.**

Na prática contudo, o que se verificou na União Europeia foi que, em muitos casos, autoridades são incapazes de cumprir suas funções por falta de recursos humanos e financiamento[67]. Somada à crescente complexidade de regulações de governança internacional sobre dados, tem-se uma preocupação quanto à efetividade desse sistema vinculado à uma autoridade estatal e ao correto entendimento de indivíduos quanto a normas ou termos. Isso porque, uma vez que muitas transferências de dados requerem o consentimento dos titulares, a falta de clareza e transparência pode dificultar uma efetiva autorização[68].

> *§ 1º O órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos constantes em documentos que fundamentem a transferencia internacional de dados, que deverão observar os principios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária do cedente e do cessionário, independentemente de culpa.*

O *caput* do artigo 34 torna evidente a influência do PL n. 5276 pelo modelo europeu. O § 1º delega ao órgão competente a elaboração de cláusulas contratuais padrão, com o intuito de diminuir os custos burocráticos para o setor privado. No mesmo parágrafo incube ao orgão competente a aprovação prévia de cláusulas contratuais específicas para transferências internacionais não abarcadas pelos outros casos da lei.

A afirmação de responsabilidade solidária entre o cedente dos dados e o cessionário, independente de culpa, denota uma salvaguarda contra eventuais tentativas de se contornar as proteções estabelecidas na legislação brasileira por meio da cessão dos dados a terceiro. Nesse sentido a GDPR 2016/679 apresenta preocupação semelhante e vai além, afirmando no seu artigo 44 que as proteções europeias se estendem a qualquer camada de transferência (*onwards transfers).* Por exemplo, se a empresa A transfere os dados para B em outro país (X), e esta transfere para C situado em país (Y), as proteções europeias seguem responsabilizando A, B e C.

66 BALTHASAR, Alexander. *'Complete Independence' of National Data Protection Supervisory Authorities – Second Try: Comments on the Judgment of the CJEU* of 16 October 2012, C-614/10 (European Commission v. Austria), with Due Regard to its Previous Judgment of 9 March 2010, C-518/07 (European Commission v. Germany).

67 European Union Agency for Fundamental Rights, 'Data Protection in the European Union: the Role of National Data Protection Authorities' (2010), <http://fra.europa.eu/fraWebsite/attachments/Dataprotection_en.pdf>, p. 46

68 KUNER, Christopher. Regulation of transborder data flows under data protection and privacy law: past, present, and future. *TILT Law & Technology Working Paper*, n. 016, 2010.

§ 2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação do órgão competente, obrigatórias para todas as empresas integrantes do grupo ou conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.

O § 2º cria a possibilidade de grupos econômicos e conglomerados submeterem à aprovação **normas corporativas globais**, o que em parte é uma tentativa de se garantir a proteção dos dados pessoais dos indivíduos ao mesmo tempo em que se diminui os custos burocráticos. Isso porque, uma vez aprovadas, as transferências dentro do grupo ocorrem sem necessidade de autorização para cada operação específica.

§ 3º Na análise de cláusulas contratuais, documentos ou de normas corporativas globais submetidas à aprovação do órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.

O § 3º pode gerar resistência de certos setores econômicos por receio de a fiscalização do órgão competente exigir acesso a dados sensíveis do ente privado, como nos casos de segredo de negócio. O artigo 10, § 4º, da Lei 12.965/2014, pode ser apontado como exemplo de equilíbrio, pois lida com a necessidade de transparência em medidas de segurança adotadas por provedores de serviço de internet, ao mesmo tempo em que exige observância aos direitos de confidencialidade relacionados aos segredos de indústria. Qualquer decisão no âmbito do processo legislativo deve levar em consideração a necessidade de atingir um equilíbrio entre as metas de proteção de dados e a transparência nas medidas de segurança, em especial para evitar qualquer retenção indevida de dados, ou a publicização de segredos de indústria não previstos pela lei estatutária existente.

§ 4º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput serão, também, analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §1° e §2° do artigo 45.

O § 4º afirma que, na análise para autorização de transferência internacional, serão consideradas como critério relevante as medidas técnicas e organizacionais adotadas pelo operador. Como exemplo de medida técnica é possível citar a verificação da existência ou não de determinado tipo de criptografia para os dados. Já como exemplo de medida organizacional aponta-se o modo como o responsável estabelece quais órgãos ou funcionários da empresa têm acesso aos dados.

Art. 35. O cedente e o cessionário respondem solidária e objetivamente pelo tratamento de dados, independentemente do local onde estes se localizem, em qualquer hipótese.

Muito embora não tenha o Projeto de Lei nº 5276/2016 adotado expressamente um princípio geral de responsabilidade (*accountability*), o artigo 35 do texto sob análise do Congresso Nacional brasileiro aparenta ser - juntamente a outros dispositivos e instrumentos previstos - expressão da ideia de "*accountability*" como princípio de proteção dos dados pessoais. Esse princípio recebeu acolhida na recente regulamentação geral europeia referente ao direito de proteção de dados pessoais, o Regulamento 2016/679.

Uma leitura atenta da redação do artigo 35, na verdade, pode gerar certa confusão se considerada a tradição romano-germânica do direito brasileiro, haja vista que as noções de *responsabilidade solidária* e *responsabilidade objetiva* são distintas e tipicamente relativas ao Direito Civil, mais especificamente ao Direito das Obrigações, que

tratam dos respectivos institutos jurídicos.

