FGV DIREITO SP
ESCOLA DE DIREITO DE SÃO PAULO

Grupo de Ensino e Pesquisa em Inovação – GEPI

Coordenação:
Profa. Mônica Steffen Guise Rosina
Prof. Alexandre Pacheco da Silva

Equipe de Pesquisa:
Carla Segala Alves
Eduardo Lazzari
Luis Fernando Prado Chaves
Maria Eugênia Geve Lacerda
Ricardo Harris Jonhston
Rodrigo Moura Karolczak

Contribuição ao Anteprojeto de Proteção de Dados Pessoais

Sumário:

Quem é o GEPI e por que ele quer contribuir

O Grupo de Ensino e Pesquisa em Inovação (GEPI) foi criado em 2011 na Escola de Direito de São Paulo da Fundação Getulio Vargas (FGV Direito SP) pela Professora Mônica Steffen Guise Rosina com o objetivo de aprofundar os debates sobre como novas tecnologias podem transformar o arcabouço jurídico-institucional do Brasil.

Desde o início de suas atividades, o GEPI voltou seus esforços de pesquisa à regulação da Internet no Brasil, identificando no debate um ambiente profícuo em reflexões sobre qual o modelo normativo mais adequado para enfrentar os desafios ao desenvolvimento tecnológico na Internet.

Em quatro anos, o GEPI buscou expandir suas linhas de pesquisa e criar instâncias de debate sobre a relação entre Direito e Inovação Tecnológica dentro da FGV Direito SP. Foram criadas atividades de ensino no âmbito da graduação (Laboratório de Empresas Nascentes de Tecnologia – LENT), do programa de intercâmbio internacional (*Digital Democracy*), e do mestrado profissional (Direito e Novas Tecnologias). Além disso, o GEPI ampliou suas linhas de pesquisa, que em 2011 eram 2, passando para 5 em 2015. São elas:

(i) Democracia digital;
(ii) Flexibilização de direitos autorais;
(iii) Empreendedorismo e empresas nascentes de base tecnológica;
(iv) Fashion law; e
(v) Privacidade e proteção de dados pessoais.

No contexto de sua linha de pesquisa sobre privacidade e proteção de dados pessoais, o GEPI vem acompanhando os esforços realizados pelo Ministério da Justiça, com especial destaque para a Secretaria de Assuntos Legislativos e para a Secretaria Nacional do Consumidor, em criar um espaço de ampla participação e debate sobre qual modelo jurídico de

proteção de dados pessoais a sociedade brasileira considera mais adequado para a Internet.

Nesse sentido, o GEPI acredita que pode participar do debate por meio de uma avaliação sobre quais são as principais fragilidades do Anteprojeto de Proteção de Dados Pessoais elaborado pelo Ministério da Justiça. Desde já deixamos claro que o Anteprojeto guarda em si muitas virtudes, como a criação de um rol de definições, a ideia de um órgão de fiscalização, um regime jurídico para a cessão de dados para terceiros, dentre outros. Contudo, acreditamos que a melhor forma de contribuição para o aprimoramento do documento é explicar quais são suas fragilidades e oferecer sugestões de mudança.

A presente contribuição foi fruto do trabalho de pesquisadores do GEPI que trabalham em regime de tempo integral na FGV Direito SP, bem como pelas contribuições de alunos de graduação e alunos da pós-graduação Lato Senso em propriedade intelectual.

Foram escolhidos três temas para a contribuição do GEPI:

(i) Modelo de consentimento;
(ii) Papéis do Estado na proteção de dados pessoais;
(iii) Transferência internacional de dados;

Para cada um dos temas selecionados, a equipe do GEPI promoveu uma pesquisa acadêmica em artigos científicos, experiências internacionais de regulação da proteção de dados pessoais e modelos de gestão de dados pessoais. Todos os materiais utilizados têm a sua indicação específica no final do documento.

Este documento, mesmo oferecendo uma contribuição acadêmica para o debate público do Anteprojeto, adotou uma estrutura menos formal e mais fluída de argumentação e exposição de dados empíricos capazes de qualificar o texto do Anteprojeto de proteção de dados pessoais. Por isso, a

estrutura de nosso texto, bem como o estilo de apresentação de nossos argumentos, se distanciam da forma tradicional da escrita acadêmica.

Por fim, a presente contribuição do GEPI foi apresentada a acadêmicos (FGV Direito Rio e UFMG), profissionais do mercado (Google, Facebook e Microsoft), sociedade civil (InternetLab, Camara-e.net e Artigo 19) e escritórios de advocacia (Opice Blum, Pinheiro Neto, entre outros) na Oficina de Discussão do Anteprojeto de Proteção de Dados Pessoais realizada no dia 12 de junho de 2015 na FGV Direito SP.

O documento final é de total responsabilidade da equipe do GEPI, tendo buscado incorporar as contribuições que o Grupo considerou pertinentes às suas avaliações.

Modelo de Consentimento

Antes de iniciarmos com a nossa contribuição ao Anteprojeto de Proteção de Dados Pessoais, julgamos necessário realizar dois breves comentários.

Compreendemos que o Anteprojeto busca legislar sobre um conjunto vasto de atividades que se utilizam de dados pessoais, tendo um escopo evidentemente maior do que apenas o meio digital. Assim, a contribuição do GEPI deve ser vista como um documento que se dedica à reflexão sobre proteção de dados pessoais no contexto da Internet, e não em outros serviços que, mesmo eletrônicos, não se localizam na rede mundial de computadores (e.g. bancos de dados privados).

Ao mesmo tempo, na elaboração do presente documento, o Grupo teve o cuidado de atentar para o conjunto normativo vigente no ordenamento jurídico brasileiro que já versa sobre proteção de dados pessoais, com especial atenção para o texto do Marco Civil da Internet (Lei n.º 12.965/2014).

Feitas as nossas considerações iniciais, a seção I do capítulo 2 do Anteprojeto de Proteção de Dados Pessoais estabelece como requisito para a realização de atividades de tratamento de dados pessoais a obtenção do consentimento do usuário titular.

Na delimitação dos elementos necessários à oferta do consentimento pelo usuário, o art 7º, além de prescrever que o consentimento não pode ser condição de fornecimento de produto ou serviço (§1º), apresenta quais são os quatro elementos essenciais que devem estar presentes quando da oferta do consentimento, são eles: (i) livre; (ii) específico; (iii) expresso; e (iv) informado.

Desta forma, cometeria um ato ilícito a empresa que realizasse atividade de tratamento de dados e não obtivesse o consentimento do usuário segundo a forma prescrita no Anteprojeto.

A este respeito, acreditamos que o Anteprojeto apresenta três problemas relevantes que merecem ser discutidos a seguir.

Crítica 1: O modelo de consentimento previsto no art. 7º do Anteprojeto aposta na premissa de que quanto mais informação for oferecida ao usuário, melhor será a sua decisão sobre a gestão de seus dados. Contudo, há indícios de que esta premissa é falsa, comprometendo o modelo escolhido.

Crítica 2: O modelo de consentimento previsto no art. 7º se baseia em documentos como termos e condições de uso de serviço e políticas de privacidade para a oferta de informação e obtenção do consentimento do usuário. Todavia, há indícios de que usuários não leem ou não incorporam as informações ali presentes em sua tomada de decisão.

Crítica 3: O Anteprojeto não estabelece critérios suficientes para a definição de indispensabilidade de dados prevista nos incisos do art. 11, criando um cenário de incerteza sobre o tratamento de dados.

A escolha por um modelo de regulação jurídica do tratamento de dados pessoais baseado na obtenção do consentimento tem como pressuposto fundamental a ideia de que o usuário é capaz de tomar decisões informadas sobre a gestão de seus dados pessoais. Quanto mais poder de controle do fluxo de informações que estão sendo tratadas por empresas, mais protegido estará o usuário.

Há pelo menos dois equívocos neste pressuposto.

Em primeiro lugar, não é verdade que quanto mais informações são recebidas pelo usuário, mais protegido ele estará. Em alguns cenários, o efeito é o oposto, pois são tantas informações a serem lidas, interpretadas, assimiladas pelo usuário, que passa a não ter condições de incorporá-las em sua tomada de decisão (NISSENBAUM, 2011: 34).

