4 de julho de 2015

Excelentíssimo Senhor Ministro José Eduardo Cardozo
Ministério de Estado da Justiça
Ministério da Justiça
Esplanada dos Ministérios
Palácio da Justiça, Bloco T, Edifício sede
70064-900 Brasília, DF
Brasil

Ref: CONTRIBUIÇÕES À CONSULTA PÚBLICA SOBRE O ANTEPROJETO DE LEI PARA A PROTEÇÃO DE DADOS PESSOAIS

Excelentíssimo Senhor Ministro,

O RELX Group, anteriormente conhecido como Reed Elsevier, agradece a oportunidade de comentar sobre o anteprojeto de lei do Ministério da Justiça para a proteção de dados pessoais. O RELX Group é uma empresa anglo-holandesa com presença no Brasil desde a década de 50. Presente em 4 cidades brasileiras e com mais de 400 funcionários, o RELX Group inclui a Reed Exhibitions Alcantara Machado, uma das principais organizadoras de feiras e exposições, e a Elsevier, a maior editora global na área médica, técnica e científica. O RELX Group também inclui a LexisNexis Risk Solutions e a FircoSoft, empresas de soluções na captação, desenvolvimento e gerenciamento de informações, provedora líder global em prevenção a lavagem de dinheiro através de soluções de filtragem, bem como com a verificação de identidade e ferramentas de prevenção de fraude servindo às necessidades dos bancos, varejistas e outras entidades brasileiras.

Como líder no mercado mundial de produtos de informação e serviços, parabenizamos o governo brasileiro pela iniciativa de criar uma estrutura de privacidade para proteger os seus cidadãos. Para as empresas intensivas em conhecimento como a nossa, criar uma estrutura que garante proteção para os indivíduos, não criando, entretanto, entraves ao uso inovador e revolucionário de dados, é de extrema importância. Isto é a chave para encontrar esse equilíbrio entre a proteção de dados pessoais e a promoção da inovação. O RELX Group felicita o governo brasileiro por incluir conceitos modernos de privacidade no anteprojeto, bem como iniciar um processo de consulta abrangente. O RELX Group apoia a criação de um órgão competente de proteção de dados, o reconhecimento da importância de permitir que os dados fluam através das fronteiras, bem como a inclusão do conceito de "boas práticas", onde as empresas podem criar mecanismos para implementar os requisitos da lei e demonstrar o seu cumprimento. No entanto, acreditamos também que há seções que requerem esclarecimentos adicionais ou modificações.

Comentários específicos:

Art. 2º Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede e do país onde esteja localizado o banco de dados, desde que:

II – os dados pessoais objeto do tratamento tenham sido proposital ou conscientemente coletados de ou sobre os indivíduos no território nacional.

Gostaríamos de sugerir linguagem para indicar que a lei só se aplica quando o operador tem como público-alvo especificamente residentes brasileiros, ou que os dados foram propositadamente coletados dentro do território nacional e, portanto, o operador sabe ou tem motivos para saber que os dados pessoais foram coletados sobre residentes brasileiros ou dentro do território nacional. Empresas oferecem serviços, como no nosso caso de produtos de triagem, aonde não é possível identificar as origens dos dados pessoais enviados pelo usuário final do produto. Como tal, é impossível identificar,

com certeza, as leis de proteção de dados internacionais cuja conformidade é necessária a menos que os operadores sejam informados.

Art. 2º Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede e do país onde esteja localizado o banco de dados, desde que:

§ 3 ~~É vedado aos~~ O tratamento de informações pessoais realizado por órgãos públicos ou entidades públicas ~~efetuar a transferência de dados pessoais constantes de bases de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto em casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado.~~ deve ser feito de forma transparente e com respeito a intimidade, vida privada, honra e imagem das pessoas, bem como as liberdades e garantias individuais.

I - As informações pessoais, a que se refere este artigo, relativas a intimidade, vida privada, honra e imagem podem ter sua divulgação ou acesso por terceiros autorizados por disposições legais ou consentimento expresso da pessoa a que se referem.

II – O consentimento mencionado no inciso I do parágrafo 3 não será exigido quando as informações forem necessárias para os casos constantes na Lei 12.527, de 18 de novembro de 2011, no artigo 31, Parágrafo 3, incisos I, II, III, IV e V.