O dispositivo em comento abrange duas abordagens quanto à transmissão de dados pessoais a países estrangeiros: a que se pauta na noção de *accountability* a reger a relação entre os agentes de tratamento de dados pessoais e o titular dos dados; e a que se baseia na responsabilidade civil e na obrigação de ressarcir danos causados.

C. Transferência internacional de dados e o princípio da responsabilidade (*accountability*)

Um dos principais critérios de disciplina da transferência internacional de dados inscritos no Projeto de Lei nº 5276/2016 segue parâmetro geográfico (artigo 33, I). Esse modelo, não obstante fomentar a elevação do nível de proteção legal da privacidade nos países destinatários de informações de caráter pessoal, tem limitações sérias para assegurar efetiva proteção dos dados pessoais por meio do respeito às normas gerais e do cumprimento dos procedimentos previstos. Esses desafios já foram, inclusive,reconhecidos pelo Grupo de Trabalho do Artigo 29 no âmbito do direito comunitário europeu à época em que era orientado pela Diretiva 95/46/CE[69].

Ao estabelecer que o agente de tratamento de informações pessoais emissor, bem como o receptor, respondem à pessoa titular pelo tratamento de seus dados "*independentemente do local onde estes se localizem, em qualquer hipótese*", formula-se no artigo 35 do projeto de lei critério não geograficamente baseado. Desse modo, não importa onde se encontra a base de dados em que as informações de natureza pessoal estão armazenadas, ou o território em que se desenvolvem as operações de tratamento dos dados pessoais a partir de sua transmissão internacional, ou sequer o marco regulatório ali existente.

Em razão da aplicação do *princípio da responsabilidade (accountability),* cedente e cessionário respondem pelas operações realizadas com dados pessoais. Por isso, devem adotar as medidas de gerenciamento necessárias para conferir efetividade e aplicação prática às normas de proteção da privacidade, seja internamente em sua estrutura organizacional, seja externamente perante terceiros.

Nesta medida, além de normas que impõem a verificação de *equiparável* nível de proteção de informações pessoais, fundadas num modelo geográfico de regulamentação do fluxo de dados entre fronteiras nacionais, o projeto de lei conjuga regra lastreada no que Christopher Kuner denomina *modelo organizacional*[70] de transferência internacional de dados pessoais. Nesse contexto, busca-se promover uma responsabilidade organizacional (*organizational accountability*) que é obtida pela criação - pelas entidades que manejam volume de informações cada vez maior - de abrangentes programas de gerenciamento de privacidade. Esses programas devem, de fato, implementar regras de boas práticas[71], códigos de conduta, normas corporativas etc., orientações internas e/ou externas aplicáveis por todo o ciclo de vida da informação objeto de tratamento[72], independentemente do local ou jurisdição em que esteja.

69 ARTICLE 29 DATA PROTECTION WORKING PARTY. *The future of privacy:* Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Bruxelas: [s. n.], 2009. p. 7-8.

70 KUNER, Christopher. Regulation of transborder data flows under data protection and privacy law: past, present and future. *OECD Digital Economy Papers*, n. 187, OECD Publishing, 2011, passim.

71 Vide o que dispõe o artigo 50 do PL nº 5276/2016.

72 CENTRE FOR INFORMATION POLICY LEADERSHIP. *Protecting privacy in a world of Big Data*: the role of enhanced accountability in creating a sustainable data-driven economy and information society, 2015. p. 2.

Por fim, ressalta-se que o instituto da responsabilidade solidária entre cedente e cessionário de transmissão transfronteiriça de dados pessoais torna-se dispensável na medida em que o princípio da responsabilidade que inspira o texto do PL nº 5.276 visa a tornar qualquer agente de tratamento de dados pessoais responsável (*accountable*) pela segurança e proteção para as informações coletadas e utilizadas, independente de que elas se localizam ou não em território brasileiro ou não. Assim, basta a enfática prescrição de que ambos são responsáveis pelo tratamento de dados independente do ponto geográfico em que se encontrem.

D. Ressarcimento de danos no contexto da transmissão transnacional de dados

Desde a década de 1980, notadamente com as *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* e a Convenção 108 do Conselho da Europa, a transmissão internacional de informações pessoais insere-se em quadro normativo que busca o equilíbrio entre a proteção do direito fundamental à privacidade e o livre tráfego de dados pessoais.

Atualmente, e como se buscou ressaltar no presente *policy paper,*a transferência é compreendida como essencial, intermitente e ubíqua na *digital economy*. Nesta medida, as leis de proteção de dados pessoais, com âmbito nacional ou regional, vigentes mundo afora, não têm por inspiração o propósito de impedir o tratamento de informações – incluindo a transmissão transfronteiriça – relativas a pessoas identificadas ou identificáveis. Na verdade, buscam conferir à pessoa titular o efetivo controle sobre seus próprios dados pessoais ainda que colocados em circulação, tanto em contexto *offline* quanto naquele *online*.