O modelo de consentimento, ou também chamado de *notice and consent* ou *notice and choice*, guarda em si o "paradoxo da transparência", definido como o fenômeno de oferta de um grande volume de informações que em teoria permitiria ao titular de dados pessoais a melhor decisão possível, contudo, na prática, tais informações não são assimiladas pelo seu volume e por sua tecnicalidade (NISSENBAUM, 2011: 36).

Hoje, a oferta de informações sobre tratamento de dados é feita a partir de dois documentos principais: (i) termos de uso e condições de serviços digitais; (ii) políticas de privacidade. Não parece que gerar mais dispositivos, cláusulas e seções nestes documentos sobre a operação de tratamento de dados pessoais seja o mais adequado como estratégia de proteção do usuário.

O Chairman da *Federal Trade Commission* (FTC) dos Estados Unidos da América, Jon Leibowitz[1], ao analisar o modelo de *notice and consent,* afirma que inicialmente políticas de privacidade até poderiam parecer uma boa ideia para informar usuários sobre a gestão de seus dados pessoais. Contudo, o que se observou é que na prática raros usuários leem ou compreendem o conteúdo deste tipo de documento.

Sob este enfoque, quanto mais documentos, cláusulas, seções, dispositivos, maior a chance do usuário simplesmente ignorar todo o texto oferecido por meio de uma política de privacidade ou um termo de uso, pois ele ficará perdido em meio a um mar de informações com dificuldades em navegar.

Na verdade, surpreende a contínua aposta de que usuários se engajem na leitura e compreensão de tais documentos, uma vez que as atividades de tratamento de dados têm cada vez se tornado mais complexas. Daniel Solove chamou este modelo de *privacy self-management*, pois pressupõe

[1] A passagem foi extraída dos comentários do *Commissioner Jon Leibowitz* no evento *"So Private, So Public: Individuals, the Internet & The Paradox f Behavioral Marketing"* em 1 de novembro de 2007 no FTC Town Hall Meeting. Para conferir na íntegra consulte a página 4 da mesa *"Behavioral Advertising: Tracking, Targeting & Technology"*. Disponível em: <https://www.ftc.gov/sites/default/files/documents/public_statements/so-private-so-public-

que o usuário tem condições de fazer a auto-gestão de sua privacidade (2013; 1886).

Solove questiona até que ponto este modelo de auto-gestão da privacidade responde à complexidade da proteção de dados pessoais do usuário na medida em que outorga ao usuário boa parte da tomada de decisão sobre a gestão de seus dados, sendo que há limites cognitivos de compreensão do que está envolvido em atividades de tratamento de dados pessoais (2013: 1886).

Vale a menção neste ponto de que vislumbramos que o APL não é completamente omisso quanto ao problema do volume de informações oferecidas ao usuário, uma vez que prevê no parágrafo 4º do art. 7º que o consentimento deverá ser fornecido de forma destacada das demais cláusulas.

Contudo, mesmo que o consentimento seja destacado, todas as demais informações que deveriam servir como base para a tomada de decisão do usuário ainda estarão dissipadas em extensos documentos com linguajar jurídico e difíceis de serem incorporados na tomada de decisão do usuário.

Smit, Noort e Voorveld (2014: 21) indagam:

> "O que significa consentimento informado em uma audiência não bem-informada? [...] Nós sugerimos uma abordagem dual aqui, não só para informar usuários (mais e melhor), mas também para reduzir preocupações sobre privacidade online, especialmente em grupos mais velhos e menos escolarizados[2]." (tradução nossa)

É latente na produção acadêmica a constante indicação de que poucos usuários leem políticas de privacidade de sites (JENSEN, POTTS, JENSEN,

[2] Do original, em inglês: "what does informed consent mean within a not-well-informed audience? [...] We suggest a dual approach here, not only to inform users (more and better) but also to reduce concerns about online privacy, especially in the older and less-educated groups."

2005; MCDONALD, CRANOR, 2008; SMIT, NOORT, VOORVELD, 2014; DE LIMA, LEGGE, 2014).

Contraditoriamente, alguns estudos também demonstram que a mera existência de uma política de privacidade leva confiança ao usuário, muito embora seu conteúdo não seja regularmente acessado (JENSEN, POTTS, JENSEN, 2005; SMIT, NOORT, VOORVELD, 2014).

Conforme pesquisa de McDonald e Cranor (2008, p. 560), a leitura de todas as políticas de privacidade também não seria desejável para o usuário médio. Para um usuário que acessa por volta de 66 novos sites ao mês, as autoras ponderam que:

> […] usando a estimativa média de 244 horas por ano para ler políticas de privacidade por pessoa, significaria uma média de 40 minutos por dia. Isto é pouco mais do que metade dos 72 minutos por dia estimados que pessoas gastam usando a Internet.[3]

A tendência também seria válida para os processos de aceitação ou rejeição de cookies. Segundo De Lima e Legge (2014, p. 69), é possível que os usuários aceitem cookies passivamente para poupar tempo ou para acessar o site de forma integral. Assim, os autores apontam para "um risco muito real de *default inertia* em que pessoas simplesmente rejeitam ou aceitam cookies *by default*, por causa desta falta de entendimento"[4] (DE LIMA, LEGGE, 2014, p. 71).

Os selos de certificação sofrem um processo semelhante, sendo sua existência, e não necessariamente conteúdo, fundamental para passar uma imagem de confiança a usuários. Em suma, os referenciais de confiança dos

[3] Do original, em inglês: "[…] using the point estimate of 244 hours per year to read privacy policies per person means an average of 40 minutes a day. This is slightly more than half of the estimated 72 minutes a day people spend using the Internet."
[4] Do original, em inglês: "[…] a very real danger of 'default inertia' whereby people simply reject or accept cookies by default, because of this lack of understanding."

usuários tendem a ser mais subjetivos, conforme Jensen, Potts e Jensen (2005, p. 220):

> "O que visualizamos foi clara evidência de como pessoas usam estes fatores [TRUSTe, rankings de políticas de privacidade, e-mail para contato, telefone para contato, endereço para contato, bandeiras de cartão de crédito, SSL e promoções] para determinar confiabilidade, não baseado em fato mas sim em aparência e primeira impressão. Políticas [de privacidade] são importantes, não apenas por o que dizem, mas porque elas estão lá.[5]" (tradução nossa)

Em segundo lugar, as informações disponibilizadas em termos e condições de uso não têm servido para orientar efetivamente o comportamento de usuários preocupados com o uso de seus dados.

A literatura acadêmica vem se debruçando sobre a relação entre a proteção de dados pessoais e o comportamento online de usuários, em particular classificando os usuários da Internet dentro de três grandes perfis, geralmente distinguindo entre alta, média e baixa preocupação com sua privacidade em ambiente virtual (JENSEN, POTTS, JENSEN, 2005; PARK, CAMPBELL, KWAK, 2012; SMIT, NOORT, VOORVELD, 2014).

Estes estudos [6] apontam que hoje não há uma correlação entre a preocupação do usuário em relação aos seus dados e ações efetivas (e.g.

[5] Do original, em inglês: "What we saw was clear evidence of how people used these factors to determine 'trustworthiness,' not based on fact but rather on appearance and first impression. Policies are important, not just because of what they say, but because they are there."

[6] A menção à estudos empíricos específicos não deve ser lido como um endosso destes e de sua metodologia. Ao contrário, eles nos servem como provocações interessantes sobre percepções consolidadas no âmbito da proteção de dados pessoais, em especial com o paradoxo da transparência. As dificuldades e limites de usuários relacionados aos conhecimentos técnicos, referenciais de confiança e capacidade de controle de seus dados seriam levantados para debater e orientar o desenvolvimento de sites e navegadores, políticas de privacidade de sites e a formulação de políticas públicas quanto aos modelos de consentimento. É necessário ressalvar que estes apontamentos se apresentam válidos principalmente no contexto estadunidense e europeu, geralmente testados e replicados em

alteração na configuração do serviço) no sentido de restringir o uso de seus dados por empresas privadas no âmbito do comércio eletrônico ou da publicidade comportamental.

