GPOPAI

Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação

USP

Projeto de Pesquisa Vigilância e Privacidade

Contribuições à Consulta Pública do Anteprojeto de Lei/APL de Proteção de Dados Pessoais

São Paulo
02 de julho de 2015

Apresentação

Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação da Universidade de São Paulo/GPoPAI USP

Projeto de Pesquisa Privacidade e Vigilância

O GPoPAI é um grupo de pesquisa sediado na Universidade de São Paulo (Campus Leste) que se dedica, em linhas gerais, à investigação dos impactos das novas tecnologias em termos de políticas públicas. Dentre os seus projetos pesquisa, encontra-se, em andamento, o projeto intitulado "Estruturação de um Campo de Estudos sobre Privacidade e Vigilância no Brasil". Um dos eixos deste projeto de pesquisa destina-se ao acompanhamento e à execução de ações participativas no campo acadêmico e da sociedade civil para fins de aprimoramento legislativo da proteção de dados pessoais no Brasil.

Nesse sentido, pretende-se qualificar o debate da consulta pública do Anteprojeto de Lei de Proteção de Dados Pessoais/APL, lançada pelo Ministério da Justiça em sua plataforma online, com justificativas teóricas e sugestões para a alteração de determinados dispositivos desta projetada normatização.

Equipe e Financiamento

O projeto de pesquisa Privacidade e Vigilância é financiado pela Fundação Ford.

Para a elaboração deste documento relativo às contribuições para a consulta pública do APL, tem-se uma equipe de pesquisa composta da seguinte maneira:

Coordenadores

Jorge A. S. Machado

Pablo Ortellado

Márcio Moretto Ribeiro

Pesquisador Autor do Texto

Bruno Ricardo Bioni

Equipe de Pesquisa

Amanda Monteiro

Beatriz Macruz

Marina Salles

L. Almeida

Caio Canic Silva

Leonardo Piccioni

Carybé Silva

Colaboradores

Margareth Kang

Renato Leite Monteiro

Metodologia

Por se tratar de uma consulta pública em que as contribuições atingem um grande volume, optou-se por descrever, sucintamente, os fundamentos teóricos das intervenções, seguida da sugestão de alteração do texto da norma, mediante um quadro comparativo entre o texto proposto e o texto sugerido. Acredita-se que esse modelo otimizará o trabalho do Ministério da Justiça na consolidação das contribuições geradas na plataforma da consulta pública para fins de aprimoramento do texto normativo do APL.

Ressalta-se, ainda, a preocupação de que a projetada legislação deve ser neutra em termos tecnológicos. Dito de outra forma, o comando normativo não deve se resumir a uma determinada tecnologia, sob pena do avanço tecnológico torná-lo obsoleto. Deste modo, a técnica utilizada para as proposições de alteração do texto do APL, valeu-se da seguinte estratégia:

i. a primeira parte é sempre genérica, buscando-se estabelecer um comando normativo que atinja um grau ótimo de flexibilidade da norma no tempo;
ii. a parte final do texto proposto, mesmo que remeta por vezes a um padrão técnico de uma determinada tecnologia, é feita de maneira exemplificativa, o que não engessa, portanto, o comando normativo. Pensou-se em tal estratégia regulatória, porque o Brasil não tem uma cultura jurídica de proteção de dados pessoais, o que é confirmado pelo nosso atraso regulatório em emitir uma lei geral sobre o tema, tal como se propõe o APL sob discussão. Ademais, mesmo os países, que já preencheram tal vácuo normativo, encontram dificuldades de empregar concretude aos comandos normativos. Por tal razão, acredita-se que essa técnica legislativa, por meio de tais proposições não taxativas, é capaz de nortear o aplicador/intérprete da legislação.

Ressalva-se que a presente contribuição não é um documento acadêmico, ainda que se faça uso de referenciais e justificativas teóricas para fundamentá-la. Priorizou-se, nesse sentido, uma linha de raciocínio baseada em exemplos para facilitar a compreensão desse documento. Do mesmo modo, procurou-se, sempre que possível, estabelecer um diálogo com as contribuições geradas pela consulta pública, o que não se limitou à plataforma *online* do Ministério da Justiça em razão do trabalho de entidades que reportaram e produziram material sobre o assunto em outros veículos de comunicação.

Consigna-se, por fim, que o presente documento consolida todas as contribuições "postadas", anteriormente, na plataforma do debate público com o acréscimo de novos temas. Nesse processo, teve-se uma perspectiva global da discussão, o que gerou modificações pontuais naquelas prévias contribuições submetidas ao debate público, a fim de empregar coesão ao texto. Verificar-se-á, por exemplo, que os itens "a.2", "b.3" e "e.3" estão interligados, de sorte que estratégia regulatória, que se pretendeu sugerir, somente faz sentido se tais pontos forem lidos/interpretados de forma conjunta.

Sumário

As contribuições foram consolidadas da seguinte forma:

A. Escopo da Lei

Identificou-se a necessidade de se ampliar o escopo de aplicação da lei sob duas vertentes:

i. inserção dos dados sobre as condições socioeconômicas e dados biométricos dos indivíduos na categoria de dados sensíveis. Propõe-se, assim, que o escopo de dados sensíveis seja alargado, empregando-se um regramento mais rígido para as novas espécies sugeridas;
ii. inclusão dos dados isolados ou agregados que sujeitem um indivíduo a um processo de decisão automatizada e dos dados anônimos na definição de dados pessoais. Sugere-se, pois, que o APL preveja, expressamente, que tais hipóteses estejam dentro do seu escopo de aplicação.

A.1. Ampliação do conceito de dados sensíveis (condições socioeconômicas e dados biométricos)

Condição socioeconômica

Historicamente, a construção da categoria de dados sensíveis justifica-se pelo potencial de tal informação ocasionar práticas discriminatórias ao seu titular. Sendo assim, entende-se que a legislação brasileira deveria ampliar o rol exemplificativo de tais informações sensíveis, incluindo aquelas relativas às condições socioeconômicas. Com efeito, os dados sobre a classe social em que está inserido um determinado indivíduo e as suas condições econômicas são suscetíveis de gerar práticas discriminatórias.

Dados biométricos

Dados biométricos são algo de difícil conceituação. Mas, em apertada síntese, decompondo a palavra em questão, poder-se-ia afirmar que são dados mensuradores das características corporais de um determinado indivíduo. Logo, tais dados representam uma particularidade única do indivíduo, já que eles não podem ser alterados ou modificados por estarem “presos” à unicidade do corpo humano. Por isso, outros dados pessoais, como registro de identidade e o número no cadastro nacional de pessoas físicas, podem até serem considerados como identificadores únicos, mas não com o grau de precisão e particularidade dos dados biométricos. Isto porque, os dados biométricos são inalteráveis em decorrência da singularidade corporal, diferentemente do que ocorre quando um dado é atribuído a um indivíduo pelo controle estatal. Nesse sentido, dados biométricos identificam um sujeito em nível global, diferentemente do registro de identidade que tem um alcance nacional. Por essa imutabilidade, singularidade e alcance é que os dados biométricos deveriam ser considerados como dados sensíveis, por serem identificadores únicos com o mais alto grau de precisão que nenhum outro dado detém a mesma capacidade.

Por tal razão, os dados biométricos podem ser tão ou mais lesivos que outros dados pessoais sensíveis. Do seu acesso podem decorrer as mais diversas atividades fraudulentas, potencializando-se, ainda mais, os chamados roubos de identidade (*identity thefts*). Mais remotamente, a clonagem jogou luz sob tais desafios, e, mais recentemente, novas tecnologias – como a impressão 3D – recolocam os holofotes

sobre essa questão da reprodução de identidades. Já imaginou alguém, reproduzindo o dedo e a impressão digital de um indivíduo?

Nesse contexto preocupante, insere-se, ainda, a constante vulgarização da utilização dos dados biométricos em que os mais diversos tipos de atividades cotidianas, como a simples entrada em um prédio, têm demandado o tratamento dos dados biométricos do cidadão. Torna-se, assim, exponencial os riscos para a privacidade do titular dos dados pessoais.

Por isso, sugere-se que os dados biométricos sejam considerados, invariavelmente, como dados sensíveis, a fim de serem adotadas medidas adicionais de segurança que é um dever próprio do regime jurídico dos dados sensíveis, e, complementarmente, reforçando-se o princípio da necessidade, a fim de se combater essa vulgarização do tratamento dos dados biométricos.

No entanto, tendo em vista a amplitude do conceito de dados biométricos, considera-se que o enquadramento de tais dados, como sendo sensíveis, deve ser definido *a posteriori* pelo órgão competente. A alteração do texto do APL justifica-se para:

i. que haja coerência no texto normativo, prevendo-se na definição de dados sensíveis a espécie dos dados biométricos. No texto proposto, ainda que os dados biométricos possam ser considerados sensíveis pelo órgão competente (artigo 13, inciso II, §2°), eles não estão listados na definição de dados sensíveis (artigo 5°, inciso III);
ii. seja reforçado o princípio da necessidade para o tratamento dos dados pessoais sensíveis (dentre os quais biométricos), a fim de se combater a sua emergente vulgarização.