O Projeto de Lei nº 5276/2016 segue essa orientação, de maneira que reconhece e conforma seus parâmetros normativos ao **perfil procedimental do direito à proteção de dados pessoais**, que se expressa no sentido de assegurar ao indivíduo progressivas e pontuais formas de um "controle *in itinere*"[73] sobre todo o circuito informativo do dado pessoal. É o que se vê, por exemplo, quando o consentimento livre e inequívoco do titular é exigido como requisito para o legítimo tratamento de dado pessoal (artigo 7º, I), principalmente se considerado informação sensível (artigo 11, I), podendo este ato de vontade também ser, como já visto, hipótese permissiva de transmissão internacional de dados (artigo 33, VII).

Essa moldura revela claramente a prevalência da tutela jurídica *preventiva*[74] que se pretende atribuir aos titulares das informações divulgadas, coletadas, armazenadas, compartilhadas e transferidas. Isto é, por meio de normas sobre tratamento de dados pessoais e sua transferência internacional, o projeto de lei visa promover a realização de direitos e liberdades fundamentais da pessoa humana prioritariamente (artigo 1º), ao evitar a ocorrência de danos decorrentes do tratamento de informações[75]. Daí, portanto,

73 MESSINA, Mara. I diritti dell'interessato. In: CARDARELLI, Francesco; SICA, Salvatore; ZENO-ZENCOVICH, Vincenzo. *Il codice dei dati personali:* temi e problemi. Milão: Giuffrè, 2004. p. 75-76.

74 Essa observação doutrinária foi feita também na Itália após a promulgação das leis gerais de proteção de dados pessoais, tanto a Lei nº 675/1996 como o posterior Dec. Legislativo nº 196/2003 hoje em vigor, que transpuseram a Diretiva 95/46/CE para o direito interno italiano (DI MAJO, Adolfo. Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela. In: CUFFARO, Vincenzo; RICCIUTO, Vincenzo; ZENO-ZENCOVICH, Vincenzo (Coords.). *Trattamento dei dati e tutela della persona.* Milão: Giuffrè, 1998, p. 244-245; RESTA, Giorgio. Il diritto alla protezione dei dati personali. In: CARDARELLI, Francesco; SICA, Salvatore; ZENO-ZENCOVICH, Vincenzo. *Il codice dei dati personali:* temi e problemi. Milão: Giuffrè, 2004, p. 25-26).

75 O artigo 6º, VIII, do PL nº 5276/2016 dispõe sobre o *princípio da prevenção*, "pelo qual devem ser adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais".

se dizer que a tutela *ressarcitória* assume nesta seara papel secundário ou de segunda ordem: a responsabilidade civil só terá lugar quando o instrumental posto à disposição dos titulares não puder obstar o dano causado pelo tratamento de dados pessoais.

É já reconhecido, deve-se salientar, que a transferência internacional de informações de natureza pessoal, em suporte digital ou não, pode ensejar obstáculos à concretização do direito à proteção dos dados pessoais do indivíduo e risco de sua ilícita utilização.[76] Por isso, apesar do viés preventivo, a responsabilidade civil deve ser considerada um importante instituto para garantir proteção mínima à pessoa humana vítima de danos decorrentes do indevido tratamento de informação.

De acordo com o PL, serão indenizados os danos que eventualmente recaírem sobre o titular dos dados pessoais objeto de transmissão por sujeito exportador localizado no território brasileiro a ente importador situado em outro país[77]. Além disso, é possível que a lesão seja de natureza *patrimonial* ou *extrapatrimonial*, *individual* ou *coletiva,* conforme, aliás, prescreve o artigo 42 do projeto de lei ao disciplinar a responsabilidade civil dos agentes do tratamento de dados pessoais.

Nestes termos, se a transferência internacional de dados for ato que se liga por nexo de causalidade a prejuízos que repercutem no patrimônio da pessoa, serão passíveis de ressarcimento tanto os danos emergentes quanto os lucros cessantes verificados[78]. O mesmo se aplica quando o tratamento efetuado por cedente ou cessionário de informações pessoais for causa de dano moral a titular de dado. Nesse sentido, haverá obrigação de indenizar quando, da transmissão de dados, a pessoa em causa (identificada ou identificável) sofrer violação a alguma situação jurídica subjetiva extrapatrimonial (*e.g.*, direito de imagem, direito à honra, direito à identidade pessoal, direito à não discriminação)[79].

Destaca-se que provavelmente os danos extrapatrimoniais serão de maior incidência prática como consequência do tratamento de dados pessoais do que os prejuízos de natureza patrimonial. A razão da afirmação encontra-se não apenas na expansão dos novos danos à pessoa[80], mas especialmente no fato de que **o direito à proteção dos dados pessoais tem caráter complexo**. Isso significa que a tutela da privacidade se presta a proteger um plexo de interesses jurídicos e não apenas, como outrora, a intimidade. Assim, mais do que assegurar o segredo, a exclusão de certas informações do conhecimento comum (sentido *negativo*), busca-se atribuir à pessoa maior poder para controlar os dados que lhe dizem respeito – principalmente aqueles sobre as convicções políticas e filosóficas, credo religioso, vida sexual, estado de saúde, entre outros – a fim de que suas liberdades não sejam tolhidas pelo fomento ao conformismo e pela discriminação social (sentido *positivo*)[81]. Em resumo, os indivíduos têm um papel

76 O Regulamento (EU) 2016/679, no considerando nº 116 ressalta justamente esse ponto: "*When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information […]*".