Há um número reduzido de usuários que domina[7] informações sobre protocolos relevantes para a gestão de seus dados pessoais como o *Platform for Privacy Preferences* (P3P) e ferramentas de monitoramento como *Web bugs* (JENSEN, POTTS, JENSEN, 2005: 212). Enquanto *cookies* são reconhecidos mais frequentemente, suas funcionalidades também são nebulosas para uma significativa maioria de usuários (*Idem*: 212-213).

Em estudo mais recente, Smit, Noort e Voorveld (2014: 21) encontram diferenças de conhecimento sobre publicidade comportamental e *cookies* entre grupos de usuários, mas, no todo, identificam que pessoas têm conhecimento insuficiente sobre publicidade comportamental. Em verdade, os usuários têm dificuldades especialmente na compreensão sobre qual ferramenta está por trás disto (no estudo foi utilizado para coleta a tecnologia *cookie*) e como gerir a coleta de seus dados.

Assim, uma característica em comum entre grupos de usuários é de que "é, portanto, possível que esta segmentação não seja apenas baseada nos conhecimentos dos respondentes sobre riscos, mas em outras estimativas de riscos e sensibilidades"[8] (JENSEN, POTTS, JENSEN, 2005: 213).

Smit, Noort e Voorveld (2014: 20) apontam que o grupo de usuários mais preocupados com sua privacidade necessita "solucionar aspectos emocionais de tomada de riscos online: eles têm menos conhecimento

pequena escala. Ainda assim, as variações específicas podem ser relevadas em favor de um quadro mais geral de usuários comuns.

[7] No estudo de Jensen, Potts e Jensen (2005), apenas 5-6% dos respondentes demonstraram conhecimento a respeito de P3P e Web bugs, enquanto cookies foram reconhecidos por 90% dos respondentes, mas apenas 14% demonstraram conhecimento.

[8] Do original, em ingles: "It is therefore possible that this segmentation is not so much based on the subjects' knowledge of risks, but on other risk estimates and sensitivities."

sobre publicidade comportamental e *cookies*, e têm uma opinião mais negativa sobre este tipo de publicidade segmentada"[9].

Assim, mesmo com muita informação disponível em termos de uso de serviço e políticas de privacidade sobre atividades de tratamento de dados, a falta de conhecimento de usuários quanto às ferramentas simples de proteção de seus dados, como alteração da configuração de serviços como redes sociais, nos leva a crer que a informação disponível não tem contribuído no auxílio à gestão de dados de usuários.

Em última instância, mesmo os usuários insatisfeitos com a coleta e utilização de seus dados em modelos de veiculação de anúncio via publicidade comportamental tendem a permanecer inertes quanto à alteração de sua condição, tomando poucas atitudes frente aos seus dados. Isso nos leva a crer que a aposta em modelo de consentimento não deve priorizar a abundância de informações, mas sim a qualidade da informação oferecida, de modo a reduzir o paradoxo da transparência.

Jensen, Potts e Jensen (2005, p. 223) recomendam o "desenvolvimento de simplificações de políticas [de privacidade], estandartização, ou políticas *machine readable*"[10] para tornar a leitura, ciência e aprovação de políticas de privacidade mais dinâmicas, enquanto também reafirmam que "maior conhecimento público sobre questões de privacidade, as capacidades e limitações de tecnologias de aprimoramento de privacidade, e o significado de políticas [de privacidade] e indicadores de confiança são todos necessários"[11] (Jensen, Potts, Jensen, 2005, p. 226).

McDonald e Cranor (2008, p. 562) apontam para uma direção semelhante, afirmando que "a consolidação da mídia significa que múltiplos sites podem

[9] Do original, em inglês: "[…] addressing the emotional aspects of taking risks online: they had less knowledge about OBA and cookies, and they held a more negative opinion of this type of targeted advertising."
[10] Do original, em inglês: "[…] development of policy simplifications, standardization, or machine readable policies."
[11] Do original, em inglês: "greater public awareness of privacy issues, the capabilities and limitations of privacy-enhancing technologies and the significance of policies and trust indicators are all necessary."

compartilhar uma política de privacidade"[12]. Park, Campbell e Kwak (2012, p. 1025), sugerem que:

> (...) conhecimento sobre riscos de dados e regulações aparentam ajudar a mitigar a tendência de ser passivo sobre a proteção de informações pessoais online [...] isto é, *prompts* (meios de comunicação) e fontes de conhecimento mais robustos são necessárias para munir usuários com a informação e motivação necessárias para se protegerem online[13].

Nesse sentido, para a proteção do usuário, o regime jurídico deve oferecer formas simplificadas e/ou dinâmicas para que ele seja capaz de escolher que informações está disposto a fornecer às empresas pelos produtos e serviços que elas estão lhe oferecendo, tendo ampla liberdade para fazê-lo a partir de uma interface funcional e de fácil manejo.

Mesmo a partir da lógica de obtenção do consentimento de usuários, a proteção de dados pessoais pode adotar diferentes formas de comunicação sobre os riscos inerentes ao tratamento de dados, permitindo que o usuário possa tomar uma decisão efetiva sobre o que deseja fazer com os seus dados.

Há pelo menos três exemplos que podem ilustrar este argumento sobre simplificação e consolidação da mídia de comunicação com o usuário, são eles: (i) AVG PrivacyFix; (ii) Terms of Service; Didn't Read; e (iii) Lightbeam. Cada uma destas ferramentas oferece uma forma mais adequada de oferta e visualização de informações relevantes ao tratamento de dados do que documentos como termos e condições de uso e políticas de privacidade.

[12] Do original, em inglês: "[...] media consolidation means that multiple sites may share one privacy policy."
[13] Do original, em inglês: "[...] knowledge about data risks and regulations seem to help mitigate the tendency to be passive about protecting personal information online [...] That is, more robust prompts and sources of knowledge are needed to equip users with the information and motivation needed to protect themselves online."

O AVG PrivacyFix é uma ferramenta (*plug-in*) de navegadores que permite maior controle ao usuário sobre a sua privacidade facilitando a adequação de opções de configuração presentes nos serviços oferecidos pelas empresas Facebook, Google e LinkedIn.

O aplicativo busca, por meio de uma interface amigável, apresentar para os seus usuários quais são os custos e benefícios de cada configuração de privacidade, deixando a escolha final para o usuário. Sua estratégia é apresentar afirmações simples ao usuário, de fácil compreensão, e, a depender da reação deste, o aplicativo o leva para as opções de configuração do serviço das empresas mencionadas para que o usuário altere dentro do próprio serviço.

Também é possível verificar quais empresas estão monitorando as atividades online de usuários, atualizações de políticas de privacidade ou vazamento de dados recentes. Ao invés de demandar do usuário a leitura de uma cláusula contratual de forma pormenorizada, o software atua como um mediador entre o usuário e as políticas de privacidade destas plataformas.

O principal diferencial do aplicativo é a sua capacidade de traduzir dispositivos contratuais com uma terminologia jurídica para afirmações simples. Ainda se o usuário desejar alterar suas configurações de privacidade, basta que ele clique na opção corrigir e o próprio aplicativo o auxilia a alterar a configuração.

Outra iniciativa que merece destaque é o projeto *Terms of Service; Didn't Read*", que consiste na avaliação e classificação de políticas de privacidade e termos de uso em uma escala de conceitos de A a E. O projeto é transparente, público e aberto, buscando informar o usuário a partir de critérios padronizados de avaliação.

A principal novidade do projeto é também oferecer uma ferramenta de navegação ao usuário como forma de facilitar o seu acesso a dados. Uma vez que o plug-in estiver instalado no navegador do usuário, cada vez que ele acessar determinado site, este terá sua nota veiculada se a equipe do

projeto já tiver examinado a sua política de privacidade.

Apesar de apresentar uma metodologia ainda em desenvolvimento, o simples levantamento resumido de boas e más práticas de sites já é uma contribuição para melhor informar a tomada de decisão de usuários de forma rápida e prática.

Por fim, outra ferramenta importante para a melhora na tomada de decisão do usuário sobre seus dados é o Lightbeam. Da mesma forma que as duas ferramentas mencionadas acima, o Lightbeam é um complemento para navegadores que indica por meio de uma interface gráfica e interativa quais são os terceiros que estão participando de atividades de tratamento dos dados pessoais do usuário.