E

Art. 24. A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado dependerá de consentimento livre, expresso, específico e informado do titular, salvo:

I - Nas hipóteses de dispensa do consentimento previstas ~~nesta~~ na Lei 12.527, de 18 de novembro de 2011, no Artigo 31, Parágrafo 1, inciso II e Parágrafo 3, incisos I, II, III, IV e V;

II – nos casos de uso compartilhado de dados previsto no inciso XVII do art. 5º, em que será dada publicidade nos termos do §1º do art. 6º; ou

III – quando houver prévia autorização de órgão competente, que avaliará o atendimento ao interesse público, a adequação e a necessidade da dispensa do consentimento.

No mundo todo, a falta de transparência e acesso aos registros do governo tem permitido que a corrupção, ineficiência e desperdício continuem sem comprovação na esfera pública. A lei brasileira de acesso à informação (Lei Nº 12.527 de 18 de novembro de 2011) marcou um passo importante para maior transparência, ao fornecer uma estrutura mais robusta para abranger o acesso à informação. A lei apresenta linguagem eficaz sobre o direito fundamental para acessar informações, especialmente com relação à divulgação de informações de interesse público. O objetivo do governo brasileiro deve ser de criar uma legislação de proteção de dados que aplica políticas equilibradas de privacidade e acesso, e que seja o mais eficiente e justa possível.

O Artigo 2, Parágrafo 3 e o artigo 24, incisos I, II e III do anteprojeto não estão em completa harmonia com a linguagem encontrada na lei de acesso à informação do Brasil, especificamente o Artigo 31, inciso II[1] e o Parágrafo 3[2]. Recomendamos uma mudança na linguagem para garantir o equilíbrio entre

[1] *Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.*

privacidade e o acesso a dados públicos. O anteprojeto não determina de maneira adequada as exceções previstas na Lei 12.527. De maneira ideal, o Artigo 2, Parágrafo 3 e Artigo 24, inciso I do anteprojeto deveriam ter linguagem similar, como sugerido acima.

A fim de encontrar este equilíbrio, países como Irlanda, Nova Zelândia, Eslovênia e Estados Unidos criaram leis de direito a acesso à informação que preveem critérios para determinar se as informações pessoais devem ser divulgadas. Este teste pode determinar a divulgação de informações, se for determinado que o interesse público na divulgação é mais importante do que o interesse privado. Isto permite que árbitros independentes, tais como tribunais ou *ombudsman* avaliem os diferentes valores e decidam caso a caso. Por exemplo, os interesses de acesso e privacidade poderiam ser beneficiados ao atrasar o acesso a determinados documentos até que uma investigação seja concluída. Em outros casos, conforme visto no Artigo 6, Parágrafo 2 da lei brasileira, bem como no Reino Unido e nos Estados Unidos, a remoção ou redação de informações particularmente confidenciais em documentos protegem os interesses de privacidade do indivíduo e é preferível do que negar o acesso por completo. O anteprojeto deveria incluir uma linguagem que reconheça que o acesso aos registros públicos tem um valor de interesse público. O reconhecimento da proteção do interesse público deve ser visto neste anteprojeto de lei da mesma maneira que é tratado no Artigo 31, Parágrafo 3, inciso V da lei de acesso à informação. Aqui estão alguns exemplos de como o acesso aos registros públicos pode beneficiar a sociedade:

- Pesquisa: O anteprojeto cria uma exceção importante, nos termos do Artigo 11, inciso IV, relacionada à pesquisa que utiliza informações públicas para realização de estudos em saúde pública, trânsito, segurança, qualidade ambiental, crimes e governança. O acesso aos dados públicos permite que cientistas façam descobertas que beneficiarão a população como um todo. Com cada vez mais dados sendo coletados digitalmente, há uma oportunidade para a integração de cuidados clínicos e de pesquisa. Esses dados fornecem grande potencial para extração de conhecimento útil para conseguir cuidar melhor dos indivíduos e o maior valor para o dinheiro gasto. Em todo o mundo, já vemos resultados na melhoria do acompanhamento e na resposta às epidemias e direcionamento de serviços, tais como de detecção do câncer em populações específicas. O aumento do volume de dados também acelera a pesquisa. Estudos, que antes exigiam décadas de coleta de dados das populações selecionadas em cenários experimentais, agora podem ser realizados em apenas alguns meses pelo processamento de grandes conjuntos de dados, produzindo resultados mais generalizáveis. Abordar a anonimização, que já é reconhecida no Artigo 11, inciso IV e deve ser refletida no Artigo 5, inciso I (ver abaixo), será significativo para responder às preocupações de privacidade na área da saúde e pesquisa para o bem público. Além disso, o reconhecimento de que a pesquisa jurídica também é outra área de interesse público importante que deve ser incluída no Artigo 11, inciso IV.