Texto proposto	Texto sugerido
Art. 5, III	**Art. 5, III**
dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos;	dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, às condições socioeconômicas, bem como dados genéticos e dados biométricos, observando-se quanto a esse último o disposto no artigo 13, §2°;
Art. 13, III	**Art. 13, III**
§ 1° A realização de determinadas modalidades de tratamento de dados pessoais sensíveis poderá ser condicionada à autorização prévia de órgão competente, nos termos do	§ 1° A realização de determinadas modalidades de tratamento de dados pessoais sensíveis poderá ser condicionada à autorização prévia de órgão competente, nos termos do regulamento, levando-se em

regulamento. § 2º O tratamento de dados pessoais biométricos será disciplinado por órgão competente, que disporá sobre hipóteses em que dados biométricos serão considerados dados pessoais sensíveis.	consideração, dentre outros princípios, o quanto disposto no artigo 6°, inciso III. § 2º O tratamento de dados pessoais biométricos será disciplinado por órgão competente, que disporá sobre hipóteses em que dados biométricos serão considerados dados pessoais sensíveis.

A.2. Ampliação do conceito de dados pessoais (decisões automatizadas e dados anônimos)

Sujeição a decisões automatizadas

Uma das maiores dificuldades de uma legislação e/ou regulamentação é acompanhar o passo do desenvolvimento tecnológico. Uma opção de técnica legislativa é introduzir conceitos abertos e neutros que possam ser futuramente complementados e interpretados de forma a se adaptar as tecnologias inovadoras.

Na seara da proteção de dados pessoais, outra dificuldade é delimitar o que poderia ser considerado um dado relacionado a uma pessoa identificável, quando por muitas vezes, devido justamente ao atual estado das tecnologias de tratamento de dados, é desnecessário identificar uma pessoa natural para sujeitá-la a uma decisão automatizada que possa influenciar o seu comportamento e, eventualmente, mitigar a sua privacidade. Um bom exemplo seria o endereço IP. Este, por si, não identifica uma pessoa natural, mas sim um terminal de computador. Todavia, como já observado pelo *Article 29 Working Party* para fins de proteção, ele deve ser considerado um dado pessoal, pois ao ser agregado com outros dados pode tornar o indivíduo identificável[1]. Ao funcionar como meio identificador para o fluxo de pacotes de dados, o IP individualiza um terminal de computador a tal ponto que a pessoa natural (usuária) será receptora de conteúdo e informações oriundas de um tratamento de dados e, em última análise, de uma decisão automatizada. Mesmo não sendo a pessoa diretamente identificável, esta é sujeita de um tratamento de dados parcial ou totalmente automatizado e, portanto, as informações que a individualizam devem ser protegidas.

Expandir o conceito de dados pessoais para incluir parâmetros tecnologicamente neutros e abertos e, também, para proteger a pessoa natural sujeita a um tratamento automatizado, está no espírito da APL que procurar garantir a manutenção de direitos fundamentais e liberdades individuais. Daí porque, não se deveria limitar o conceito de dados pessoais ao de identificadores eletrônicos por ser uma categoria que pode, eventualmente, tornar-se obsoleta no curso do tempo. Com efeito, processos de decisões automatizadas poderão ser, futuramente, operacionalizados por outros meios de identificação que não, necessariamente, o eletrônico. Por isso, a importância do texto normativo em alargar o seu espectro para cobrir toda e qualquer informação isolada ou agregada que sujeite um determinado indivíduo a um processo de decisão automatizada.

---

[1]Article 29 Working Party Opinion 04/2007 on the concept of personal data, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Dados Anônimos devem estar dentro do escopo do APL

"Quando uma regulamentação afirma que algum dado é "anônimo", ela está desconectada das melhores teorias da ciência computacional." (Cory Doctorow,*2013*).[2] "Um dado pode ser anônimo ou útil, mas nunca os dois" (Paul Ohm, 2010).[3] Tais afirmações sintetizam que o processo de anonimização é reversível e, que, portanto, um dado anônimo é sempre uma informação que pode levar a identificação de um indivíduo. Tais problemas minam, portanto, a própria semântica de dados anônimos, sendo, em última análise, uma teorização impossível (Antivigilância, 2015). Logo, o APL não deveria ter deixado dúvidas de que dado anônimo é, para os fins da lei, dado pessoal e, como tal, deveria estar dentro do escopo de proteção da lei, sob pena de se criar uma *ficção jurídica* perigosa para a (des)proteção dos dados pessoais.

Ao mesmo tempo, contudo, não se pode perder de vista que a anonimização é um padrão de segurança para a proteção de dados pessoais, devendo ser encorajada. Nesse sentido, a inovação em sentido amplo - seja dos modelos de negócio e na área das políticas públicas com o *open data* na era das cidades inteligentes - devem tomá-la como padrão, até para viabilizar tais práticas dependentes da mineração de base dados volumosas em que seria impraticável colher o consentimento de todos os titulares dos dados pessoais.

Por isso, concorda-se com as contribuições geradas na plataforma (InternetLab Reporta n° 04/2015) de manter dentro do escopo da lei a regulação dos dados anônimos, elencando-os como uma das exceções do consentimento. Tal exceção não deve, no entanto, esvaziar a regra eleita pelo APL, qual seja, de que o consentimento informado, expresso, específico e livre deve parametrizar o fluxo das informações pessoais. Por isso, tal exceção deve ser restringida às seguintes hipóteses e requisitos, sob pena da exceção tornar-se a regra:

i. no setor público para a implementação de políticas públicas (os casos de *open data* no exemplo das chamadas cidades inteligentes), devendo-se observar, no entanto, os limitadores propostos nessa contribuição para que haja uma paridade regulatória entre setor privado e estatal (vide: item e.3 dessa contribuição);
ii. no setor privado, o tratamento de dados anonimizados deve observar o teste proposto nessa contribuição para a hipótese de dispensa de consentimento baseada no "interesse legítimo" (vide: item b.3 dessa contribuição);
iii. a reversão do processo de anonimização é vedada, salvo mediante consentimento dos próprios titulares dos dados pessoais;
iv. o compartilhamento e o uso que se faz da base de dados anonimizados deve ser objeto de publicidade pelo setor privado, e objeto de autorização pelo setor público, de acordo, respectivamente, com o que dispõe o §3º do artigo 39, e artigo 24;
v. a disponibilização pública parcial e/ou completa de uma base de dados anonimizados estará sujeito à autorização do órgão competente, o qual avaliará

---

[2] http://www.politics.org.br/edicoes/prote%C3%A7%C3%A3o-de-dados-na-ue-certeza-da-incerteza
[3] "This research unearths a tension that shakes a foundational belief about data privacy: Data can be either useful or perfectly anonymous but never both."

os riscos de sua reidentificação, possibilitando, sempre que possível, a publicação de suas estatísticas agregadas ou outro formato adequado para fins de prevenção da reversão do processo de anonimização.

Registra-se que a publicidade disposta na alínea "e" é de total relevância para que o órgão competente e demais entidades legitimadas para a proteção de interesses difusos e coletivos possam fiscalizar esse trânsito de informações anonimizadas. Com efeito, como ensina Paul Ohm, o problema da reidentificação está atrelado, sobretudo, ao risco de se agregar dados anônimos com outra base de dados, de modo a permitir a fácil reversão do processo de anonimização – o que ele denomina de "entropia" da informação.

Por isso, uma forma de viabilizar a regulação desse fluxo informacional seria a criação da obrigação de emissão de relatórios de transparência, nos quais se identifica a origem da base de dados anonimizadas, as suas as entidades e atributos e, por fim, quem será o seu destinatário – com quem se compartilha. Seguindo-se, novamente, os ensinamentos do pesquisador da Colorado Law School, o legislador deve se preocupar com os atores cujo poderio informacional pode representar a "ruína", isto é, a reversibilidade do processo de anonimização. A proibição, tão somente, da reidentificação pode ser pouco, ou, quase nada, eficaz para se prevenir danos decorrentes da reversão do processo de anonimização.

O supracitado relatório não se confunde com a disponibilização pública de uma base de dados anonimizados. Naquele, relata-se, genericamente, no que consiste a própria base de dados (atributos e entidades) e o caminho por ela a ser percorrido – quem e com quem se compartilha. Enquanto que na outra, alínea "e", trata-se da disponibilização da base de dados em sua completude que, por tal motivo, deve ser, previamente, autorizado pelo órgão competente, verificando-se os riscos de reidentificação. Nesse sentido, as diversas pesquisas em que se comprovou a falácia teórica dos dados anônimos deram-se com a análise de base de dados anônimas disponibilizadas ao público (Caso AOL e Netflix, por exemplo). Dessa forma, a avaliação de tais riscos é o que deve parametrizar a proibição ou não da disponibilização da base de dados anonimizados, resguardando-se, sempre que possível, a possibilidade de tornar pública as suas estatísticas agregadas e/ou outro formato, cuja probabilidade de reidentificação seja reduzida.