O intuito do complemento é informar o usuário de maneira transparente sobre os sites que realizam monitoramento via cookies, ou outras ferramentas de monitoramento, mas não necessariamente encoraja usuários a deletar o seu rastro digital. A visualização dos dados é realizada por meio de uma rede de pontos.

Acreditamos que o texto do Anteprojeto deve ser mais explícito sobre a necessidade da adoção de novas formas de apresentação de informações sobre o tratamento de dados. O parágrafo 4º do art. 7º, ao exigir que o consentimento seja fornecido de forma destacada das demais cláusulas contratuais, parece assumir que o principal instrumento que rege a relação entre usuário e entidade que realiza o tratamento são os termos de uso ou políticas de privacidade, o que em nossa visão é um equívoco.

Desta forma, não afirmamos que documentos como termos de uso ou políticas de privacidade são dispensáveis, contudo, não acreditamos que o modelo de consentimento deve ter estes documentos como principal canal de oferta e visualização de informações sobre o tratamento de dados.

Acreditamos que referidos instrumentos criam relações jurídicas importantes e devem ser preservados. É a sua leitura que não deve ser considerada

como pressuposto do sistema, ou seja, não deve ser encarada como algo que o usuário irá se embasar para consentir o uso de suas informações.

Assim, enfatizamos a necessidade de encontrar soluções mais eficientes para a forma de realização do consentimento do usuário, viabilizando a proposta para prestadores de serviço e usuários de forma menos onerosa.

À luz da proposta de Robinson *et al* (2009) para a provisão de dados governamentais abertos, uma solução viável, por exemplo, seria o requerimento de dados *machine readable* referentes aos parâmetros de políticas de privacidade e termos e condições de uso utilizados pelos prestadores de serviço online. A partir da disponibilização pública destes parâmetros, empresas também poderiam competir na oferta de softwares de gestão de privacidade, como algumas efetivamente já o fazem a partir de configurações internas de privacidade, como nos casos Facebook, Google e LinkedIn.

Isto, por um lado, abre um novo espaço de interação e controle do usuário, e, por outro, permite a atuação empresarial dentro de interesses legítimos, mediando a forma da coleta de informações que compõem o universo de segmentos como o de *Big Data*. No entanto, ressalvamos que esta proposta necessita de intensa elaboração mediante atuação do Órgão Competente e debate público, já que definir os parâmetros e como divulgá-los não é tarefa simples ou politicamente neutra.

Outro tópico relevante sobre o modelo de consentimento é a ausência de uma definição dos critérios de indispensabilidade. O parágrafo 1º do art. 7º do Anteprojeto estabelece que o usuário não poderá ser constrangido a oferecer seus dados como condição para o recebimento de produto ou serviço, exceto na hipótese em que determinado dado pessoal seja indispensável para o fornecimento do produto ou serviço.

Acreditamos que os incisos do art. 11 do Anteprojeto não são capazes de sanar algumas dúvidas importantes sobre indispensabilidade de dados, em

especial, para dados que são fundamentais para a prestação de serviços eletrônicos.

Aqui cabe questionar o que se deve entender sobre indispensabilidade de um dado para a prestação de um serviço ou fornecimento de um produto. Isto porque boa parte das empresas que realizam atividades de tratamento de dados tem nessa informação o seu principal ativo. Por essa razão, muitos serviços são oferecidos de forma gratuita na Internet. Indispensabilidade, nesse sentido, pode assumir muitas interpretações.

Em um serviço de navegação e informação sobre trânsito oferecido por meio do aplicativo da *Waze* é difícil definir o limite entre dados dispensáveis daqueles indispensáveis a prestação do serviço. Poderíamos dizer que os dados referentes à geolocalização dos usuários seriam indispensáveis, contudo, não estaríamos seguros em afirmar que os dados de comunicações entre os usuários do aplicativo seriam dispensáveis à prestação do serviço, tendo em vista que podem aprimorar as rotas de tráfego dos demais membros da rede.

Empresas que promovem o tratamento não terão segurança suficiente para saber se as informações que anunciam como essenciais para a oferta do serviço, por exemplo por melhorar a experiência de navegação do usuário, serão também consideradas como indispensáveis, e, portanto, suficientes para serem exigidas como contraprestação para acesso aos serviços.

Desta forma, se o Anteprojeto realiza um esforço de criar definições para termos relevantes ao diploma, acreditamos ser razoável que o texto apresente critérios para avaliação do que pode ser considerado como dado indispensável, evitando o cenário de incerteza que o texto atual parece criar.

Talvez a própria ideia de indispensabilidade de dados pessoais não seja a via mais adequada para o modelo de consentimento, uma vez que temos dúvidas sobre quais critérios poderiam ser utilizados para se diferenciar um dado dispensável daquele indispensável.

Nesse sentido, uma alternativa à indispensabilidade já aplicada na Europa é o interesse legítimo como exceção à regra geral de consentimento. Como principal vantagem, a exceção via interesse legítimo se mostra mais flexível para lidar com a diversidade de modelos de negócio e tecnologias inovadoras difundidos pela internet.

Mesmo que ainda não se tenha no âmbito europeu uma definição estrita de quais são os critérios necessários para a configuração do interesse legítimo, a Comissão Europeia e o Conselho Europeu já avançaram no apontamento de alguns critérios mínimos para a definição de interesse legítimo, aos quais cabe a menção a seguir: (*i*) natureza e a fonte do interesse legítimo; (*ii*) o impacto no titular dos dados; (*iii*) relação entre o titular dos dados e o responsável; e (*iv*) adoção de salvaguardas adicionais de ordem técnica e/ou organizacional.

Ademais, em nossa visão parece existir ainda uma contradição entre a indispensabilidade do dado como exceção a obrigação da outorga do consentimento por parte do usuário (parágrafo 1º do art. 7º) e a possibilidade de revogação do consentimento oferecido sem qualquer ônus ao usuário titular do dado (parágrafo 6º do art. 7º).

Pela forma como os artigos se apresentam no Anteprojeto, não está devidamente claro se a revogação do consentimento sem ônus ao usuário (parágrafo 6º do art. 7º) entra em conflito com a exceção de indispensabilidade do dado prevista parágrafo 1º do art. 7º.

As incertezas e falta de precisão quanto aos critérios de definição do que pode ser considerado como dado indispensável associadas à possibilidade de revogação do consentimento sem ônus ao titular do dado podem juntas criar um cenário em que o usuário possa pleitear a revogação de dados indispensáveis à oferta de determinado serviço ou produto, uma vez que pode ser interpretado que o consentimento foi oferecido nas duas hipóteses, não podendo apenas na primeira ser um impeditivo do tratamento de dados.

Recomendação 2: Acreditamos que seja necessária uma definição sobre quais serão os critérios para a delimitação de dado indispensável como exceção a regra de obtenção do consentimento livre, expresso, específico e informado do usuário. A alternativa europeia de interesse legítimo oferece critérios que podem contribuir ao modelo jurídico brasileiro de proteção de dados pessoais.

O Anteprojeto de proteção de dados pessoais não dispõe de um capítulo específico sobre os papéis do Estado em seu sistema jurídico de proteção de dados pessoais. Esta ausência poderia nos conduzir a um diagnóstico de que o Anteprojeto trata entidades estatais que realizam atividades de tratamento de dados pessoais da mesma forma que trata entidades privadas. Contudo, há diferenças de tratamento relevantes que merecem uma análise mais cuidadosa, em especial ao capítulo IV – Comunicação e Interconexão.

Em seu art. 2º, *caput*, o Anteprojeto estabelece que a lei se aplica a qualquer operação de tratamento de dados realizada por pessoa natural, jurídica de direito público ou privado. Em seu parágrafo 3º há, inclusive, a vedação expressa aos órgãos públicos e entidades públicas de transferência de dados pessoais constantes nas bases que administram ou que venham ter acesso em razão de suas competências, sendo permitida o acesso por terceiros mediante concessão e permissão com finalidade específica.