77 Uma transmissão internacional de dados pessoais envolve pelo menos três operações de tratamento: i) a que tornou disponível as informações pessoais ao agente responsável (cedente) – *v. g.*, coleta dos dados; ii) a transmissão dessas informações a país estrangeiro pelo cedente; e iii) o tratamento (*v. g.*, armazenamento em banco de dados) que o receptor dos dados pessoais efetua em seu estabelecimento situado em país estrangeiro (GIMÉNEZ, Alfonso Ortega. *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*. Madri: Agencia Española de Protección de Datos, 2015. p. 61).

78 Sobre os danos patrimoniais ou materiais dispõe o artigo 402 do Código Civil brasileiro: "Salvo as exceções expressamente previstas em lei, *as perdas e danos devidas ao credor abrangem, além do que ele efetivamente perdeu, o que razoavelmente deixou de lucrar*." (grifou-se).

79 Esta noção de dano moral segue conceituação elaborada pela Profª. Maria Celina B. de Moraes. Sobre o assunto v. MORAES, Maria Celina Bodin de. *Danos à pessoa humana:* uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2009. p. 182-192.

80 Cf. SCHREIBER, Anderson. *Novos paradigmas da responsabilidade civil.* 2. ed. São Paulo: Atlas, 2009. p. 87-89.

81 RODOTÀ, Stefano. *Tecnologie e diritti.* Bolonha: Il Mulino, 1995, p. 101-102; DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 141-147.

a desempenhar na escolha se algum tipo específico de dados ainda está sujeito tanto à uma decisão autônoma, quanto à discricionariedade privada.

Por tais razões, uma ineficaz proteção de dados pessoais abre portas para (i) a violação a outros direitos e liberdades fundamentais (PL nº 5276/2016, artigo 1º), como, por exemplo, o direito à identidade pessoal, a liberdade de opinião e expressão e o direito à honra; e (ii) a danos morais provocados devido a lesão à pessoa humana.

Ainda no que tange aos danos ressarcíveis, o artigo 42 do Projeto de Lei brasileiro não ignora os danos de espectro coletivo ou difuso que podem advir da atividade desenvolvida pelos agentes de tratamento de dados pessoais. É importante considerar o massivo e perene fluxo de informações de caráter pessoal via *Web* e as operações realizadas por entes públicos e privados que utilizam avançadas técnicas do *Big Data.* Nesse contexto, se de tratamento(s) realizado(s) por cedente ou cessionário em transferência internacional de informações pessoais sobrevier lesão a interesses individuais homogêneos ou interesses metaindividuais, haverá a possibilidade de judicialização do conflito por meio de ações coletivas, disciplinadas pelo Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990) e pela Lei nº 7.347, de 24 de julho de 1985[82,83].

Aspecto de grande relevância sobre a tutela reparatória é a natureza do critério de imputação de responsabilidade por danos dos agentes exportador e importador de informações.Verifica-se que o critério pode ser *subjetivo* ou *objetivo* e fundado na *culpa* ou no *risco*.

O artigo 35 do PL nº 5276/2016, em consonância ao que dispõe no seu artigo 42, faz opção pelo regime de *responsabilidade civil objetiva*, significando isso que a imputação de danos ao agente de tratamento de dados pessoais não é determinada pela falta de diligência, ou desconformidade a um *standard* de conduta, ao realizar operação com informação pessoal. Semelhante escolha fez o legislador espanhol na *Ley Orgánica 15/1999,* que no artigo 19.1[84] prescreveu a responsabilidade independente de culpa dos agentes pela indenização dos danos causados aos titulares dos dados pessoais[85]. Essa opção feita no direito espanhol não reflete de forma direta orientação da Diretiva 95/46/CE, porquanto esta não seguiu direção clara[86] ao prever no artigo 23:

82 O artigo 22 do PL nº 5276/2016 assim determina: "*A defesa dos interesses e direitos dos titulares de dados poderá ser exercida em juízo individual ou coletivamente, na forma do disposto na Lei no 9.507, de 12 de novembro de 1997, nos arts. 81 e 82 da Lei no 8.078, de 11 de setembro de 1990, na Lei no 7.347, de 24 de julho de 1985, e nos demais instrumentos de tutela individual e coletiva*".

83 Encontra-se em tramitação na 23ª Vara Cível e na 9ª Vara Cível da Circunscrição Especial de Brasília/DF ações civis públicas propostas pelo Instituto Brasileiro de Política e Direito de Informática – IBDI em face do Google, em que se pedem a condenação do réu ao pagamento de indenização por danos morais coletivos em razão de coleta "indiscriminada" de dados dos cidadãos brasileiros, feita pela empresa mediante o Google Street View e o extinto Google Buzz. TJDF, Google/Instituto Brasileiro de Política e Direito da Informática - IBDI, Nº 2015.01.1.000575-6 - Ação Civil Coletiva, decisão de 02/05/2017, disponível em: <http://bit.ly/2qBGIT8>; e TJDF, Google/Instituto Brasileiro de Política e Direito da Informática - IBDI, Nº 2013.01.1.096604-4 - Ação Cautelar Preparatória, decisão de 11/04/2013, disponível em: <http://bit.ly/2oV64iP>. Em tese, é possível que numa situação como essa tenha ocorrido transferência internacional de dados. Já nos Estados Unidos da América, no recente caso *Mark Siegal v. Snapchat Inc.* uma *class action* foi proposta em face da sociedade empresária titular do aplicativo para celulares *Snapchat,* haja vista que, ao sentir do demandante, a empresa tem coletado ilegalmente dados biométricos de milhões de usuários por meio da tecnologia de reconhecimento facial aplicada às fotos dos usuários, criando e armazenando "modelos de face" (*face templates*), o que seria feito sem observar o *Biometric Information Privacy Act* do Estado de Illinois (TASSIN, Paul. *Snapchat Class Action Says Facial Recognition Technology Illegal*. Disponível em <https://goo.gl/O4JCG0>. Acesso em 03.06.2016).