Versão original	Sugestão de alteração
Art. 5	Art. 5
I - dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos	I - dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos, incluindo informações, isoladas ou agregadas, que possam sujeitar um indivíduo a um tratamento total ou parcialmente

	automatizado;
IV – dados anônimos: dados relativos a um titular que não possa ser identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular;	IV – anonimização: ato de tornar um dado não correlacionável ao seu titular, utilizando-se de técnicas que procurem não identificá-lo, direta ou indiretamente, com um indivíduo. Os dados anônimos são, para fins desta lei, dados pessoais em razão da possível reversibilidade de seu processo, ainda que disponha de regras próprias nos termos desta legislação;
XIV – dissociação: ato de modificar o dado pessoal de modo a que ele não possa ser associado, direta ou indiretamente, com um indivíduo identificado ou identificável;	XIV – ~~dissociação: ato de modificar o dado pessoal de modo a que ele não possa ser associado, direta ou indiretamente, com um indivíduo identificado ou identificável;~~ (deletar o inciso, uma vez que dissociação é uma das técnicas de anonimização, substiuindo-se a espécie pelo gênero em todas as passagens da legislação)
Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando o tratamento for indispensável para:	**Art. 11.** O consentimento será dispensado nas seguintes hipóteses:
	(...)
IV – realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;	VII – quando os dados forem anonimizados por um processo que deverá atingir um padrão de razoabilidade a ser, periodicamente, definido e fiscalizado pelo órgão competente para minimizar as possibilidades de reversão do processo de anonimização, devendo-se observar as seguintes hipóteses e requisitos;
	a) no setor público para a implementação de políticas públicas, observando-se o quanto disposto nos artigos 24 e 25;
	b) no setor privado para fins de interesses legítimos, de acordo com o disposto no inciso VIII deste artigo 11;
	c) a reversão do processo de anonimização é proibida, salvo mediante consentimento dos próprios titulares dos dados pessoais;
	d) o compartilhamento e o uso que se faz da base de dados anonimizados deve ser objeto de publicidade pelo setor privado, e

	objeto de transparência e autorização pelo setor público, de acordo, respectivamente, com o que dispõe o §3º do artigo 39, e artigo 24 e seguintes;
	e) a disponibilização pública parcial e/ou completa de uma base de dados anonimizados estará sujeito à autorização do órgão competente, o qual avaliará os ricos de sua reidentificação, possibilitando-se, sempre que possível, a publicação de suas estatísticas agregadas ou outro formato adequado para prevenir a reversão do processo de anonimização.
Art. 12. É vedado o tratamento de dados pessoais sensíveis, salvo:	**Art. 12.** É vedado o tratamento de dados pessoais sensíveis, salvo:
c) realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;	c) realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a anonimização dos dados pessoais;
Art. 17. O titular dos dados pessoais tem direito a obter:	**Art. 17.** O titular dos dados pessoais tem direito a obter:
IV – dissociação, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei.	IV – anonimização, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei.
§ 5º O responsável deverá informar aos terceiros a quem os dados tenham sido comunicados sobre a realização de correção, cancelamento, dissociação ou bloqueio dos dados, para que repitam idêntico procedimento.	§ 5º O responsável deverá informar aos terceiros a quem os dados tenham sido comunicados sobre a realização de correção, cancelamento, anonimização ou bloqueio dos dados, para que repitam idêntico procedimento.
Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo responsável, que verificará a observância das próprias instruções e das normas sobre a matéria.	**Art. 39.** O operador deverá realizar o tratamento segundo as instruções fornecidas pelo responsável, que verificará a observância das próprias instruções e das normas sobre a matéria.
§ 2º Órgão competente poderá determinar ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados, nos termos do regulamento.	§ 2º Órgão competente poderá determinar ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados, nos termos do regulamento.
	§ 3º Em caso de compartilhamento de

	base de dados anonimizados, o responsável deverá elaborar relatório de impacto à privacidade, a que alude o dispositivo anterior, descrevendo, obrigatoriamente, quais são as entidades e atributos das informações contidas na base de dados, e, por fim, quem será o seu recipiente.
Art. 50. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis por órgão competente:	**Art. 50.** As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis por órgão competente:
III – dissociação dos dados pessoais;	III – anonimização dos dados pessoais;

B. Consentimento

O consentimento é, como destacado pelo próprio Ministério da Justiça, a regra geral legitimadora para o tratamento dos dados pessoais. Dedica-se, pois, uma seção inteira – Seção I do Capítulo II do APL – que aloca o consentimento, como a forma prescrita, para delimitar a (i)licitude de toda e qualquer atividade de processamento de dados pessoais. Tem-se, assim, uma estratégia regulatória muito clara, qual seja, de que ao titular deve ser assegurado o direito de autodeterminar as suas informações pessoais (autodeterminação informacional), sendo, em última análise, o parâmetro nuclear para a proteção dos dados pessoais.

Nesse contexto, identificou-se a necessidade de que os comandos normativos em torno do consentimento devem avançar para a operacionalização de um consentimento real, a fim de funcionalizar um controle significativo por parte do titular sobre seus dados pessoais. Tal sugestão subdividiu-se sob três vertentes:

i. uma melhor delimitação do artigo 7º, § 1º, do APL, a fim de que a referida "indispensabilidade" em tal dispositivo não vulnere a programada perspectiva de controle dos dados pessoais, sobretudo em vista dos modelos de negócio denominados *zero-price advertisement business model*;
ii. o acréscimo de outros mecanismos, além das "destacadas cláusulas contratuais", que garantam uma comunicação mais adequada e eficiente para que o titular exerça o seu direito de controle sobre seus dados pessoais;
iii. uma melhor delimitação das hipóteses do consentimento, tal como a proposição de um teste para a cogitada exceção de interesses legítimos

B.1. A indispensabilidade dos dados pessoais e o consentimento "livre": melhor delimitação do artigo 7º, § 1º, do APL

O modelo de negócio prevalente na Internet é o chamado *zero-price advertisement business*. O consumidor não paga uma quantia monetária para acessar e utilizar serviços e produtos. Isto porque, eles são rentabilizados pelo uso de seus dados pessoais minerados para a entrega de publicidade e/ou conteúdo direcionado. Esse arranjo econômico é, portanto, conflitante com a "livre" escolha (consentimento) da utilização de dados pessoais, pois o usuário, no mais das vezes, deve concordar com tal prática, sob pena de não ter acesso ao serviço ou produto ("*take it or leave it*").

Nesse contexto, o texto do APL deve ter uma redação clara para contrabalancear tais interesses, sob pena de haver uma distorção da própria proteção de dados pessoais ancorada no consentimento do seu titular. Nesse sentido, tais modelos de negócio devem ser, a escolha do usuário, menos invasivos, minimizando-se, sempre que possível, a coleta e o tratamento de seus dados pessoais (princípios da necessidade, finalidade e etc.). Atualmente, por exemplo, os consumidores detêm, na maioria das aplicações, apenas controle sobre quais informações suas serão acessíveis por outros usuários, mas não em face do próprio serviço/produto.

Por isso, o § 1º, do artigo 7º, do APL deve ser completado por outro dispositivo para deixar claro que a "*microeconomia dos dados pessoais*" deve encontrar limites, possibilitando-se, ao menos, um *controle "granular"* em face das próprias aplicações.

Entende-se por um controle granular, a opção do titular em determinar, por exemplo: a) quais os tipos de dados pessoais serão coletados (geolocacionais, referentes ao seu estado saúde e etc..); b) a quais tipos de tratamento seus dados pessoais estarão sujeitos (para a entrega de conteúdo e/ou publicidade direcionada, para ativar determinadas funcionalidades de um aplicativo mobile e etc.); c) por quanto tempo e frequência durará o tratamento de suas informações pessoais.[4]

O consentimento granular estabelece, portanto, limites à microeconomia dos dados pessoais, na medida em que resguarda a opção do titular em emitir autorizações, de forma fragmentada, no tocante ao fluxo de seus dados pessoais. Por exemplo, uma aplicação pode oferecer inúmeras funcionalidades cujo funcionamento demanda, indispensavelmente, uma gama de dados pessoais para a sua operacionalização. Com a ressalva do consentimento granular, o titular poderá fazer o uso de tal aplicação, determinando, de forma correlacionada, quais dados pessoais seus serão tratados de acordo com as funcionalidades que pretende fazer uso. O titular possuiria, assim, um controle sobre seus dados pessoais em face do próprio produto e/ou serviço, na medida em que pode, de forma compartimentalizada, escolher como se dará o tratamento de suas informações pessoais.

Caso contrário, a ausência de tal ressalva possibilitaria, em tese, uma interpretação viciada do dispositivo supracitado. O modelo de negócio poderia determinar a indispensabilidade de um fornecimento irrestrito dos dados pessoais, esvaziando, por fim, a própria perspectiva de controle por parte do titular, ora disposta no *caput* do artigo 7º.

Versão original	Sugestão de alteração
Art. 7º O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11. §1º O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo em hipóteses em que os dados forem indispensáveis para a sua realização.	**Art. 7º** O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11. §1º O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo em hipóteses em que os dados forem indispensáveis para a sua realização. §2º Mesmo em tais hipóteses de indispensabilidade dos dados pessoais para o fornecimento de um produto ou serviço, deve-se assegurar ao titular opções menos invasivas mediante um controle granular dos seus dados pessoais, observando-se, especialmente, os princípios e a proteção contratual disposta nesta legislação.

[4] C.f., Opinion 02/2013 on apps on smart devices da Article 29 Working Party, p. 15 e Opinion 8/2014 on the on Recent Developments on the Internet of Things da Article 29 Working Party, p. 22).

B.2. uma comunicação adequada para operacionalizar um consentimento real

O consentimento deve ir além das "destacadas cláusulas contratuais", devendo-se verificar como a própria tecnologia poderia operacionalizar o consentimento. Diversos estudos já demonstraram que o canal de comunicação dos termos de uso de políticas de privacidade é ineficaz: poucas pessoas procedem a leitura desses textos que são longos, técnicos e complexos. E, mesmo que procedessem, estudos demonstram que a relação custo/tempo é insuportável. Por exemplo, um usuário despenderia mais de U$3.354,00 por mês - relação tempo/produtividade - para tal desiderato (McDonald and Cranor, 2009). Daí porque, é questionável se a existência de cláusulas contratuais destacadas é a melhor solução para que o usuário externalize o seu consentimento, e, por conseguinte, proteja seus dados pessoais.