Interessante notar que a vedação prevista no parágrafo 3º do art. 2º nos remete ao incidente[14] envolvendo o Acordo-Técnico celebrado entre o Tribunal Superior Eleitoral e a empresa Serasa Experian S.A. em agosto de 2013. Na ocasião, o acordo previa o fornecimento de dados pessoais de eleitores que estavam armazenados em bancos de dados do Tribunal para a

[14] O Acordo-Técnico entre a Serasa Experian S.A. e o Tribunal Superior Eleitoral foi assinado sob a lógica de que os dados cadastrais de leitores seriam dados públicos e portanto, poderiam ser objeto de transação entre a empresa e o Tribunal. As informações cadastrais compreenderiam a situação da inscrição eleitoral, nome, CPF e dados relativos à óbito e a quitação eleitoral. Um dado muito relevante para a empresa na época era a verificação de quais eleitores ainda estavam vivos, uma vez que em suas atividades de cobrança há uma dificuldade de se ter este dado com um amplo grau de certeza. Na visão da empresa, os dados sobre óbito são públicos e sua disponibilização traria o benefício social de contribuir para a melhora na prevenção de fraudes no mercado de crédito. Para mais informações sobre o caso consulte: <http://www.tse.jus.br/noticias-tse/2013/Agosto/corregedoria-geral-eleitoral-suspende-acordo-entre-tse-e-serasa>. Veja também o inteiro teor da decisão da Corregedoria-Geral do Tribunal Superior Eleitoral sobre o Acordo-Técnico entre o Tribunal e a Empresa em: <http://www.justicaeleitoral.jus.br/arquivos/tse-serasa-acordo-cooperacao-tecnica>.

Serasa em troca de certificados digitais oferecidos pela empresa. A Corregedoria-Geral Eleitoral suspendeu preliminarmente o convênio por constatar a existência de riscos relacionados a quebra de sigilo de informações.

Este talvez tenha sido o caso que evidenciou com maior clareza a posição de entidades estatais na gestão de dados pessoais de usuários, demonstrando a necessidade de que o Estado seja também objeto de uma regulação de proteção de dados pessoais. Isto porque o acordo reconhecia informações cadastrais como nome, número do cadastro de pessoas físicas (CPF), inscrição eleitoral, dentre outras como informações públicas, disponíveis para transações. Porém, quando o acordo veio a público, a reação de alguns setores da sociedade a respeito da destinação de tais informação não pareceu a mesma compartilhada pelo Tribunal e pela empresa.

O art. 3º, *caput*, do Anteprojeto inclusive estende a aplicação das regras de proteção previstas para a administração pública em seu texto às empresas públicas e sociedades de economia mista não permitindo o surgimento de dúvidas sobre a aplicação das regras de proteção de dados pessoais no âmbito estatal.

Sendo assim, como o Anteprojeto confere um tratamento diferenciado para entidades estatais? E se o faz, quais seriam os problemas desta diferenciação? A esse respeito oferecemos três críticas ao texto do Anteprojeto:

Crítica 1: O texto do Anteprojeto utiliza o termo "órgão competente" em dois sentidos diferentes, como autoridade de proteção de dados pessoais e como órgão com competência para gerir dados pessoais de usuários. Este uso deve ser corrigido para se evitar equívocos na aplicação das normas ali inscritas.

Crítica 2: O art. 4º do Anteprojeto ao excluir a aplicação do regime proteção de dados pessoais em atividades de tratamento de dados pessoais para fim exclusivo de segurança pública, defesa, segurança do Estado ou investigação e repressão de infrações penais parece estar se omitindo de uma dimensão central para a proteção do usuário.

Crítica 3: Há contradições na dispensa do consentimento livre, expresso, específico e informado pelo órgão competente em atividades de comunicação e interconexão realizadas por empresas e órgãos estatais, conforme prevista no inciso III do art. 24.

Ao utilizar a expressão "órgão competente", o Anteprojeto o faz em dois sentidos: como autoridade específica de regulação da proteção de dados pessoais, como pode se ver no art. 10, inciso VII, alínea c e no parágrafo 4º do mesmo artigo; e como órgão com competência específica para lidar com dados pessoais, como se observa no parágrafo único do art. 4º do Anteprojeto.

Em nossa visão, para tornar o texto mais claro e eliminar qualquer confusão em relação à dualidade de sentidos apontada, acreditamos ser importante que o Anteprojeto utilize expressões distintas para cada um destes órgãos.

Recomendação 1: Diferenciar os dois sentidos da expressão "órgão competente" de modo a evitar problemas de interpretação do texto do Anteprojeto. Uma possibilidade é a adoção da expressão autoridade de proteção de dados pessoais, diferenciando-a da expressão órgão competente.

Segundo a redação do art. 4º, *caput*, do Anteprojeto:

> *"Os tratamentos de dados pessoais para fins exclusivos de segurança pública, defesa, segurança do Estado, ou atividades de investigação e repressão de infrações penais, serão regidos por legislação específica,*

observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei."

Pela redação, o tratamento de dados realizado pelo Estado no âmbito de suas atividades de garantia da segurança e defesa e repressão de infrações criminais deve ter um diploma próprio, com previsões específicas, desde que não entre em conflito com os princípios da proteção de dados e os direitos do titular dos dados, ambos previstos Anteprojeto.

Parece-nos que o artigo busca harmonizar as peculiaridades destas atividades com o regime de proteção de dados criado pelo Anteprojeto, justificando um diploma normativo próprio.

Porém, mesmo que a intenção de harmonização esteja clara na redação do artigo, há espaços importantes de proteção de dados pessoais que em nossa visão deveriam ser encarados pelo Anteprojeto, em especial, uma proteção específica contra o uso de softwares de monitoramento e espionagem por autoridades de segurança pública e defesa.

Em recente notícia[15] do Jornal Folha de São Paulo, foi descrita a utilização de softwares de armazenamento de dados pessoais de aparelhos celulares de linhas monitoradas com autorização judicial. O interessante da notícia é que, mesmo o monitoramento das ligações tendo sido autorizado pelo Poder Judiciário, a Polícia Federal se valeu de um software para coletar outras informações dos investigados, ou seja, dados pessoais que, em princípio, não estavam no escopo da autorização.

Não nos parecem existir justificativas específicas no âmbito da segurança pública e repressão de infrações criminais que justificassem tal iniciativa. Entendemos que seria o caso da lei de proteção de dados pessoais tratar de tal situação. Nos termos do texto do artigo 4º, parece haver uma exclusão total para este tipo de situação, deixando a cargo de uma norma que ainda não foi sequer posta no debate público sobre proteção para estes dados.

[15] Disponível em: <http://www1.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml>

Na verdade, em nossa visão, no que tange ao acesso a dados pessoais, o sistema jurídico brasileiro já dispõe de regras específicas de proteção aos registros, dados pessoais e comunicações privadas previstas na Lei n.º 12.965 de 2014 – Marco Civil da Internet – prevendo, por exemplo, no §2º do art. 10. Essa disposição estabelece que o conteúdo de comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, com as ressalvas do § 3º do mesmo artigo referentes a requisição de dados cadastrais que informem qualificação pessoal, filiação e endereço por autoridades administrativas competentes.

Todavia, acreditamos que o art. 4º não deva excluir totalmente a regulação da proteção de dados para um diploma específico. Parece-nos que o Anteprojeto poderia fazer referência às normas do Marco Civil da Internet, reforçando a necessidade de que qualquer atividade de tratamento neste contexto também dependerá de ordem judicial.

O cidadão precisa ter um regime de proteção de seus dados pessoais que se aplique inclusive para atividades de tratamento relacionadas à segurança pública e à repressão de infrações criminais. Não são poucos os relatos que nos chegam sobre uso de técnicas de monitoramento e de estratégias de coleta de dados realizados por autoridades policiais em relação a extração[16] de dados pessoais no âmbito de investigações criminais ou no controle de manifestações públicas. Por isso, acreditamos que seja necessário um debate mais profundo sobre quais têm sido essas técnicas de monitoramento e como a regulação de proteção de dados pessoais pode incorporá-las em seu regime, não prejudicando a boa condução das ações de investigação no âmbito da segurança e defesa.