- Autenticação de identidade e prevenção à fraude: Fraude é um problema crescente em todo o mundo. Na área da saúde, a análise de dados díspares espalhados por todo o sistema de saúde pode ajudar a identificar a fraude, abuso e desperdício, o que é de interesse público Esses dados são uma combinação de dados não tratados do sistema de saúde e de bancos de dados de registros públicos. As tecnologias e análises orientadas por dados podem detectar e revelar indicadores de fraude médica e abuso, identificando padrões e anomalias em dados

---

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

[2] *§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:*
I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
III - ao cumprimento de ordem judicial;
IV - à defesa de direitos humanos; ou
V - à proteção do interesse público e geral preponderante.

encontrados em registros públicos. Nos Estados Unidos, alguns pacientes que receberam alta do hospital têm o tratamento domiciliar como um benefício. O FBI (Federal Bureau of Investigation) trabalhando com parceiros do setor privado descobriu uma operação de um indivíduo que, em cinco anos, roubou mais de US$ 20 milhões do Medicare, sistema de seguros de saúde gerido pelo governo dos Estados Unidos. Ele obteve informações pessoais de centenas de beneficiários do Medicare e utilizou esses dados para inscrevê-los como pacientes de tratamento domiciliar das empresas que ele administrava. Ele orientou a sua equipe para alterar os registros dos pacientes, assinar pedidos médicos fraudulentos, fazer diagnósticos incorretos de pacientes com problemas médicos que eles não tinham, e cobrou por tratamentos desnecessários. Geralmente, os fraudadores falsificam documentos para receber pagamentos ilegais no setor de tratamento domiciliar. Uma das principais ferramentas para prevenir fraudes como estas é a verificação e autenticação de identidade. Essas ferramentas contam com o uso das informações contidas em registros públicos. Além de ajudar a combater a fraude na área da saúde, ferramentas de autenticação de identidade ajudam a dissuadir a fraude em outras áreas também, como roubo de identidade, benefícios de pensão, assistência pública e fraude fiscal.

- Crianças desaparecidas: Cada ano, milhares de crianças desaparecem ao redor do mundo. Mais de três quartos de todas as crianças sequestradas são assassinadas nas três primeiras horas após o seu desaparecimento. Existem vários programas no mundo todo que envia informações sobre a criança desaparecida para determinados indivíduos e locais. O acesso aos registros públicos leva à disseminação mais rápida de informações e até mesmo o retorno dessas crianças à segurança.

- Prevenção da lavagem de dinheiro: A lavagem de dinheiro é um fenômeno global, evidente em muitas partes do mundo. As técnicas variam de movimentação simples de grandes quantidades de dinheiro nas fronteiras a técnicas mais sofisticadas ocultas em operações de comercio exterior. Conforme o comércio avança, aumenta a ameaça de lavagem de dinheiro neste âmbito. O principal método pelo qual os criminosos lavam dinheiro é por meio de transferência de valores de produtos comercializados. Por exemplo, se traficantes de drogas no México querem lavar dinheiro, eles considerariam entrar em uma operação comercial obtendo uma carta de crédito. Eles poderiam criar uma empresa de importação fictícia no Brasil que 'compraria' produtos de um exportador no México e pagaria mais do que os preços normais por determinado produto. O importador pagaria os produtos inflacionados através de um banco para o vendedor no México. Este vendedor também poderia ser uma empresa de 'fachada' com sede no México. O vendedor no México receberia então os valores através de um banco local. Do ponto de vista do banco, a operação seria adequada, uma vez que os documentos relevantes foram utilizados. No entanto, o valor dos produtos foi adulterado, resultando em transferência de dinheiro através da comercialização. Há ocorrências destes negócios acontecendo globalmente. Por que isso é significativo? A lavagem de dinheiro pode ser minimizada com os bancos revisando os negócios que foram financiados e realizando verificações de *due diligence* em seus clientes a fim de determinar a legitimidade desses negócios. Os órgãos reguladores estão cada vez mais focados em garantir que bancos identifiquem para onde os produtos estão sendo enviados; qual transporte será utilizado; e se os produtos estão potencialmente servindo para fins de dupla utilização. Ao saber mais sobre clientes empresariais novos e existentes, maus agentes vão aprender rapidamente que o comércio exterior, por exemplo, não é um caminho atrativo para a lavagem de seus ganhos ilícitos.