Nesse contexto, a própria tecnologia deve empoderar o indivíduo conquanto ao controle das suas informações pessoais. Por exemplo, uma possível interação entre o usuário e o computador (*human computer interaction*/HCI) parece ser algo mais factível (Ryan Calo, 2011). A HCI considera a capacidade cognitiva do usuário para nele despertar uma reação que o habilitará a tomar uma real e efetiva decisão (Girish Prabhu, 1997). A exemplo de estímulos visuais que alertam e provocam o usuário para tal desiderato, ao invés de textos longos e de difícil compreensão de políticas de privacidade. Por isso, configurações mais limitativas - abordagem da *privacy by default* - estimularão uma interação com o usuário para colher o seu consentimento de forma pulverizada, tornando-o mais significativo e real.

Não se deve perder de vista, contudo, que essa interação pode gerar o mesmo efeito colateral das políticas de privacidade, qual seja, uma fadiga no consumidor prejudicial à autodeterminação de suas informações pessoais. Veja-se, nesse sentido, o exemplo europeu dos *disclaimers* dos *cookies* que afetaram, demasiadamente, a experiência de navegação dos usuários, de modo que eles o aceitavam, independentemente, de compreender no que resultava tal interação. Ao final, tal interação propiciou o descontrole, ao contrário do controle dos dados pessoais em razão dos usuários terem sido *sobrecarregados* com tais mensagens/alertas.

Por tal razão, deve-se pensar, complementarmente, como a própria tecnologia poderia automatizar a escolha do cidadão conquanto as suas preferências de privacidade, simplificando as suas escolhas (FTC, 2012). Nesse sentido, por exemplo, o *tracking preferences* da W3C possibilita que o usuário pré-estabeleça suas opções de privacidade para que tal protocolo, automaticamente, externalize-as durante a sua navegação. Desse modo, a experiência de navegação do usuário não seria tão afetada, evitando-se a sua exaustão em consentir, a todo o momento, para o fluxo de seus dados pessoais. Em outros termos, a própria tecnologia pode *massificar* as preferências de privacidade do consumidor diante, igualmente, de uma grande gama de relações por ele travadas em que o fluxo de seus dados pessoais é contínuo.

Em suma, tais considerações convergem com a linha matriz teórica da chamada *behavioral economics*. Esse campo da ciência econômica, cujo objeto é investigar os limites da racionalidade dos agentes econômicos, já identificou inúmeras limitações cognitivas do ser humano para autogerenciar suas informações pessoais. Por isso, o *policy making* de toda e qualquer legislação de proteção de dados pessoais deve levar

em consideração tais limitações, visando-se, sobretudo, a adoção de tecnologias que empoderem o cidadão com um melhor controle de suas informações pessoais - *privacy enhancing technologies* (Acquisiti, 2009). Tal vulnerabilidade pode e deve ser equacionada por meio da própria arquitetura da internet (Solove, 2004), notadamente por meio de tecnologias que habilite o cidadão a desempenhar um controle significativo sobre seus dados pessoais. Cabe ao operador fazer uso de tais tecnologias, estabelecendo-se uma comunicação eficiente para despertar no titular a capacidade de autogestão de seus dados pessoais, o que consiste, em última análise, em um dever de informação (Bioni, 2014).[5] Sugere-se, assim, as seguintes alterações no artigo 7º mediante o acréscimo de 03 novos parágrafos:

Versão original	Sugestão de alteração
Art. 7º O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11.	**Art. 7º** O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11.
(...)	(...)
§4º O consentimento deverá ser fornecido de forma destacada das demais cláusulas contratuais.	§4º O consentimento deverá ser fornecido de forma destacada das demais cláusulas contratuais;
	§5º O operador tem o dever de informar o titular a respeito do tratamento dos seus dados pessoais, utilizando-se das técnicas adequadas para que ele exerça um controle significativo sobre seus dados, como, por exemplo, um processo contínuo de interação pelo qual haja um consentimento recorrente e renovado, visando, todavia, não o sobrecarregar com o exercício de tal direito;
	§6º O quanto disposto no parágrafo anterior não prejudica a adoção de outras tecnologias que, concomitantemente,

[5] BIONI, Bruno Ricardo. O dever de informar e a teoria do diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores: convergências e divergências a partir da análise da ação coletiva promovida contra o Facebook e o aplicativo 'Lulu'. Revista de Direito do Consumidor, v. 94, p. 305: “Verifica-se, por todo o exposto, que o dever de informação funcionaliza a autodeterminação informacional/informativa, já que é necessário empregar uma comunicação adequada, na qual a informação prestada seja eficiente para tal desiderato, não só cientificando seu receptor da sua faculdade de autodeterminação informacional, mas, principalmente, como, em sede do ambiente eletrônico, fazer uso de tal funcionalidade (...) Percebe-se, portanto, que a informação avoca, antes de qualquer coisa, um papel que precede a autodeterminação informacional. Com efeito, trata-se de elemento que contorna o exercício de tal direito, circundando a própria racionalização da autodeterminação informacional”.

	empoderem o titular com um controle mais significativo sobre seus dados pessoais, tal como a implementação de mecanismos que expressem, de forma automatizada, as suas preferências de privacidade no tocante ao fluxo de seus dados pessoais;
§5º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.	§7º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais, respeitando as provisões do art. 10, §2º no caso de alteração das finalidades.
	§8º Os produtos e serviços deverão implementar mecanismos que asseguram, por configuração padrão, somente o tratamento de dados pessoais que são realmente necessários para o propósito específico que ensejou a sua coleta e que não vão além do mínimo necessário para tanto, bem como, por padrão, evitar o acesso aos dados por um número indefinido de indivíduos.[6]
§6º O consentimento pode ser revogado a qualquer momento, sem ônus para o titular.	§9º O consentimento pode ser revogado a qualquer momento, sem ônus para o titular.
§7º São nulas as disposições que estabeleçam ao titular obrigações iníquas, abusivas, que o coloquem em desvantagem exagerada, ou que sejam incompatíveis com a boa-fé ou a equidade.	§10º São nulas as disposições que estabeleçam ao titular obrigações iníquas, abusivas, que o coloquem em desvantagem exagerada, ou que sejam incompatíveis com a boa-fé ou a equidade.
§8º Cabe ao responsável o ônus da prova de que o consentimento do titular foi obtido em conformidade com o disposto nesta Lei.	§11º Cabe ao responsável o ônus da prova de que o consentimento do titular foi obtido em conformidade com o disposto nesta Lei.

[6] "The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals." (Redação proposta para a reforma da diretiva de proteção de dados da união europeia).

B.3. Hipóteses de dispensa do consentimento e o debate em torno do "interesse legítimo": a necessidade da criação de "filtros" para assegurar a regra do consentimento

O APL acompanhou a linha matriz de outras leis de proteção de dados pessoais ao redor do mundo, estabelecendo o consentimento do usuário como o vetor central para a proteção dos dados pessoais (vide: item B dessa contribuição). Nesse sentido, as exceções de tal regra não podem ser amplas ou mesmo genéricas, sob pena de se reduzir "a pó" a proteção dos dados pessoais baseada no consentimento do titular. Realizou-se, assim, um diagnóstico das hipóteses de dispensa de consentimento em três blocos (artigo 11 do APL):

Setor Público

No primeiro bloco com relação às hipóteses de dispensa do consentimento em favor do Estado (incisos II e VII), sugere-se uma nova redação que se afaste de uma permissão genérica, vinculando-a aos princípios da necessidade do APL e da eficiência da administração pública.[7] Se a qualidade da gestão pública em sentido *latu sensu* é, cada vez mais, pensada e arquitetada mediante a análise dos dados pessoais do cidadão, deve-se assegurar que tal prática esteja adstrita ao mínimo necessário para que o direito à privacidade não seja por ela sufocada. Da mesma forma, tais atividade devem se submeter a um procedimento próprio que garanta uma melhor regulação dos dados pessoais na esfera estatal (item e.3 dessa contribuição).

Produção científica e conhecimento

Em um segundo bloco, analisou-se a hipótese de dispensa de consentimento para a produção de pesquisa e conhecimento (inciso IV). Tal hipótese deve estar restrita, literalmente, aos casos de pesquisa "pura"[8] desvinculada de interesses comerciais e políticos. Caso contrário, o setor empresarial e estatal valer-se-iam de tal exceção para se desvencilharem da regulação que lhes é própria.

Propõe-se, ainda, a expressa vedação de tais pesquisas voltadas para as atividades de inteligência e investigação criminal dado o potencial danoso em face da liberdade do cidadão. Acredita-se que, com essa nova redação, tal hipótese de dispensa do consentimento restará, devidamente, limitada para que ela não seja uma "porta aberta" para distorcer a regra geral do consentimento.

Setor privado

No terceiro e último bloco, verificou-se as hipóteses de dispensa do consentimento pertinentes ao setor privado. Tal análise subdividiu-se em duas frentes: i) uma hipótese

---

[7] A eficiência trata-se de um princípio próprio da administração pública que, inclusive, encontra-se previsto no texto constitucional – artigo 37, *caput*, da Constituição Federal.

[8] Essa já havia sido a contribuição do GPoPAI na primeira consulta público sobre APL no ano de 2011.

já presente no APL (inciso III: execução de procedimentos pré-contratuais ou contratuais) e; ii) outra cogitada ao longo do debate público (interesses legítimos).