84 ESPANHA, *Ley Orgánica 15/1999,* 199. Disponível em: <https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>. Acesso em 20 de junho de 2016. *"Artículo 19. Derecho a indemnización. 1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. [...]".*

85 GIMÉNEZ, Alfonso Ortega. *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*. Madri: Agencia Española de Protección de Datos, 2015. p. 61-62. Muito embora seja do parecer de que o regime é de responsabilidade objetiva, o autor ressalta que trata-se de responsabilidade civil extracontratual.

86 Id., ibid., p. 62.

> 1. Os Estados-membros estabelecerão que qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto incompatível com as disposições nacionais de execução da presente directiva tem o direito de obter do responsável pelo tratamento a reparação pelo prejuízo sofrido. 2. O responsável pelo tratamento poderá ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano lhe não é imputável.

A confirmar essa falta de posicionamento induvidoso, na transposição da citada Diretiva para o direito interno da Itália – primeiro com a Lei nº 675/1996[87], depois com o Decreto Legislativo nº 196/2003[88] – afirmou-se que o sistema ali adotado foi o da *responsabilidade pressuposta*[89] ou *responsabilidade semi-objetiva*[90], que muito se aproxima da ideia de responsabilidade por culpa presumida. Essa modalidade inverte o ônus probatório e admite a exclusão da responsabilidade se o agente demonstrar a adoção de todas as medidas idôneas a fim de evitar o dano.

A nova regulamentação geral europeia da proteção de dados de caráter pessoal, que toma lugar com o Regulamento 2016/679, não parece ter se afastado da anterior Diretiva de 1995, eis que o texto normativo adotou redação praticamente idêntica conforme se vê a partir da leitura do artigo 82, que trata do *right to compensation and liability*[91].

Sendo, porém, confirmada no Brasil a opção pelo regime de responsabilidade objetiva no terreno da atividade de tratamento de dados pessoais, como atualmente se apresenta no PL nº 5276/2016, a responsabilização por danos decorrentes de ilícita transferência internacional de informações pessoais haverá de ser, em grande medida, uma discussão sobre causalidade, é dizer, se o indevido tratamento de dados é necessária causa dos danos sofridos pela pessoa.

Se o debate for travado judicialmente, será possível exigir do agente de tratamento de dados pessoais a inequívoca comprovação de excludente de responsabilidade: só assim se afastará o reconhecimento da obrigação de indenizar, porquanto admissível é a distribuição dinâmica do ônus da prova a fim de evitar que o titular de dados tenha que se desincumbir de prova diabólica, ou seja, impossível (Código de Processo Civil, artigo 373, § 1º[92]; PL nº 5276/2016, artigo 42, parágrafo único).

As excludentes de responsabilidade alegáveis pelo cedente ou cessionário das

87 ITÁLIA. *Legge 675/1996,* 1996. Disponível em: <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/28335>. Acesso em 20 de junho de 2016. O regime de responsabilidade civil era delineado pelos arts. 18, 9º e 29.

88 ITÁLIA. Decreto Legislativo n. 196, de 2003. Disponível em: <http://www.camera.it/parlam/leggi/deleghe/03196dl.htm>. Acesso em 20 de junho de 2016. Consolida-se no artigo 15, com remissão feita ao artigo 2050 do *Codice Civile*, norma sobre a tutela reparatória.

89 DI CIOMMO, Francesco. Il danno non patrimoniale da trattamento dei dati personali. In: PONZANELLI, Giulio (Coord.). *Il "nuovo" danno non patrimoniale*. Pádua: CEDAM, 2004. p. 261-263.

90 SICA, Salvatore. Le tutele civili. In: CARDARELLI, Francesco; SICA, Salvatore; ZENO-ZENCOVICH, Vincenzo. *Il codice dei dati personali:* temi e problemi. Milão: Giuffrè, 2004. p. 553.

91 "*Article 82. Right to compensation and liability.* 1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. 2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. 3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage. […]".

92 BRASIL. *Lei nº 13.105,* 2015. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Acesso em 20 de junho de 2016.

informações são, nomeadamente, *fato exclusivo da vítima ou de terceiro*, e *caso fortuito ou de força maior*. Quanto ao fato de terceiro deve-se ter em conta que terceiro é alguém que não possui vínculos com os agentes de tratamento de dados pessoais[93]. Nesse sentido, se a transmissão de informações de natureza pessoal para país estrangeiro tiver ensejo com ato de sujeito integrante do quadro organizacional de determinado ente, fato de terceiro não existe, ainda que o ato praticado não seja da atribuição ou competência do autor da ilícita transferência. Por sua vez, caso fortuito ou de força maior como hipótese interruptiva do nexo de causalidade têm as marcas da *imprevisibilidade* e da *inevitabilidade*. Se o fato não tiver essas características, a excludente de responsabilidade não se configura.