Os casos acima mencionados são apenas alguns exemplos do uso benéfico de registros públicos que contenham dados pessoais. Usos de interesse público costumam abranger emprego, serviços de verificação de identidade e crédito, prevenção ou investigação de fraude e até mesmo o uso de dados imobiliários para facilitar o funcionamento eficiente do mercado imobiliário. O anteprojeto deve considerar uma linguagem similar a da lei de acesso à informação, onde as agências governamentais podem fornecer dados pessoais a pessoas físicas ou jurídicas sem obter os consentimentos das pessoas em

causa se os órgãos determinarem que isso é para o bem comum, contanto que esses destinatários utilizem os dados em conformidade com a lei.

Art. 5º Para os fins desta Lei, considera-se:

I – dado pessoal: dado relacionado à pessoa natural identificada ou razoavelmente identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos;

Parágrafo 1 – dados anônimos ou descaracterizados estão excluídos desta lei.

Dados anônimos ou descaracterizados referem-se aos dados pelos quais não é possível estabelecer uma ligação com um indivíduo específico. Esta é uma ferramenta importante para empresas e pesquisadores onde os elementos identificáveis dos dados pessoais são removidos para torná-los seguros em termos de privacidade, mantendo ainda o seu valor comercial e científico. Nesses casos, não há fundamento suficiente para acreditar que as informações possam ser utilizadas para identificar um indivíduo. Embora os dados sejam geralmente coletados para uma única finalidade, há um número crescente de casos nos quais a análise de dados leva a descobertas importantes que beneficiam a sociedade em geral. Por exemplo, os dados de telefones celulares em grande escala podem ajudar planejadores urbanos e engenheiros a compreender melhor os padrões de tráfego e, assim, projetar redes viárias que minimizarão o congestionamento. Nesse caso, o conjunto de dados inclui informações pessoalmente identificáveis, mas essas informações podem ser utilizadas para identificar padrões e tendências e auxiliar na tomada de decisões. A descaracterização e a anonimização podem ser realizadas de forma eficaz e devem ser excluídas do âmbito da aplicação deste anteprojeto, desde que a possibilidade de identificação de um indivíduo seja insignificante ou inexistente.

O anteprojeto também deve considerar o custo, a dificuldade, a natureza prática e a probabilidade de que os dados possam identificar o indivíduo. Sugerimos que de acordo com os procedimentos padrão de funcionamento e realidades técnicas, este artigo se concentre nos dados relativos a uma pessoa ou indivíduo razoavelmente identificável, já que em vários cenários a identificação de qualquer indivíduo seria tecnicamente impossível ou muito improvável. Por não incluir dados anônimos e descaracterizados no âmbito deste projeto de lei, o governo brasileiro estaria incentivando usos novos e inovadores.

Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando o tratamento for indispensável para:

I - cumprimento de uma obrigação legal pelo responsável;

II - tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública;

III - execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular, observado o disposto no § 1º do art. 6º;

IV - realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;

V - exercício regular de direitos em processo judicial ou administrativo;

VI - proteção da vida ou da incolumidade física do titular ou de terceiro;

VII – tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades

sanitárias;

VIII – O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

IX – O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º

§ 1º Nas hipóteses de dispensa de consentimento, os dados devem ser tratados exclusivamente para as finalidades previstas e pelo menor período de tempo possível, conforme os princípios gerais dispostos nesta Lei, garantidos os direitos do titular.

§ 2 Nos casos de aplicação do disposto nos incisos I e II, será dada publicidade a esses casos, nos termos do Parágrafo 1 do Art. 6.