Execução de procedimentos pré-contratuais ou contratuais

A primeira refere-se ao inciso III, sugerindo-se a supressão de tal hipótese. Isto porque, seja para um procedimento pré-contratual ou para o cumprimento de obrigações contratuais, o titular deve, durante as tratativas negociais ou no próprio contrato, autorizar o tratamento de seus dados pessoais. Por exemplo, quem busca um financiamento, ou, quem deve provar sua liquidez financeira durante uma relação contratual autoriza, em razão do próprio interesse negocial subjacente, que seus dados pessoais sejam tratados para aferir sua capacidade financeira. O consentimento está, portanto, presente em tais situações.

Nesse sentido, o artigo 7°, alínea "b", da Diretiva da União Europeia,[9] aborda tal questão estipulando que o tratamento dos dados pessoais para a "performance" de um contrato, ou, como etapa preliminar necessária para uma relação contratual, deve se dar por requisição (entenda-se autorização) do titular. Portanto, não faz sentido a manutenção de tal hipótese de dispensa de consentimento que não está, nem mesmo, abraçada pela experiência estrangeira que talvez seja a fonte inspiradora desse dispositivo. Caso contrário, bastaria a mera tratativa negocial e/ou uma relação contratual, a fim de que o tratamento dos dados pessoais fosse realizado à revelia do consentimento do seu titular, configurando-se, em última análise, uma hipótese muito abrangente capaz de minar o pilar regulatório do APL.

Interesses legítimos

Observa-se que, durante o debate público, houve uma série de contribuições no sentido de que se deveria criar, a exemplo do que ocorre no direito comunitário europeu, outra hipótese para a dispensa do consentimento (American Bar Association, Center for Information Policy Leadership e Information Technology Industry Council).

Tratar-se-ia, especificamente, de uma hipótese em que o tratamento dos dados pessoais não demandaria a exigência de um consentimento expresso. As contribuições convergem para uma linha argumentativa no sentido de que exigir, a todo o momento, o consentimento do titular para o tratamento dos dados pessoais esbarraria, basicamente, em duas consequências indesejáveis: i) uma fadiga do próprio titular em controlar as suas informações pessoais, já que este seria sobrecarregado com uma enxurrada de alertas conquanto ao fluxo de seus dados pessoais; ii) um sistema inflexível prejudicial à inovação, tornando-se impraticável tratamentos adicionais dos dados pessoais que, no curso de uma relação já pré-estabelecida, melhoraria a sua experiência e, por vezes, até mesmo a sua segurança, como no caso de mineração de dados para fins de prevenção de fraudes.

---

[9] "Member States shall provide that personal data may be processed only if: (…) b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps **at the request** of the data subject prior to entering into a contract;"(grifos não constam do original)

O primeiro argumento é, de certa forma, alinhado com as preocupações já endereçadas nessa contribuição. No item b.3, abordou-se o *overloaded information* como fator prejudicial para a operacionalização de um consentimento genuíno a desencadear um controle significativo dos dados pessoais. Tem-se, no entanto, que essa adversidade deve-se muito mais às práticas correntes do mercado que dificultam, ao invés de facilitar, a autodeterminação informacional. Por isso, defende-se que tal matriz argumentativa não deve sabotar, ou mesmo, fragilizar o pilar normativo do APL, qual seja, o consentimento como a regra geral para o tratamento dos dados pessoais. Pelo contrário, deve-se apostar e pavimentar um caminho para que futuras tecnologias otimizem sua estratégia regulatória central, como se procurou sugerir com os acréscimos de parágrafos na seção relativa ao consentimento.

O segundo argumento é, também, convergente com outro apontamento desta contribuição, desta vez tecido sobre a necessidade da inclusão dos dados anônimos no escopo de aplicação do APL. No item a.2, observou-se que a capacidade de inovação é, cada vez mais, dependente da mineração de base de dados volumosas, hipóteses nas quais seria impraticável colher o consentimento de todos os titulares para o tratamento dos dados pessoais. Ter-se-ia, assim, um regime pouco flexível para fins de inovação, sobretudo com as possibilidades permitidas pela tecnologia do *Big Data*. Por isso, sugeriu-se, seja pela falácia teórica dos dados anônimos, seja para fins de um regime mais flexível à inovação, que os dados anônimos consistissem em uma nova hipótese de exceção do consentimento.

Diante de tais observações preliminares, tem-se que a cogitada nova exceção – interesses legítimos - pode ser combinada com o que foi sugerido a respeito dos dados anônimos, tornando-se a anonimização como um padrão e um dos requisitos para tal hipótese de dispensa do consentimento ao setor privado. É imprescindível a criação desses e outros requisitos para que tal exceção - a dispensa do consentimento – não se torne a regra,[10] sob pena de faltar coerência ao texto normativo do APL.

Por um lado, tais requisitos consistirão em um teste[11] para assegurar que, mesmo não havendo um *consentimento expresso*, os dados pessoais estarão dentro de uma esfera de controle do cidadão (alíneas "a", "b" e "c" do dispositivo sugerido). A exceção baseada no interesse legítimo está mais atrelada à *desqualificação* do consentimento como sendo expresso, do que, propriamente, à dispensa completa do consentimento (específico, livre e informado). Nesse sentido, o teste proposto visa garantir que o tratamento dos dados pessoais, lastreado nessa exceção, não seja desarrazoado, ferindo as legítimas expectativas de privacidade do seu titular.

E, sob outra vertente, um dos requisitos do teste proposto consistirá em um dever do operador de prevenção de danos à privacidade dos cidadãos, como a adoção do processo de anonimização e outras medidas adequadas de segurança que minimizem tais riscos (alínea "d").

---

[10] Veja-se a Opinião 06/2014 – the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC- da Article 29 que atenta que exceção do consentimento inequívoco, baseada no interesse legítimo, deve ser objeto de um teste de equilíbrio (*balance test*), sob pena de se propiciar abusos com a utilização de exceção.

[11] Buscou-se inspiração no teste proposto pela Article 29 em sua opinião 03/2013 – purposes limitation – p.43.

Tem-se como oportuno esse momento para que as contribuições dialoguem entre si, estruturando-se um verdadeiro debate que é o desiderato final da consulta pública. Neste caso, especificamente, pela preocupação de que essa cogitada nova exceção ao consentimento possa resultar em uma falta de controle dos dados pessoais por seu titular, o que deve ser equilibrado pela existência de requisitos que justifiquem o uso de tal exceção (InternetLab, Reporta n° 17/2015).

Alíneas "a", "b" e "c": a manutenção de uma determinada esfera de controle sobre os dados pessoais

Os três primeiros requisitos sugeridos preveem, respectivamente, que:

i. o tratamento dos dados pessoais deve guardar uma relação com o propósito para o qual os dados pessoais do titular foram, originariamente, coletados e para, daí;
ii. serem respeitadas as legítimas expectativas do titular com base no contexto da relação jurídica mantida por ele com o operador;
iii. que seja considerada a natureza dos dados pessoais – e.g. se sensíveis – e o impacto que o tratamento dos dados pessoais terá sobre a pessoa em causa.

Tais requisitos são abstratos e comportam uma série de interpretações. Contudo, tal norma, com conceitos abertos, é necessária para que a lei de proteção de dados pessoais seja flexível, a fim de não engessar a própria inovação dependente, por exemplo, da mineração de base de dados volumosas e, não descurando de um de dever de lealdade e boa-fé conquanto à proteção dos dados pessoais do cidadão. Ressalta-se, nesse sentido, que tal ideia está, parcialmente, alinhada com os cenários europeu e americano. Entidades já emitiriam documentos de *policymaking*, sugerindo-se tal ideia de privacidade baseada no contexto da relação jurídica, respectivamente, o *Article 29* (Opinião 06/2014) e a Federal Trade Commission (FTC, 2012).

Alguns exemplos podem ser esclarecedores para desvendar o alcance das normas sugeridas.

Exemplo 1

Esses requisitos permitiriam o tratamento de dados pessoais, sem que houvesse consentimento expresso, para uma determinada finalidade que é decorrente e ínsita de qualquer relação: a segurança e a prevenção de fraudes, por exemplo. Antes do Big Data, não era possível que uma instituição financeira pudesse minerar os dados pessoais dos seus consumidores para identificar padrões que fugissem à normalidade e constituíssem atividades fraudulentas. Tal tratamento dos dados é, certamente, vantajoso para o titular das informações pessoais, atendendo o *contexto* e às *legítimas expectativas* da relação subjacente com o operador da base de dados, e, por fim, tem um *impacto positivo* para a própria pessoa em causa.

Por outro lado, fugiria, contudo, ao contexto e à expectativa do consumidor, se a mineração dos dados fosse utilizada para categorizar perfis de consumidores inadimplentes por determinada regionalidade, e, assim, direcionar e/ou estabelecer um novo critério para concessão de crédito. Tal finalidade não detém, certamente, qualquer *relação* com o *propósito que originou* a coleta dos dados pessoais do cidadão para fazer uso de serviços bancários de forma geral, fugindo, completamente, da sua esfera de controle e de suas *expectativas* de acordo com o contexto de tal relação. Soma-se, ainda, o *impacto negativo* sobre a pessoa em

causa que teria a sua liberdade de contratar/consumo prejudicada. Nessa hipótese, gerar-se-iam, ademais, práticas discriminatórias, e.g. de acordo com as condições socioeconômicas prevalentes de determinadas regiões, o que é vedado pelo inciso IX do artigo 6º, e, em última análise, *impacta negativamente* o titular dos dados pessoais.