[16] Em debates e encontros com entidades da sociedade civil e acadêmicos, pudemos ter contato com relatos que narram atos de monitoramento de dados pessoais de usuários realizados por autoridades policiais. Obviamente, como relatos estas informações são parciais e merecem ser apuradas por instâncias competentes, não sendo este o espaço adequado para tanto. Contudo, estas informações são mencionadas aqui apenas como uma ilustração dos riscos inerentes da não aplicação das regras previstas no Anteprojeto, tendo em vista a previsão do *caput* art. 4º.

Recomendação 2: Acreditamos que seja necessário uma nova reflexão sobre a redação do art. 4º do Anteprojeto à luz de técnicas de monitoramento e tratamento de dados pessoais no âmbito da segurança pública e defesa.

O inciso III do art. 24 estabelece que, na hipótese de comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público com pessoa de direito privado, dispensa-se o consentimento quando houver prévia autorização de órgão competente, que avaliará o atendimento do interesse público para a autorização desta dispensa.

Em nossa visão, o artigo apresenta algumas contradições que merecem uma análise mais cuidadosa. Para isso, nos valemos do incidente narrado no início desta seção, a cessão de dados do cadastro eleitoral disponíveis no banco do Tribunal Superior Eleitoral para a empresa Serasa Experian S.A.

Pela previsão do art. 24, inciso III, qualquer[17] órgão competente, e não apenas o Órgão Competente (autoridade de proteção de dados pessoais), responsável pela regulação da proteção de dados pessoais no âmbito federal, poderá dispensar a obtenção do consentimento para operações de comunicação e interconexão definidas nos incisos X e XI do art. 5º do Anteprojeto.

Imaginemos a mesma situação envolvendo o TSE e a Serasa, só que agora sob a luz da dispensa prevista no inciso III do art. 24.

A solicitação da Serasa de transferência de dados pessoais do banco de dados do TSE para o seu banco de dados, sob a justificativa de que tal transferência cumpre o interesse público de redução do número de fraudes em atividades de comerciais, poderia ser objeto de dispensa pelo próprio

[17] Para sustentar nossa leitura para o uso da expressão "qualquer" fazemos referência a redação do inciso III que utiliza a partícula de e não do na passagem "prévia autorização de órgão competente". Nesse sentido, nossa leitura do dispositivo é a de que qualquer órgão que tenha competência de gerir determinado dado pessoal, como no caso apresentado o Tribunal Superior Eleitoral, pode dispensar a obtenção de consentimento quando julgar que há um imperativo de interesse público que justifique tal dispensa.

TSE, entidade competente para gerir tais dados. Na visão do Tribunal, tal iniciativa poderia ser adequada, na medida em que auxiliaria no combate a fraudes e necessária pelo volume de fraudes presentes nas atividades comerciais no Brasil.

O TSE poderia justificar o recebimento de serviços de certificação digital pela empresa como uma contrapartida que atende o interesse público de aprimoramento dos seus serviços frente ao cidadão. Na visão do Tribunal, a certificação digital seria necessária tendo em vista todos os esforços de digitalização realizados pelo Poder Judiciário, bem como seria adequada na medida em que não comprometeria recursos financeiros públicos para a sua implementação.

Como resultado, o ente público interessado na dispensa do consentimento livre, específico, expresso e informado poderá ele mesmo promover a dispensa, desde que ofereça uma justificativa de interesse público, fato que consideramos muito problemático tendo em vista a indeterminação do que consideramos como interesse público.

Nesse sentido, uma transferência controversa, amplamente discutida e que teve a sua aplicação suspensa na época, pela previsão do inciso III do art. 24, poderia ter fundamento jurídico para ser realizada com certa facilidade.

Segundo o parágrafo único do art. 24, a autorização de dispensa prevista no inciso III do mesmo artigo poderá ser condicionada à comunicação da interconexão aos titulares (inciso I) e ao oferecimento da opção de cancelamento de seus dados ao seu titular (inciso II).

Trazendo para a ilustração apresentada, o eleitor que tivesse os seus dados de cadastro eleitoral cedidos pelo TSE receberia uma comunicação de que seus dados estariam sendo transferidos para os bancos de dados da Serasa. O eleitor insatisfeito com a transferência de seus dados cadastrais pelo TSE poderia solicitar o cancelamento de seus dados (inciso XVI do art. 5º), ou seja, a eliminação de seus dados do banco de dados do TSE. Contudo,

pressupõe-se que estes dados são de extrema relevância para os fins da Justiça Eleitoral, o que inviabiliza o seu cancelamento.

Não está claro no texto legal se o cancelamento se estende aos dois bancos de dados, o de origem e o de destino, ou se apenas ao banco de dados de destino. Pela redação do artigo, o cancelamento poderia se dar nos dois, trazendo um problema ainda mais grave do que a dispensa do consentimento.

Portanto, a permissão que o artigo parece oferecer para qualquer órgão competente autorizar a dispensa do consentimento livre, expresso, específico e informado em atividades de comunicação e interconexão nos parece ser um equívoco, em especial pela possibilidade de nestas atividades permitir ao titular dos dados cancelar os seus dados no banco de origem.

Recomendação 3: A dispensa de consentimento prevista no art. 24, inciso III, deve ser restrita ao Órgão Competente (autoridade de proteção de dados pessoais) e não a qualquer órgão que tenha competência na gestão de dados pessoais. Este avaliará as solicitações de dispensa encaminhadas por outros órgão públicos.

Por fim, cabe mencionar a importância de se realizar um debate público sobre a formação do Órgão Competente referido no Anteprojeto. De fato, o Anteprojeto pouco versa sobre suas definições para além de algumas prerrogativas em lei. No entanto, nossa posição é de que é preciso debater pública e democraticamente a respeito da estruturação do Órgão Competente principalmente em torno de suas funções, organização institucional, composição e procedimentos de tomada de decisão, entre outros.

A economia atual, globalmente integrada, depende cada vez mais de um fluxo contínuo de informações. Serviços associados às Tecnologias da Informação e Comunicação passaram a operar a partir de uma rede internacional, impondo desafios relevantes para a regulação jurídica dos países. Um bom exemplo disso são as tecnologias de armazenamento de dados na nuvem (*cloud computing*).

Por meio de tais serviços de armazenamento em nuvem, diversos dados podem estar acessíveis de diversos locais do globo ao mesmo tempo, sem que o usuário comum tenha conhecimento da localidade exata onde estes encontram-se hospedados.

Além disso, o atual modelo de rede e de armazenamento em nuvem levou à difusão de *data centers*[18] pelo mundo e à amplificação da troca global de informações. Não é por acaso, portanto, que transferências internacionais de dados têm levantado preocupações legítimas sobre os locais para os quais são transferidos os dados pessoais de usuários, bem como quais são as normas jurídicas aplicadas no país onde os dados são transferidos.

Não nos parecem haver controvérsias em relação ao postulado de que o usuário tem de ter formas de proteção de seu dado pessoal, mesmo que este sofra um tratamento fora do Brasil. Há, sem dúvida, problemas relacionados a como criar regras jurídicas no âmbito nacional que possam garantir algum nível de proteção para relações que se operacionalizam no contexto internacional, entre jurisdições diferentes.

18 Quanto a esse aspecto, constatamos que há registros da existência de *data centers* em pelo menos 104 (cento e quatro) países do globo terrestre. Tal apuração levou em consideração as informações registradas na página <http://www.datacentermap.com/datacenters.html>, acessada pela última vez em 02/07/2015, na qual os registros sobre a existência de data centers no mundo são mantidos e inseridos de forma colaborativa, em regra pelos próprios prestadores dos serviços.

A esse respeito, a referência preponderante nos debates tem sido a transferência de dados pessoais de usuários, obtidos por provedores de serviços de aplicação ou conexão no contexto de sua atuação, para terceiros (*third parties*) interessados no uso, transmissão ou hospedagem destes dados. São diversas razões que justificam a transferência de dados a terceiros no contexto dos serviços online, sendo as mais comuns o *outsourcing*[19] e uso para fins de publicidade comportamental.

É de se esperar que um anteprojeto de lei de proteção de dados pessoais equilibre um modelo que ofereça uma estratégia de proteção ao usuário quando da transferência internacional de seus dados para terceiros, bem como um modelo que seja capaz de sustentar a existência legítima da transferência internacional de dados, tendo em vista as características de interdependência global que observamos nos dias atuais.