Se, de toda sorte, houver dano ressarcível imputado ao emissor e/ou ao receptor de dados pessoais em fluxo transnacional, o adimplemento da obrigação de indenizar que então surge pode ser exigida de um e/ou outros agente de tratamento de dados pessoais, em razão *responsabilidade solidária.* Nesses casos, aplica-se o regime das obrigações solidárias positivado nos arts. 275 a 285 do Código Civil brasileiro. A dicção do artigo 44 do projeto de lei é expressa neste sentido[94].

93 Cf. MARTINS, Guilherme Magalhães. *Responsabilidade civil por acidente de consumo na Internet*. 2. ed. rev., atual. e amp. São Paulo: Revista do Tribunais, 2014, p. 157.

94 BRASIL. *Lei 10.406*, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em 20 de junho de 2016. "Art. 44. Nos casos que envolvem a transferência de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos eventualmente causados".

3. Conclusões e Recomendações

A análise do Capítulo V do Projeto de Lei nº 5.276/2016 permite verificar a influência do modelo europeu de proteção de dados sobre a futura disciplina normativa da transferência internacional de dados no Brasil. A esse sistema modelo geográfico de proteção, contudo, opõem-se algumas críticas, que podem ser superadas, alternativamente, pelo chamado ***modelo organizacional***.

Diferentemente do modelo europeu, que adota critérios geográficos centrados na figura do Estado como garantidor de proteção, a alternativa do modelo organizacional coloca os deveres de diligência para com os dados nas mãos das empresas que os coletam, transferem e tratam. Existem diversas razões, elencadas a seguir, para que este modelo seja preferível ao geográfico; ou para que haja uma hibridização dos dois, resultando em um modelo *sui generis*.

O modelo europeu adota um critério essencialmente geográfico para definir as situações em que a transferência internacional de dados é permitida ou não. Em um mundo cada vez mais globalizado, regulações baseadas em critérios territoriais se revelam problemáticas e obsoletas, na medida em que a geografia passa a importar cada vez menos no âmbito da tecnologia e dos negócios. O modelo organizacional é capaz de transcender as fronteiras dos Estados, fazendo com que o nível de proteção dos dados os acompanhe por onde forem, uma vez que os deveres de diligência são atribuídos à entidade que os coleta e não ao Estado para onde serão transferidos os dados.

O **modelo organizacional** seria compatível com o disposto no artigo 11 do Marco Civil da Internet que demanda a aplicação da lei brasileira aos dados coletados no Brasil, e não resultaria em problemas jurisdicionais pelo fato de os dados terem sido transferidos para outras jurisdições.

Um dos problemas de se atribuir o dever de diligência da proteção de dados transferidos aos Estados é a baixa eficácia das normas de proteção. A experiência europeia demonstrou que as autoridades responsáveis por fiscalizar a proteção de dados em cada país europeu sofrem com falta de recursos. Isso resulta em lentidão e ineficácia na proteção dos dados até mesmo de seus nacionais, com diversas atividades de tratamento de dados alheias às autoridades fiscalizadoras.

As Autoridades de Proteção de Dados (DPAs) europeias são consideradas, em geral, onerosas e ineficientes. Desse modo, resta impactada sua capacidade de fazer cumprir as regras de proteção de dados nacionais. Assim, a ideia de que os dados pessoais de usuários brasileiros estariam apropriadamente protegidos apenas por terem sido transferidos para países onde a legislação lhes confere satisfatório grau de proteção é equivocada. Além disso, seus benefícios pretendidos não compensam, na prática, os custos econômicos advindos da burocracia envolvida.

O legislador deve levar em consideração, ainda, a estrutura do Estado brasileiro, já significativamente burocrática e ineficiente, e sua capacidade para atender as demandas de autorização de transferência internacional de modo a não significarem um entrave às atividades econômicas envolvidas.

O modelo organizacional que recomendamos tenta contornar esses problemas obrigando as entidades exportadoras a manterem uma proteção contínua de dados pessoais transferidos para outras organizações independentemente de sua localização geográfica. Essa proteção realizar-se-ia por meio da obrigatoriedade de cláusulas contratuais entre exportador e importador de dados, bem como da responsabilidade solidária entre eles. Atualmente, o projeto de Lei encaminhado ao Congresso abarca essa possibilidade em seu artigos 34 e 35. Entretanto, ainda mantém o centro do modelo de proteção em torno de autorizações prévias por parte da autoridade competente. Entendemos que esse ponto é problemático e burocrático, e que um modelo híbrido, que propicie maior liberdade e signifique menores entraves, deve ser adotado para alcançar o equilíbrio entre eficiência e proteção.

Por essas razões, propomos que as transferências internacionais de dados para países cujo grau de proteção de dados ainda não tenha sido avaliado ou não seja considerado equivalente ao brasileiro devam ser liberadas *a priori*, observadas as seguintes condições:

- As entidades exportadoras se comprometam a adotar medidas de proteção adequadas tanto em suas próprias operações de transferência internacional quanto naquelas envolvendo outras entidades estrangeiras;
- Os contratos de transferência internacional com importadores localizados em jurisdições sem nível de proteção equivalente ao brasileiro contenham cláusulas de diligência na proteção dos dados pessoais que atendam às exigências da lei brasileira;
- Que os contratos de transferência internacional com importadores localizados em jurisdições sem nível equivalente ao brasileiro contenham cláusulas que permitam à entidade exportadora, eventualmente responsabilizada por uma violação cometida pela importadora, dela cobrar regresso.