Exemplo 2

Toma-se, ainda, o exemplo de pesquisas científicas altruísticas na área da saúde. Seria razoável que tais bases de dados pudessem ser reutilizadas para a implementação de outras pesquisas científicas igualmente altruísticas ou mesma para a prevenção de surtos epidêmicos na área da saúde e no respectivo campo de políticas públicas.

Seria, contudo, contrário ao *contexto de tal relação subjacente*, às *expectativas legítimas* do titular dos dados pessoais e ao *propósito* altruístico que norteou, *originariamente*, tal coleta dos dados pessoais, se tais informações pessoais fossem compartilhadas com empresas farmacêuticas, ou, mesmo com empresas securitárias que poderiam parametrizar a sua atuação comercial. Nessa situação, ter-se-ia um *impacto negativo* sobre a esfera de liberdade do titular dos dados pessoais. Isto porque, eventualmente, a condição de saúde do titular, revelada por seus dados pessoais, poderia implicar em um aumento da contraprestação por tais serviços, ou, mesmo a recusa de contratação.

Alíneas "d": dever de prevenção para a minimização de riscos

Por último, tal tratamento de dados pessoais deve-se se dar, sempre que possível, de forma anonimizada e, sem prejuízo, de outras medidas de segurança que venham a minimizar os riscos à privacidade da pessoa em causa. Há, por exemplo, uma maior dificuldade em se limitar a liberdade ou discriminar uma pessoa, quando um dado não é, diretamente, a ela correlacionável. Previne-se, pois, um impacto negativo sobre a pessoa em causa (alínea "c"). Da mesma forma, em um eventual incidente de segurança, uma base de dados anonimizadas traria, em tese, menos riscos aos titulares de dados pessoais, já que para "alcançá-los" seria necessário reverter tal processo para reidentificá-los.

Registre-se que a anonimização referida deve ser lida, conjuntamente, com o dispositivo que regulamenta o uso e compartilhamento de base de dados anonimizadas. Em outras palavras, a interpretação conjunta de tais dispositivos é que disporá, *cumulativamente*, a respeito das obrigações do operador que faz uso de tal exceção, como, por exemplo, a emissão de relatório de transparência em caso de compartilhar uma base de dados anonimizada com terceiros (artigo 11, inciso VII, alínea "d").

Esse e os demais requisitos consistirão, portanto, em um teste limitador – "filtro legal" – de tal hipótese de dispensa de consentimento, acomodando-se, ao mesmo tempo, a proteção dos dados pessoais e a inovação, mantendo-se, ainda, a perspectiva de controle por parte do titular sobre seus dados pessoais. Em suma, na medida em que há o bônus de se valer da exceção ao consentimento expresso, tem-se o ônus de se observar tais deveres (leia-se requisitos) para que seja válido o uso de tal exceção, sob pena do tratamento dos dados pessoais ser ilícito.

Versão original	Sugestão de alteração
Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando o tratamento for indispensável para:	**Art. 11.** O consentimento será dispensado nas seguintes hipóteses e quando for indispensável para:
I – cumprimento de uma obrigação legal pelo responsável;	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;	II – tratamento e uso compartilhado de dados para o atendimento eficiente das finalidades próprias do Estado, observando-se o quanto disposto no artigo 24 e seguintes;
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;	~~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 anonimização dos dados pessoais;	III – realização de pesquisa histórica, científica ou estatística, desde que tais atividades não estejam vinculadas a atividade comercial, de administração pública, investigação criminal ou inteligência, garantindo-se, sempre que possível, a anonimização dos dados pessoais;
V – exercício regular de direitos em processo judicial ou administrativo;	IV – exercício regular de direitos em processo judicial ou administrativo;
VI – proteção da vida ou da incolumidade física do titular ou de terceiro;	V – 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.	VI – tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias, observando-se o quanto disposto no artigo 24 e seguintes.
§ 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.	VII – (nova hipótese de dados anônimos: item a.2 dessa contribuição)
§ 2º Nos casos de aplicação do disposto nos incisos I e II, será dada publicidade a	VIII – para interesses legítimos do operador, desde que não se sobreponha aos direitos fundamentais, liberdade e privacidade do titular previsto no artigo 1°, levando-se em consideração:[12]

[12] Já que as sugestões foram pensadas a partir do dispositivo 7(f) da Diretiva da União Europeia, deve-se, igualmente, ser observada a redação de tal dispositivo, sem prejuízo dos requisitos sugeridos:

esses casos, nos termos do parágrafo 1º do art. 6º. § 3º No caso de descumprimento do disposto no §2o, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado.	a) a relação entre o propósito especificado, originariamente, para a coleta dos dados pessoais e o tratamento adicional a que se refere esse inciso; b) o contexto da relação com o operador, em que se deu previamente a coleta dos dados pessoais, e as expectativas legítimas do seu titular, de acordo com o disposto no inciso II do artigo 6º; c) a natureza dos dados pessoais e o impacto que o tratamento dos dados pessoais terá sobre o titular; d) a adoção de medidas de segurança capazes de prevenir a ocorrência de danos em virtude do tratamento dos dados pessoais, e, sempre que possível, a anonimização, de acordo o que dispõem, respectivamente, os artigos 6º, inciso VIII, e as obrigações estabelecidas no inciso VII deste artigo 11. (sugerem-se as mesmas modificações com relação ao artigo 12, inciso II, que propõe, das alíneas “b” à “f”, basicamente as mesmas hipóteses de dispensa do consentimento acima tratadas pelo artigo 11)

“processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)”.

C. Direitos do titular e regime de responsabilidade civil

C.1. Direito de portabilidade: privacidade como elemento de competitividade

O consentimento somente será significativo se o usuário tiver opções, dentre os fornecedores de produtos e serviços, que lhes ofereçam melhores práticas conquanto à proteção de seus dados pessoais. A privacidade pode e deve ser um elemento de competição, a fim de que o próprio titular possa se valer de tal competitividade para fazer escolhas significativas (Bioni e Leite Monteiro, 2015). Por isso, deve ser elencado como um dos seus direitos, a portabilidade pela qual o titular possa "trocar" de prestador de serviço ou fornecedor de produto, levando com ele seus dados pessoais.

Ressalta-se que o exercício de tal direito dar-se-á, tão somente, mediante uma simples requisição por parte do titular. O ônus de estabelecer a transmissão dos dados deve ser imputado aos fornecedores de produtos ou serviços, cabendo a eles garantir a interoperabilidade entre suas bases de dados para funcionalizar tal migração, tal como já ocorre na telefonia móvel. Trata-se, em suma, de questões indissociáveis para o exercício efetivo de tal direito, sob pena da sua operacionalização recair sobre aquele que não possui a expertise técnica para tanto.

Sugere-se, por fim, a modificação da redação do direito de acesso. O acesso aos dados pessoais deve se dar mediante a obtenção de uma cópia em formato estruturado e em padrão aberto. Caso contrário, estar-se-ia comprometida a exequibilidade de tal direito, seja por conta de um formato ilegível, seja em razão de um padrão não executável em certos sistemas operacionais. Mais uma vez, o ônus operacional para o exercício dos direitos da legislação deve recair sobre quem tem expertise técnica para tanto, tornando menos assimétrica a relação entre o titular e o operador dos dados pessoais.

Versão original	Sugestão de alteração
Art. 17. O titular dos dados pessoais tem direito a obter:	**Art. 17.** O titular dos dados pessoais tem direito a obter:
I – confirmação da existência de tratamento de seus dados;	I – confirmação da existência de tratamento de seus dados;
II – acesso aos dados;	II – acesso aos dados, mediante a obtenção de cópia eletrônica, em formato estruturado e padrão aberto, de todos os seus dados pessoais junto ao operador responsável pelo tratamento de seus dados pessoais;
III – correção de dados incompletos, inexatos ou desatualizados; e	III – correção de dados incompletos, inexatos ou desatualizados; e
IV – anonimização, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei.	IV – anonimização, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta

	Lei. V - obter a portabilidade através de transmissão, mediante sua requisição, dos seus dados pessoais para outro fornecedor de serviço ou produto, cuja técnica, modalidade e procedimento poderão ser definidos pelo órgão competente ou por melhores práticas de mercado e, sem prejuízo, de revogar o seu consentimento nos termos do §6°, do artigo 7.[13]

C.2. Regime de responsabilidade civil objetiva: atividade de risco

Deve-se considerar que o tratamento de dados pessoais é uma atividade de risco, até porque eventual incidente de segurança pode ter consequências desastrosas para os titulares das informações pessoais das mais variadas formas: de uma eventual prática discriminatória até fraudes patrimoniais que são possibilitadas pelo acesso aos dados pessoais.

Tal risco acabará por incrementar os padrões de segurança de quem exerce a atividade risco, já que este procurará minimizar eventuais prejuízos decorrentes de indenizações. Um exemplo claro disso é o serviço de *internet banking* no qual as instituições bancárias são responsabilizadas, na maioria das vezes, por fraudes bancárias, indenizando seus clientes, independentemente de qualquer omissão, negligência, imperícia ou imprudência. Por isso, elas investem, cada vez mais, em padrões de segurança para mitigar tais perdas.

A mesma tônica deve ser adotada na legislação de proteção de dados pessoais.