Desde já, nossa análise da proposta do Anteprojeto de proteção de dados assume que não há apenas um modelo para a regulação da transferência internacional de dados. De forma ampla, para os fins da presente contribuição, destacamos pelo menos duas orientações regulatórias [20] presentes no debate sobre transferência internacional de dados: (i) a

[19] Para além de uma definição fechada de outsourcing, nos valemos da ideia de terceirização de serviços para os fins desta contribuição. A mais comum delas é a contratação de serviços de hospedagem de dados em data centers em outros países por provedores de serviços na Internet. Evidentemente, empresas de grande porte como Google, Facebook, Amazon, dentre outras, dispões de seus próprios data centers em diferentes países, respeitando suas estratégias próprias de transferências de dados. Contudo, há um número significativo de empresa que hospedam os seus dados por meio da contratação de terceiros, em países que não possuem legislações próprias de proteção de dados pessoais.

[20] Fazemos aqui uso da expressão orientação regulatória, pois nossa intenção é apontar para estruturas normativas que adotam estratégias de intervenção sobre a transferência internacional de dados distintas. O uso da palavra orientação foi a forma encontrada por nós em não descrever sistemas jurídicos com algum grau de similaridade como sistemas iguais. Nosso intuito foi o de comparar duas posturas distintas, uma mais rígida, de maior proteção, a postura europeia, focada no país de destino do dado, e outra mais flexível, focada na criação de responsabilidade para o provedor de serviços que transferiu o dado para o terceiro. De forma alguma o esforço desta seção deve ser encarado como uma tentativa de exaurir a explicação sobre transferência internacional de dados, debate complexo e repleto de peculiaridade. Buscamos criar ferramentas para avaliação da escolha presente no Anteprojeto e quais os problemas que visualizamos a partir dela.

europeia, embasada nas normas da União Europeia sobre proteção de dados, e (ii) a canadense, respaldada em sua lei de proteção de dados e em suas *guidelines*.

O capítulo V – transferência internacional de dados – do Anteprojeto de Proteção de Dados Pessoais prescreve como regra geral do modelo brasileiro de regulação da transferência internacional de dados a equivalência do nível de proteção de dados entre os países de origem e destino da transferência (art. 28, *caput*).

O parágrafo único do art. 28 do Anteprojeto estabelece quais são os critérios adotados para a verificação de equivalência entre os níveis de proteção de dados dos países, sendo eles: (i) normas gerais e setoriais da legislação em vigor do país de destino; (ii) natureza dos dados; (iii) observância dos princípios gerais de proteção de dados pessoais previstos no Anteprojeto; (iv) adoção de medidas de segurança previstas em regulamento; e (v) outras circunstância relativas à transferência.

O art. 29 do Anteprojeto cuida da hipótese de transferências para países que não proporcionem o mesmo nível de proteção que o Anteprojeto oferece. Para estes casos, o Anteprojeto prevê a necessidade de um consentimento especial, fornecido mediante manifestação própria e distinta de outras oferecidas (inciso I do art. 29) e a disponibilização de informação prévia e específica sobre o caráter internacional da operação, com destaque para os riscos envolvidos (inciso II do art. 29).

Nesse sentido, o modelo brasileiro não cria uma proibição a transferência internacional de dados. Contudo, para os países que não adotem um regime equivalente ao brasileiro, o Anteprojeto exige a obtenção de um consentimento especial, ou seja, em tese, aposta no fornecimento de mais informações ao usuário sobre os riscos da transferência internacional.

Em uma análise do capítulo V do Anteprojeto, fica clara a inspiração no modelo europeu prescrito na Diretiva 95/46/EC editada pelo Parlamento Europeu em 24 de outubro de 1995.

Como regra geral, o parágrafo 56[21] da diretiva europeia estabelece que se a transferência de dados for necessária no âmbito do comércio internacional, ela poderá ser realizada desde que garantido um nível adequado de proteção no país de destino do dado pessoal. Quando não oferecido este nível adequado de proteção, a Diretiva, por meio de seu parágrafo 57[22], proíbe a transferência. Disposições muito semelhantes ao disposto no art. 28 do Anteprojeto.

O parágrafo 58[23], por sua vez, prevê que exceções poderão ser feitas à proibição prevista no parágrafo 57, prescrevendo a necessidade de obtenção do consentimento do titular do dado, bem como limitando o número de situações para as quais as exceções poderão ser feitas, modelo novamente semelhante ao previsto nos incisos do art. 28 do Anteprojeto.

Da mesma forma, nota-se uma semelhança entre os parágrafos 59[24] e 60[25] da diretiva europeia com o artigo 30 do Anteprojeto de Proteção de Dados

---

[21] No original: *"(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;"* Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

[22] No original: *"(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;"* Fonte: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

[23] No original: *"(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;"* Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

[24] No original: "*(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards;*

Pessoais, pois, em ambos os casos, os responsáveis pelo tratamento podem compensar a falta de equivalência de outros países por disposições contratuais que assegurem uma equivalência no nível de proteção, sendo estas objeto de análise do Órgão Competente de Proteção de Dados Pessoais no Brasil.

Nesse sentido, podemos dizer que o modelo de transferência de dados previsto no Anteprojeto, sob inspiração europeia, se estrutura a partir de uma regra geral de equivalência de nível de proteção de dados entre país de origem e destino da transferência. Assim, cria exceções para a hipótese de transferência de dados para países que não apresentem o mesmo nível de proteção, as quais serão avaliadas pelo Órgão Competente mencionado no Anteprojeto.

No entanto, verifica-se que a Diretiva Europeia foi editada em um período em que a relevância das transferências de dados pela internet não assumia, nem de longe, a magnitude que possui hoje. Portanto, retomando o quanto exposto na introdução deste tópico, em nosso entendimento, a legislação brasileira vindoura não deve tão-somente repetir as disposições europeias, editadas há duas décadas, sem que haja uma especial preocupação com o contexto atual do uso da internet como principal forma de transmissão de dados no mundo.

Além dos problemas apontados, mesmo que o Anteprojeto apresente a possibilidade de que empresas privadas possam incorporar os princípios de proteção em suas cadeias contratuais pelo mundo, garantindo o nível de equivalência esperado na transferência internacional de dados, a aposta em um consentimento especial baseado na ideia de oferta de informações detalhadas ao usuário sobre os riscos da transferência internacional de dados não nos parece tão acertada quanto defendida, pois ainda reforça o

---

whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;" Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

[25] No original: "(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;" Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

que chamamos de "paradoxo da transparência", exposto na seção sobre o modelo de consentimento.

Como expusemos em tópico próprio, há dados empíricos que indicam que os usuários não leem os textos que deveriam ser efetivamente informativos. Via de regra, não estão aptos ou dispostos a ler extensas páginas de texto legal para então tomar uma decisão informada. É de se questionar em que medida vale a aposta na sistemática de consentimento especial, que, na prática, pressupõe ainda mais informação a ser considerada pelo titular dos dados.

Nossos apontamentos sobre o modelo de consentimento, definitivamente, não devem ser interpretados como qualquer forma de mitigação à proteção do titular. Em verdade, a reflexão é necessária para se apurar até que ponto um consentimento informado ou especial, obtido por meio de textos legais que via de regra não são lidos, trazem a efetiva proteção à privacidade do usuário que a lei vindoura pretende garantir.

Além disso, ao nosso ver, o texto do Anteprojeto confere excessiva autonomia ao Órgão Competente na avaliação dos critérios de equivalência de níveis de proteção. Avaliação de normas gerais e setoriais, natureza dos dados, modelos de segurança, não são capazes de servir como guia para tomada de decisão, ao contrário, são janelas para o exercício da discricionariedade do agente público.

Nesse sentido, destacamos que o Órgão Competente assume papel central na transferência internacional dos dados, uma vez que, fundamentalmente, será responsável por: (*i*) autorizar a transferência; e (*ii*) avaliar o nível de proteção de outros países.