§ 3 No caso de descumprimento do disposto no §2, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado.

A lista atual de dispensa de consentimento é muito limitada e não permite várias importantes funções econômicas, desde a prevenção à fraudes até investigações criminais.

Na União Europeia (Diretiva 95/46/CE de proteção de dados, Artigo 7), os dados pessoais podem ser tratados somente quando:

a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento; ou
b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou
c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou
d) O tratamento for necessário para a protecção de interesses vitais da pessoa em causa; ou
e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ou
f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º

Recomendamos a inclusão de isenções semelhantes à linguagem encontrada nos incisos E (Interesse Público) e F (Interesse Legítimo) da Diretiva de Proteção de Dados da UE.

Uma exceção no caso de interesse público é significativa para o exercício de uma autoridade oficial ou na execução de uma tarefa pública. Por exemplo, autoridades fiscais, como a Receita Federal do Brasil, podem coletar e processar a declaração de imposto de renda de um indivíduo para determinar e confirmar o valor do imposto a ser pago. Outro exemplo é uma associação médica profissional responsável pela realização de procedimentos disciplinares contra membros no caso de fraude médica e abuso. Estes são todos casos de interesse público, onde um indivíduo, como o médico que cometeu fraude, se for dada a opção, não autorizaria a inclusão das suas informações pessoais em um banco de dados para esta finalidade. Os casos como esses acima são benéficos para a sociedade em geral e devem ser permitidos na legislação brasileira.

Gostaríamos também de recomendar a inclusão de linguagem que permite o tratamento para fins de interesses legítimos adotados pelo responsável. A ideia do interesse legítimo é buscar o equilíbrio entre

a proteção dos indivíduos em relação ao tratamento dos seus dados pessoais e a utilização desses dados. O anteprojeto deve criar uma estrutura que proteja os direitos e as liberdades dos indivíduos e, ao mesmo tempo, permita o fluxo livre dos dados necessários para a criação de novos negócios e para o crescimento contínuo da economia digital no Brasil. Alguns contextos comuns incluem a execução de processos jurídicos, incluindo a cobrança de dívidas por meio de procedimentos fora do tribunal, a prevenção à fraude, uso indevido de serviços, ou a lavagem de dinheiro, entre outros. O governo brasileiro deve garantir que a nova lei não proíba a existência de determinadas atividades econômicas. Estes são exemplos de interesses legítimos que devem ser permitidos sob a nova legislação proposta.

Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando os dados são provenientes de órgãos reguladores ou jurídicos, ou quanto o tratamento for indispensável para:

E

Art. 12. É vedado o tratamento de dados pessoais sensíveis, salvo:

II – sem fornecimento de consentimento do titular, quando os dados forem de acesso público irrestrito ou quando os dados são provenientes de órgãos reguladores ou jurídicos ...

E

Art. 15. Os dados pessoais serão cancelados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades ou categorias de dados:

III- dados provenientes de órgãos reguladores ou jurídicos;

E

Art. 19. O titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil ou avaliar aspectos de sua personalidade.

Parágrafo 2 – Ficam ressalvados os tratamentos de dados pessoais necessários ao cumprimento de obrigação legal ou quando os dados são provenientes de órgãos reguladores ou jurídicos.

E

Art. 32. No caso de transferência internacional de dados de um país estrangeiro para o Brasil, somente é permitido o seu tratamento no território nacional quando nas operações realizadas naquele país tiverem sido observadas suas normas relativas à obtenção de consentimento, exceto quando os dados são provenientes de órgãos reguladores ou jurídicos.

Os dados provenientes de órgãos reguladores ou jurídicos devem ser excluídos de várias instâncias mencionadas no anteprojeto de lei, tais como consentimento (artigo 11), dados pessoais sensíveis (artigo 12), conservação de dados (artigo 15) e direito à solicitar revisão (artigo 19). A utilização de dados provenientes de órgãos reguladores ou jurídicos está sujeita às leis vigentes. Uma das nossas empresas utiliza listas de sanções de pessoas ou grupos terroristas emitidas por autoridades, tais como OFAC (Office of Foreign Assets Control dos Estados Unidos), bem como informações sobre Pessoas Expostas Politicamente (PEP). Essas informações são essenciais para investigar e prevenir crimes financeiros, como lavagem de dinheiro e corrupção. As informações utilizadas pela nossa empresa precisam refletir as listas publicadas pela autoridade emissora. Como tal, a pessoa em causa deve, por exemplo, discutir a sua presença na lista diretamente com a autoridade emissora, e não conosco. Sugerimos que os Artigos 11, 12, 15 e 19 contenham uma exceção para dados fornecidos por órgãos reguladores ou jurídicos.