Daí porque, o sistema que deve ser adotado é o da atividade de risco, a fim de que quem exerça a atividade de tratamento de dados pessoais seja responsabilizado objetivamente - independentemente de culpa. Essa é a tendência nas demais relações de consumo em que quem exerce uma atividade somente não será responsabilizado havendo culpa exclusiva da vítima ou força maior.

---

[13] "Article 18 Right to data portability 1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject. 2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn. 3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)." (redação proposta para a reforma da diretiva de proteção de dados da União Europeia).

Versão original	Sugestão de alteração
Art. 35. Todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano material ou moral, individual ou coletivo, é obrigado a ressarci-lo.	**Art. 35.** O tratamento de dados pessoais é atividade de risco e todo aquele que, em razão do exercício de tal atividade, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a ressarci-lo, independentemente de culpa, nos termos desta lei.
	§ 1º A exclusão da responsabilidade do operador e dos demais agentes que integram a cadeia de tratamento de dados pessoais somente se dará nos casos de culpa exclusiva da vítima ou força maior.
§ 1º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar excessivamente onerosa;	§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar excessivamente onerosa;
§ 2º O responsável ou o operador podem deixar de ser responsabilizados se provarem que o fato que causou o dano não lhes é imputável.	**Art. 38.** Os órgãos e entidades públicas responderão, independentemente de culpa, pelos danos morais, patrimoniais, individual ou coletivo causados a outrem decorrentes da gestão das suas bases dados.
Art. 38. As competências e responsabilidades relativas à gestão de bases de dados nos órgãos e entidades públicos, bem como a responsabilidade pela prática de atos administrativos referentes a dados pessoais, serão definidas nos atos normativos que tratam da definição de suas competências.	§1º As competências quanto à gestão de base de dados nos órgãos e entidades públicas serão definidas em atos normativos, sem prejuízo da responsabilidade civil objetiva do Estado por danos oriundos de tal atividade, conforme estabelecido no dispositivo anterior.

D. Transferência Internacional e p*rivacy by design*

A transferência internacional é um ponto central no APL, uma vez que nenhuma efetividade terá a nossa legislação se ela for permissiva para que haja a transmissão irrestrita de dados pessoais dos brasileiros para os chamados "paraísos dos dados pessoais" – *data forum shopping* - onde abusos podem ser perpetrados em prejuízo da privacidade do titular dessas informações.

Todavia, muitos argumentam ser inócua a tentativa de restringir a transferência internacional de dados através de procedimentos burocráticos ou regulamentação específica, pois a livre circulação de dados através de diferentes fronteiras nacionais estaria imbuída na própria metodologia de transmissão de dados da Internet por meio, *e.g.,* do protocolo TCP/IP. Que mesmo na existência de princípios como os da equivalência no nível proteção, os dados iriam circular, naturalmente, por diferentes jurisdições, umas mais protetivas, outras menos. Entretanto, esse argumento *per se* não deve inviabilizar medidas mais protetivas. Vejamos.

A ideia de privacidade é intrinsecamente ligada à ideia de perceptibilidade. Dificilmente haverá uma violação de privacidade perpetrada por meio de uma mera transmissão de dados. Independe a informação que os protocolos carregam, pois o conteúdo da informação não é percebido, uma vez que a infraestrutura de comunicação da Internet é o que pode ser conhecida por "*dumb network*". Ou seja, ela não deve (dentro dos limites do ser e do dever ser) ter conhecimento sobre o que circula no seu meio, deve apenas garantir o envio de um dado de um ponto para outro e utilizar o mínimo de dados possível para realizar tais atos (menor esforço).

Desta forma, quando uma legislação de proteção de dados refere-se à transferência internacional é necessário ter em mente que se trata de atos de tratamento que podem, eventualmente, tornar a informação cognoscível, como a coleta e/ou armazenamento. Isto porque, de fato, não é do interesse do legislador alterar a arquitetura *end-to-end* da Internet ou restringir o livre fluxo de dados. A mera transmissão de dados não é o destinatário das previsões da lei. Logo, o argumento de que a tentativa de implementar restrições é inócua deve ser interpretado sob o foco de que, realmente, tenta-se regular através de medidas limitadoras de transferência de dados internacionais.

D.1. Supressão do consentimento como hipótese de transferência internacional

Por isso, o APL deve ser restritivo conquanto a tal prática, o que determina a adoção de uma posição *paternalista* que não permita tal transferência em decorrência, tão somente, do consentimento do usuário. Deve-se, assim, eliminar a possibilidade da transferência internacional baseada na simples hipótese de consentimento do usuário. Tal transferência deve, na linha do que já determina o APL, ser objeto da verificação do nível de proteção da legislação, do *enforcement* de tal legislação, medidas de segurança e etc.

Caso contrário, o consentimento do próprio titular das informações pessoais poderá esvaziar qualquer efetividade da lei de proteção de dados pessoais, já que, em tese, a transferência internacional nele ancorada seria um meio de "burlar" todos os direitos e

deveres previstos na lei. O consentimento não deve, em última análise, ser um subterfúgio para comprometer toda a efetividade do corpo normativo da lei geral de proteção de dados pessoais, ainda que ele seja o seu pilar legislativo.

A autonomia da vontade não deve ser levada às últimas consequências, situando o seu próprio emissor em uma situação de extrema vulnerabilidade, tal como na hipótese de transferência internacional baseada, tão somente, no consentimento. Nesse caso, os dados pessoais trafegariam por ambientes com déficits regulatórios, tornando-se, ainda mais, suscetível a ocorrência de danos à privacidade do titular dos dados pessoais.

Mutatis mutandis, tratar-se-ia da hipótese, já vedada pelo texto proposto no APL, de que seria nula determinada cláusula contratual que estabelecesse obrigações iníquas, abusivas que coloquem o titular dos dados pessoais em situação de extrema desvantagem. Isto porque, a transmissão dos dados para um país com um nível deficitário de proteção de dados pessoais representa *per si* uma situação iníqua e de extrema desvantagem para o objeto regulatório em questão, qual seja, a proteção dos dados pessoais.

D.2. Selos de certificação

De forma similar ao sistema europeu de proteção de dados pessoais, o APL implementa outras possibilidades de transferência internacional de dados, seja através do reconhecimento pelo órgão competente do nível de proteção do país-destino, seja através de cláusulas-padrão ou normas corporativas globais.

Todavia, a própria experiência europeia tem demonstrado que a viabilização de transferências internacionais através desses métodos pode ser demasiadamente burocrática, ou, torna-se uma ficção jurídica, como o *Safe-Harbour Agreement* entre a União Europeia e os Estados Unidos. Por isso, diversos outros sistemas de proteção de dados têm sugerido métodos mais eficientes para garantir um nível adequado de proteção. Um bom exemplo para fins de inspiração são as Regras de Privacidade Transfronteiriças da APEC (CBPR). Dentre as regras, há a possibilidade da utilização de uma certificação internacional que se refere a um selo ou marca de privacidade atribuído aos operadores e responsáveis pelo processamento de dados pessoais por organização, pública ou privada, reconhecida pelo órgão competente. Tal selo é o que atesta, portanto, que determinados países-destinatários estão em conformidade com a legislação protetiva do país-transmissor ou que aqueles conferem nível de proteção similar ou superior aos estabelecidos por estes últimos. O objetivo maior desse método seria desburocratizar os procedimentos necessários para permitir a transferência internacional, levando em consideração as próprias características da economia digital e da arquitetura da Internet, além de diminuir o fardo do órgão competente.

D.3. *Privacy by design*

Sob outra ótica, a privacidade deve ser um valor na fase de desenvolvimento de *softwares* e *hardwares*, de modo que as próprias aplicações tenham nelas imbuído tal valor. Esse é, em poucas palavras, o conceito de *privacy by design* (Rubistein e Good, 2012) que pode ser uma diretriz para padrões de segurança no APL, tal como um dos critérios para a transferência internacional de dados, incentivando-se tal prática.

Este critério poderia ser operacionalizado por meio da vinculação do operador às cláusulas contratuais-padrão (artigo 29 do APL). Empregar-se-ia, assim, uma maior vinculação do operador conquanto ao seu compromisso de respeitar o nível de proteção adequada dos dados pessoais do país-transmissor. Isto porque, tais compromissos contratuais seriam traduzidos por uma *accountability imbuída* no desenvolvimento da própria tecnologia para o tratamento dos dados pessoais.

Em suma, sugere-se que o APL seja alterado para remover a possibilidade de transferência internacional de dados através do mero consentimento, para incluir a certificação internacional como forma de reconhecimento do nível de proteção, e, por fim, para que a *privacy by design* seja mais um dos critérios para permitir a transferência internacional.