Essas duas responsabilidades atribuídas pelo Anteprojeto ao Órgão Competente enseja algumas preocupações relacionadas à burocratização e à viabilidade de se consolidar a legítima transferência internacional de dados, principalmente se considerarmos o dinamismo imposto pela lógica global de serviços em rede.

A crítica ao modelo de atribuição de excessivo poder ao Órgão Competente, ainda que matéria de regulação posterior, não significa defender, em absoluto, que deva haver qualquer prejuízo à proteção dos dados pessoais no contexto da transferência internacional. O que se pretende aqui é provocar um debate que enseje discussões sobre modelos alternativos de regulamentar a questão da transferência internacional de dados levando-se em consideração toda a lógica da descentralização da prestação dos serviços globais, principalmente os de alta tecnologia.

As consequências práticas da aplicação do texto legal, tal como estabelecido no Anteprojeto, chegam a ser de difícil mensuração, pois, em nosso entender, não resta evidente qual a abrangência da aplicação desse artigo, muito menos quais os impactos que as regras previstas podem gerar na sistemática do funcionamento das comunicações globais atualmente existentes.

O texto não parece pretender que, no caso em concreto, se assuma, implicitamente, a possibilidade de haver um desvio da aplicação das regras sobre transferência internacional de dados para determinadas situações, por força da lógica de funcionamento de um modelo de negócio. Assim, entendemos adequado que haja uma reflexão sobre as regras da transferência internacional de dados de maneira ampla, procurando vincular o texto legal aos seus impactos na arquitetura da rede.

Desta forma, a síntese de nossas duas críticas são:

Crítica 1: Os critérios adotados para a verificação de equivalência entre os níveis de proteção de dados pessoais adotados pelos países em operações de transferência internacional de dados previstos nos incisos do art. 28 são de difícil aplicação, pois são demasiadamente genéricos.

Crítica 2: Conforme já explorado na seção do modelo de consentimento, a aposta do art. 29, inciso II, em oferecer informações detalhadas sobre os riscos de operações de transferência internacional de dados padece dos problemas presentes no "paradoxo da transparência".

Na nossa visão, caso o Ministério da Justiça decida manter no Anteprojeto a decisão sobre a avaliação do nível de proteção no Órgão Competente previsto no diploma, acreditamos que seja necessária a edição de uma regulamentação sobre quais serão os critérios específicos adotados para a avaliação sobre o nível de equivalência de proteção esperado.

O modelo de transferência de dados como está prescrito no Anteprojeto ainda suscita muitas questões relevantes para a sua operacionalização. A título de exemplo podemos citar algumas delas:

(i) Qual o limite da sua aplicação e a quem se destina?

(ii) Será necessária a verificação de existência no país de destino das informações de todos os princípios presentes na lei brasileira de proteção de dados pessoais para que se tenha o nível de proteção equiparável?

(iii) A proteção de dados do país de destino terá, necessariamente, de se basear na obtenção de consentimento livre, expresso, específico e informado para atividades de tratamento de dados?

(iv) A falta de um destes elementos já torna os sistemas incompatíveis?

(v) Sistemas jurídicos que não possuam autoridade reguladora de proteção de dados não serão considerados como equivalentes?

Tendo em vista as dificuldades de operacionalização apontadas, nos valemos de algumas disposições do modelo canadense de proteção de dados pessoais presente no *Personal Information Protection and Eletronic*

Documents Act (PIPEDA). Em contraste com o modelo europeu baseado em níveis de adequação de sistemas jurídicos de proteção de dados pessoais, o modelo de transferência canadense optou por uma abordagem organizacional (*organization-to-organization*) para regular a transferência internacional de dados.

Em nosso entendimento, o PIPEDA não proíbe nenhuma entidade que participa de operações de transferência internacional de dados de transferir dados para outra entidade em uma jurisdição que não conte com um nível adequado de proteção de dados pessoais. Todavia, as entidades que participam de operações de transferência podem ser responsabilizadas civilmente nestas operações.

A autoridade de proteção de dados pessoais canadense (*Office of the Privacy Commissioner of Canada* - OPC) pode receber reclamações de usuários e abrir investigações sobre práticas inadequadas de gestão de dados pessoais que contrariem as regras do país sobre proteção de dados, como por exemplo, o desvio de finalidade no uso dos dados por parte de empresas.

O princípio estruturante desse sistema de responsabilidade baseado nas organizações participantes da transferência internacional de dados é o *principle 4.1.3 of Schedule 1* da PIPEDA[26], o qual estabelece que:

> *Uma organização é responsável pelos dados que estão em sua posse ou sua custódia, incluindo os dados que tem sido transferidos para terceiros para tratamento. A organização deverá se valer de disposições contratuais ou outros meios para oferecer um nível de proteção*

[26] No original: "*An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.*" Tradução nossa. Disponível em: <aws-lois.justice.gc.ca/eng/acts/P-8.6/index.html>.

> *equivalente enquanto o dado está sendo tratado pelo terceiro.* (tradução nossa)

Nesse sentido, nossa sugestão de aprimoramento do Anteprojeto é a de adequação do modelo de inspiração europeia, baseado na ideia de avaliação de níveis de equivalência por autoridades regulatórias, a um modelo de inspiração canadense, baseado na avalição de condutas que contrariem as regras e os princípios da proteção de dados nas atividades de transferência internacional de dados.

Ressaltamos que, em nosso entender, muito do modelo canadense já está incorporado no art. 22 e, principalmente, artigo 30, §1º do Anteprojeto. Mas, diferente do que está disposto no APL, em que o Órgão Competente realizará a avaliação sobre a equivalência de níveis de proteção de dados pessoais entre os países de origem e destino do dado pessoal e outorgará, ou não, a autorização para transferência, se necessário, o modelo canadense retira esta avaliação de sua autoridade de proteção. Nesse ponto, tal modelo prevê que referida autoridade poderá abrir investigações quando necessário e solicitar informações, inclusive por meio de auditorias, quando identificar potenciais violações ao regime de proteção, mas sem a necessidade de autorização prévia.

Por estas razões, o reforço de um modelo de responsabilidade civil para a transferência internacional de dados, em substituição ao modelo de autorizações e consentimento especial da redação atual, nos parece mais acertado para o Anteprojeto.

Recomendação 1: Substituição do modelo de transferência internacional de dados baseado no consentimento especial e nas autorizações do Órgão Competente, pautadas na equivalência entre legislações, para um modelo que se baseie, primordialmente, na atribuição de responsabilidade a empresas pela custódia de dados pessoais, bem como pela adoção de padrões de proteção de dados previstos no Anteprojeto em suas cadeias contratuais

Referências

DE LIMA, Desiree; LEGGE, Adam. (2014) The European Union's approach to online behavioural advertising: Protecting individuals or restricting business? Computer Law & Security Review, v. 30, p. 67-74.

JENSEN, Carlos; POTTS, Colin; JENSEN, Christian. (2005) Privacy practices of Internet users: Self-reports versus observed behavior. Int J. Human-Computer Studies, v. 63, p. 203-227.

MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. (2008) The Cost of Reading Privacy Policies. A Journal of Law and Policy for the Information Society, v. 4, n. 3, p. 540- 565.

NISSENBAUM, Helen. (2011) A Contextual Approach to Privacy Online. Daedalus, the Journal of the American Academy of Arts & Sciences, v. 140, n. 4, p. 32-48.

PARK, Yong Jin; CAMPBELL, Scott W.; KWAK, Nojin. (2012) Affect, cognition and reward: predictors of privacy protection online. Computers in Human Behavior, v. 28, p. 1019-1027.

ROBINSON, David; YU, Harlan; ZELLER, William P.; FELTEN, Edward W. (2009) Government Data and the Invisible Hand. Yale Journal of Law and Technology, v. 11, n. 1, art. 4.

SMIT, Edith G.; NOORT, Guda Van; VOORVELD, Hilde A.M. (2014) Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behavior in Europe. Computers in Human Behavior, v. 32, p. 15-22.

SOLOVE, Daniel J. (2013) Privacy Self-Management and the Consent Dilemma. Harvard Law Review, v. 126, p. 1880-1903.

TADDEI, Stefano; CONTENA; Bastianina. (2013) Privacy, trust and control: Which relationships with online self-disclosure? Computers in Human Behavior, v. 29, p. 821-826.