Art. 28. A transferência internacional de dados pessoais somente é permitida para países que proporcionem nível de proteção de dados pessoais equiparável ao desta Lei, ressalvadas às seguintes exceções:

I - Quando a transferência for necessária para a cooperação judicial internacional entre órgãos público de inteligência e de investigação, de acordo com os instrumentos de direito internacional;

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

III - Quando órgão competente autorizar a transferência, nos termos de regulamento;

IV - Quando a transferência resultar de um compromisso assumido em acordo de cooperação internacional;

V - Quando a transferência for necessária para a execução de política pública ou está atribuição legal do serviço público, sendo dada publicidade nos termos do § 1 do art. 6.

Parágrafo único. O nível de proteção de dados do país deve ser avaliado por órgão competente, que levará em conta:

I - Normas gerais e setoriais da legislação em vigor do país de destino;

II - Natureza dos dados;

III - Observância dos princípios gerais da proteção de dados pessoais previstos nesta lei;

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

V - outras circunstâncias específicas relativas à transferência.

E

Art. 30. A autorização referida no inciso III do caput do art. 28 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 para uma transferência específica, em cláusulas contratuais-padrão ou em normas corporativas globais, nos termos do regulamento.

§ 1 Órgão competente poderá elaborar cláusulas contratuais-padrão, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária, independente de culpa, de cedente e cessionário.

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

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

Para evitar uma interrupção do comércio internacional, propomos uma disposição que regeria o período após a data de vigência desta Lei, mas antes que as cláusulas contratuais-padrão sejam aprovadas pelo órgão competente. Esse disposto permitirá que: Enquanto o órgão competente não publicar as cláusulas

contratuais-padrão que serão utilizadas na transferência de dados pessoais para um país nos termos deste Artigo, transferências de dados pessoais podem acontecer de acordo com o Artigo 28 contanto que um contrato legalmente vinculativo esteja em vigor ou que exista uma norma reconhecida no setor ou internacionalmente entre o cedente e cessionário. O cedente estrangeiro precisa tratar e proteger os dados pessoais em conformidade com a lei brasileira, as normas reconhecidas no setor e internacionalmente que se aplicariam se os dados ainda estivessem no Brasil, incluindo a conformidade com as provisões referentes à segurança de dados pessoais, limitações sobre o tratamento de dados pessoais e usos pelo cedente, bem como um compromisso em cooperar com as solicitações do titular para exercer seus direitos com relação aos seus dados pessoais. Haveria uma exceção no caso de dados provenientes de órgãos reguladores ou jurídicos (mencionado acima).

Seção II e III – Órgão competente

O anteprojeto de lei delega várias responsabilidades a um "órgão competente" que não existe e o anteprojeto não trata de sua criação. Da nossa experiência em outras partes do mundo, o RELX Group é favorável a existência de um órgão competente único com orçamento e funcionários próprios. Este órgão competente deve ser criado simultaneamente com essa estrutura de privacidade.

O órgão competente terá a capacidade de investigar e intervir, e possuirá poder consultivo. Este poder consultivo é importante para as empresas, porque o órgão terá o conhecimento apropriado para interpretar a lei de proteção de dados pessoais em cenários diferentes. Por último, a autoridade competente também serve como um *ombudsman*, investigando reclamações individuais contra a má administração de empresas, bem como de autoridades públicas.

Conclusão

Gostaríamos de agradecer a oportunidade de compartilhar os nossos comentários e esperamos poder continuar contribuindo para políticas públicas no Brasil na âmbito de privacidade e dados pessoais que permitam que o país continue a crescer economicamente e inovar, enquanto garantindo privacidade a seus cidadãos.

Atenciosamente,

Departamento de Relações Governmentais
RELX Group