A partir desse arranjo, seria obrigação das autoridades brasileiras de proteção de dados a fiscalização contínua e posterior dos contratos das entidades exportadoras como forma de garantir que cumprem as exigências da lei brasileira. Esse modelo *ex post* de fiscalização já é operacionalizado no Brasil no que tange à cobrança de tributos. Por exemplo, um município deve fiscalizar prestações de serviço para conferir se recolheram o ISS (Imposto sobre Serviços), mas não tem capacidade de verificar a integridade de todos os possíveis contribuintes. Essa limitação não se torna, entretanto, entrave para a realização de novos negócios.

4. Referências

Livros e Artigos

ARTICLE 29 DATA PROTECTION WORKING PARTY. *The future of privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.* Bruxelas: [s. n.], 2009. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf>. Acesso em 16/06/2016.

_____. *Opinion 3/2010 on the principle of accountability.* Bruxelas: [s. n.], 2009, p. 7. Disponível em: < http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf>. Acesso em 10/06/2016.

BLAS, Frédéric. Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales. *Rev. Derecho del Estado*, v. 23, p. 37, 2009.

CARDARELLI, Francesco; SICA, Salvatore; ZENO-ZENCOVICH, Vincenzo. "*Il codice dei dati personali: temi e problemi*". Milão: Giuffrè, 2004.

CENTRE FOR INFORMATION POLICY LEADERSHIP. Protecting privacy in a world of Big Data: the role of enhanced accountability in creating a sustainable data-driven economy and information society, 2015. Disponível em <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_1_the_role_of_enhanced_accountability_21_october_2015.pdf>. Acesso em 11/06/2016.

CERDA SILVA, Alberto. "El 'nivel adecuado de protección' para las transferencias internacionales de datos personales desde la Unión Europea*." Revista de derecho (Valparaíso)*, n. 36, p. 327-356, 2011.

COMISSÃO EUROPEIA, *Transatlantic Data Flows: Restoring Trust through Strong Safeguards,*117 final, Brussels, 29 February 2016, Disponível em: <http://europa.eu/rapid/press-release_IP-16-433_en.htm>. Acesso em 15 de junho de 2016.

CUFFARO, Vincenzo; RICCIUTO, Vincenzo; ZENO-ZENCOVICH, Vincenzo (Coords.). *Trattamento dei dati e tutela della persona.* Milão: Giuffrè, 1998.

DI CIOMMO, Francesco. "Il danno non patrimoniale da trattamento dei dati personali." In: PONZANELLI, Giulio (Coord.). *Il "nuovo" danno non patrimoniale*. Pádua: CEDAM, 2004. p. 255-281.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Data Protection in the Europe-*

an Union: the Role of National Data Protection Authorities (2010), <http://fra.europa.eu/fraWebsite/attachments/Dataprotection_en.pdf>. Acesso em 20 de junho de 2016.

GEPI - Grupo de Ensino e Pesquisa em Inovação, FGV São Paulo. *Contribuição ao Anteprojeto de Proteção de Dados Pessoais.* São Paulo, p. 4-15, 2015.

GIMÉNEZ, Alfonso Ortega. *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*. Madri: Agencia Española de Protección de Datos, 2015.

KUNER, Christopher. "Data protection law and international jurisdiction on the Internet (part 1)". *International Journal of Law and Information Technology*, vol. 18. n. 2, p. 176 - 193, 2010.

_____. "Data protection law and international jurisdiction on the Internet (part 2)". *International Journal of Law and Information Technology*, vol. 18. n. 3, p. 227 - 247, 2010.

_____. "Extraterritoriality and regulation of international data transfers in EU data protection law." *International Data Privacy Law,* v. 5, n. 4, p. 235-245, 2015.

_____. "Regulation of transborder data flows under data protection and privacy law: past, present and future." *OECD Digital Economy Papers*, n. 187, OECD Publishing, 2011. Disponível em <http://dx.doi.org/10.1787/5kg0s2fk315f-en>. Acesso em 20/05/2016.

_____. "The European Union and the Search for an International Data Protection Framework", in *Groningen Journal of International Law* vol. 2, n. 2, 2014, p. 55-71.

MARTINS, Guilherme Magalhães. *Responsabilidade civil por acidente de consumo na Internet*. 2. ed. rev., atual. e amp. São Paulo: Revista dos Tribunais, 2014.

MORAES, Maria Celina Bodin de. *Danos à pessoa humana:* uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2009.

MORGADO, Laerte Ferreira. *O cenário internacional de proteção de dados pessoais. Necessitamos de um Código Brasileiro?* Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336>. Acesso em 30 de maio de 2016.

RODOTÀ, Stefano. *Tecnologie e diritti.* Bolonha: Il Mulino, 1995.

SCHREIBER, Anderson. *Novos paradigmas da responsabilidade civil.* 2. ed. São Paulo: Atlas, 2009.

SVANTESSON, Dan Jerker B. "The regulation of cross-border data flows." *International Data Privacy Law,* p. 180 - 198, 2011.

WEBER, Rolf H. “Transborder data transfers: concepts, regulatory approaches and new legislative initiatives.” *International Data Privacy Law,* p. 117 - 130, 2013.

NISSENBAUM, Helen. “A Contextual Approach to Privacy Online.” *Daedalus, the Journal of the American Academy of Arts & Sciences*, v. 140, n. 4, p. 32 - 27, 2011.

REINALDO FILHO, Demócrito. *A Diretiva Europeia sobre Proteção de Dados Pessoais - uma Análise de seus Aspectos Gerais.* Disponível: < http://www.lex.com.br/doutrina_24316822_A_DIRETIVA_EUROPEIA_SOBRE_PROTECAO_DE_DADOS_PESSOAIS__UMA_ANALISE_DE_SEUS_ ASPECTOS_GERAIS.aspx>. Acesso em 30 de maio de 2016.

Documentos e casos

ALEMANHA. Federal Data Protection Act, de 14 de janeiro de 2003. Disponível em: <http://www.gesetze-im-internet.de/englisch_bdsg/federal_data_protection_act.pdf>. Acesso em 30 de maio de 2016.

ARGENTINA, *Decreto n. 1558/2001*, de 29 de novembro de 2001. Disponível em: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70368/norma.htm>. Acesso em 30 de maio de 2016.

_____. *Lei n. 25.326*, de 30 de outubro de 2000. Disponível em: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>. Acesso em 30 de maio de 2016.

BRASIL, *Constituição Federal,* de 05 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acessoem 15 de junho de 2016.

_____, *Lei n. 12965*, de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 21 de maio de 2016.

_____. *Decreto n. 5.015*, de 12 de março de 2004. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm>. Acesso em 15 de junho de 2015.

_____. *Decreto n. 5.687*, de 31 de janeiro de 2006. .Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Decreto/D5687.htm>. Acesso em 16 de junho de 2016.

_____. *Lei n. 10.406*, de 10 de janeiro de 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em 20 de junho de 2016.

_____. *Lei n. 13.105,* de 16 de março de 2015. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Acesso em 20 de junho de 2016.

CHILE, *Lei n. 19.496*, de 28 de janeiro de 1997. Disponível em: <http://www.leychile.cl/

Navegar?idNorma=61438>. Acesso em 30 de maio de 2016.

COLOMBIA. *Ley Estatutaria n. 1.581*, de 17 de outubro de 2012. Disponível em: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>.Acesso em 15 de junho de 2016.

DECISÃO DA COMISSÃO de 30 de Junho de 2003 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais na Argentina. Disponível em: < http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32003D0490&from=PT>. Acesso em 30 de maio de 2016.

ESPANHA, *Ley Orgánica 15/1999,* de 14 de dezembro de 1999. Disponível em: <https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>. Acesso em 20 de junho de 2016.

EUA, *Judicial Redress Act,* de 18 de março de 2015. Disponível em: <https://www.congress.gov/bill/114th-congress/house-bill/1428>. Acesso em 15 de junho de 2016.

EUA-UE,*Umbrella Agreement,* de 08 de dezembro de 2015. Disponível em: <http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm>. Acesso em 15 de junho de 2016.

FRANÇA. *Loi Fédérale sur la Protection des Données,* de 19 de junho de 1992. Disponível em: <https://www.admin.ch/opc/fr/classified-compilation/19920153/201401010000/235.1.pdf>. Acesso em 15 de junho de 2016.

IRLANDA. *Data Protection Act,* 2003. Disponível em: <https://dataprotection.ie/viewdoc.asp?DocID=1467&ad=1>. Acesso em 15 de junho de 2016.

ITÁLIA. *Decreto Legislativo n. 196*, de 29 de julho de 2003. Disponível em: <http://www.camera.it/parlam/leggi/deleghe/03196dl.htm>. Acesso em 20 de junho de 2016.

_____. *Legge 675/1996,* de 31 de dezembro de 1996. Disponível em: <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/28335>. Acesso em 20 de junho de 2016.

ONU, *Declaração de Salvador sobre as Estratégias Abrangentes para os Desafios Globais: Prevenção de Crime e Sistemas de Justiça Criminal e seu Desenvolvimento num Mundo em Mudança*. 2010. Disponível em: <http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/In-session/ACONF.213L6_Rev.2/V10529061A_CONF213_L6_REV2_S.pdf>. Acesso em 01 de junho de 2016.

_____. *Convenção das Nações Unidas contra a Corrupção*, 2000. Disponível em: <https://www.unodc.org/lpo-brazil/pt/corrupcao/convencao.html>. Acesso em 16 de junho de 2016.

_____. *Convenção das Nações Unidas contra o Crime Organizado Transnacional,* 2000.Disponível em: <https://www.unodc.org/lpo-brazil/pt/crime/marco-legal.html>. Acesso em

15 de junho de 2016.

PARLAMENTO EUROPEU E CONSELHO, *Direita 2016/680,*de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L0680&from=PT>. Acesso em 15 de junho de 2016.

_____, *Diretiva 95/46/CE*, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: < http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em 30 de maio de 2016.

SUIÇA. *Loi fédérale sur la protection des données*, de 19 de junho de 1992. Disponível em: <https://www.admin.ch/opc/fr/classified-compilation/19920153/201401010000/235.1.pdf>. Acesso em 16 de junho de 2016.

URUGUAI. *Ley 18.331 (Protección de datos personales y acción de 'habeas data'")*, de 11 de agosto de 2008. Disponível em: <http://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n%C2%B0-18331-de-11-de-agosto-de-2008.html>. Acesso em 16 de junho de 2016.