Versão original	Sugestão de alteração
Seção IV – Segurança e Sigilo dos Dados	**Seção IV – Segurança e Sigilo dos Dados**
Art. 42. O operador deve adotar medidas de segurança técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, ou qualquer forma de tratamento inadequado ou ilícito.	**Art. 42.** O operador deve adotar medidas de segurança técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, ou qualquer forma de tratamento inadequado ou ilícito.
Parágrafo único. As medidas de segurança devem ser compatíveis com o atual estado da tecnologia, com a natureza dos dados e com as características específicas do tratamento, em particular no caso de dados sensíveis.	§1° As medidas de segurança devem ser compatíveis com o atual estado da tecnologia, com a natureza dos dados e com as características específicas do tratamento, em particular no caso de dados sensíveis.
	§2° O operador deverá levar em consideração, durante todo o tratamento dos dados pessoais, os direitos e obrigações previstos nessa lei, implementando medidas técnicas e organizacionais concebidas para a proteção dos dados pessoais.
	§3° O órgão competente irá estabelecer os padrões técnicos mínimos para tornar aplicável o quanto disposto no parágrafo anterior, levando-se em consideração desde a fase de concepção do produto ou

	serviço até a sua execução.[14]
CAPÍTULO V – TRANSFERÊNCIA INTERNACIONAL DE DADOS	CAPÍTULO V – TRANSFERÊNCIA INTERNACIONAL DE DADOS
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 as seguintes exceções:	**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 as seguintes exceções:
(...)	(...)
Art. 29. Nos casos de países que não proporcionem nível de proteção equiparável ao desta Lei, o consentimento de que trata o art. 7º será especial, fornecido:	~~**Art. 29.** Nos casos de países que não proporcionem nível de proteção equiparável ao desta Lei, o consentimento de que trata o art. 7º será especial, fornecido:~~
I – mediante manifestação própria, distinta da manifestação de consentimento relativa a outras operações de tratamento; e	~~I – mediante manifestação própria, distinta da manifestação de consentimento relativa a outras operações de tratamento; e~~
II – com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos, de acordo com as circunstâncias de vulnerabilidade do país de destino.	~~II – com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos, de acordo com as circunstâncias de vulnerabilidade do país de destino.~~
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	**Art. 29.** 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

[14] "**Protection By Design And By Default** 1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals. 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services. 4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)." (redação proposta para a reforma da diretiva de proteção de dados da União Europeia).

contratuais aprovadas para uma transferência específica, em cláusulas contratuais-padrão ou em normas corporativas globais, nos termos do regulamento.	contratuais aprovadas para uma transferência específica, em cláusulas contratuais-padrão, em normas corporativas globais ou certificação de nível internacional reconhecida pelo órgão competente, nos termos do regulamento.
§ 1º 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.	§ 1º 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.
§ 2º 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, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.	§ 2º 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, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.
§ 3º Na análise de cláusulas contratuais ou de normas corporativas globais submetidas à aprovação de órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.	§ 3º Na análise de cláusulas contratuais ou de normas corporativas globais submetidas à aprovação de órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.
	§ 4º A certificação internacional mencionada no *caput* do presente artigo faz referência a selo ou marca de privacidade atribuído aos operadores e responsáveis pelo processamento de dados pessoais por organização, pública ou privada, reconhecida pelo órgão competente, atestando que estes estão em conformidade com a legislação protetiva de um ou mais países e de que estes conferem nível proteção similar ou superior aos estabelecidos pela presente lei.

	§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no *caput* serão, também, analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §2° e §3°do artigo 42.
Art. 31. O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa.	**Art. 31.** O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa.
Art. 32. No caso de transferência internacional de dados de 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.	**Art. 32.** No caso de transferência internacional de dados de 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.
Art. 33. Órgão competente poderá estabelecer normas complementares que permitam identificar uma operação de tratamento como transferência internacional de dados pessoais.	**Art. 33.** Órgão competente poderá estabelecer normas complementares que permitam identificar uma operação de tratamento como transferência internacional de dados pessoais.

E. Disparidade regulatória entre setor privado e estatal[15]

A proposta encaminhada abaixo sugere uma maior ênfase na proteção dos dados pessoais manejados pelo setor público que pode ser mais bem regulamentada no APL. Acredita-se que a regulação do Estado no tratamento de dados pessoais é tão, senão mais importante que a regulamentação do setor privado.

De fato, a proteção da privacidade nasce, historicamente, como um anteparo contra os abusos de poder pelo Estado, com as demandas pela inviolabilidade do lar e o sigilo de correspondência presentes já na Petição de Direitos Inglesa de 1628. A Lei brasileira que regulamente o tratamento de dados pessoais deve seguir essa matriz de proteção do indivíduo no exercício de seus direitos civis e políticos contra o abuso do poder do Estado.

As revelações do ex-analista da *National Agency Secutity*/NSA, Edward Snowden, confirmam tal preocupação, tendo sido revelado um esquema de vigilância em massa que, até hoje, não se sabe, ao certo, a extensão do programa. Cabe observar que, ao que tudo indica, tal esquema de vigilância em massa contou com a colaboração de corporações privadas e mais de um país em específico – os chamados *Five Eyes*. Nesse sentido, temas como a interconexão de base de dados privados e do setor público, bem como a transferência internacional acabam, por invariavelmente, circundar tal tensão regulatória. Uma estratégia regulatória mais ou menos permissiva em tais aspectos tem, portanto, um impacto crucial na proteção dos dados pessoais dos cidadãos e, em última análise, na própria efetividade da nossa futura legislação de proteção de dados pessoais (Observatório da Privacidade e Vigilância, 2015).

Nesse contexto, identificou-se uma certa permissividade abrangente no tocante às disposições regulatórias em face do Estado presentes no APL, o que configura, de certa maneira, uma disparidade frente a outras disposições mais rígidas desenhadas em face do setor privado. Quer-se, com isso dizer, que se deve buscar um equilíbrio entre tais aspirações regulatórias. Se, por um lado, o APL pode ser vanguardista para a proteção dos dados pessoais em face do setor privado, ele pode, por outro lado, representar um retrocesso no que diz respeito à proteção da privacidade em face do Estado. Desta feita, buscou-se sugerir propostas sob três frentes:

i. todas as disposições normativas sobre o tema devem ser reunidas no capítulo V, empregando-se uma melhor organicidade e sistematização ao tratamento da matéria, facilitando, em última análise, o trabalho de interpretação/aplicação da lei que contará com uma ordem sequencial lógica sobre o tema;

ii. regulamentação do tratamento de dados no curso de investigações criminais;

iii. um procedimento mais rígido para o tratamento dos dados pessoais pelo setor público, devendo sempre haver autorização do órgão competente para o tratamento de base de dados compartilhadas e objeto de interconexão.

[15]Essas considerações já haviam sido tecidas pelo GPoPAI na primeira consulta pública do APL (2011).

E.1. Organicidade nas disposições regulatórias sobre o tema

Acredita-se que, salvo melhor juízo, não houve uma alocação sistematizada das normas sobre tal temática. Via de regra, as disposições preliminares servem para esclarecer o escopo de aplicação da lei, estabelecer definições terminológicas e princípios, enfim, disposições que irão orientar, genericamente, a aplicação/interpretação da lei. Quaisquer disposições regulatórias que delineiem um comando normativo específico devem ser reunidas em seções ou capítulos que, por uma identidade temática, desenharão sequencialmente os deveres e direitos pertinentes a tal matéria. Facilita-se, em última análise, a própria interpretação/aplicação da lei.

Por isso, acredita-se que o §3° do artigo 2°, parágrafo único do artigo 4° e o §1° e §2° do artigo 6° devem ser reunidos no capítulo IV – Comunicação e Interconexão –, porque eles regulamentam a transferência de um banco de dados para outro envolvendo o setor público. Dito de outra forma, esses dispositivos não são normas introdutórias/gerais, mas comandos normativos que regulamentam, especificamente, a atividade do fluxo de dados pessoais envolvendo a administração pública.

Nesse sentido toma-se, como exemplo, o §1° do artigo 6°, que é citado três vezes no Capítulo V. Trata-se de um indicativo que tal norma deveria estar nele alocada, pois a sua recorrente remissão revela que tal norma parametriza a própria aplicação da regulamentação proposta naquele capítulo.

Em outros termos, não se trata de uma disposição preliminar. Pelo contrário, trata-se de uma norma que impõe, especificamente, o dever da administração pública ser transparente, publicizando as suas atividades de tratamento, tal como toda e qualquer atividade de interconexão e comunicação de dados – a temática do Capítulo V.

E.2. Difusão de dados pessoais para investigações criminais

Nossa proposta é que a requisição de dados para a investigação criminal necessite de autorização judicial e só possa ser autorizada para crimes de maior potencial ofensivo. Segue-se a lógica do Marco Civil da Internet/MCI (Lei n° 12.965/14: seção II do Capítulo II) pela qual se impede, via de regra, que os dados pessoais possam ser solicitados diretamente pela autoridade policial, criando um filtro para as solicitações não fundamentadas. Avança-se, no entanto, no sentido de restringir essa possibilidade à investigação de delitos de maior potencial ofensivo, impedindo a banalização da requisição e manipulação dos dados pessoais, reduzindo o potencial de dano causado por vazamentos e pelo tratamento indevido e, por fim, alargando tal proteção para dados que vão além do ambiente eletrônico – o escopo limitado de aplicação do MCI.

Transporta-se, ainda, dois pontos levantados na regulamentação do Marco Civil da Internet para a discussão do debate público do APL. Trata-se de questões pertinentes para a proteção de dados pessoais no curso de investigações criminais para, também, ampliar o seu escopo de aplicação para além do ambiente eletrônico.

A primeira para que se excepcione o acesso a dados pessoais, sem autorização judicial, somente à seara dos dados cadastrais e para um espectro limitado de

autoridades, tal como propõe, taxativamente, a Lei de Lavagem de Dinheiro e das Organizações Criminosas (IASP, 2015).

A segunda para que as autoridades requerentes dos dados pessoais tenham a obrigação de emitir relatórios de transparência sobre tais requisições extrajudiciais e judiciais (Brito Cruz, 2015). Contudo, entenda-se que tal obrigação deve ser ampliada para que as entidades privadas emitam, também, tais relatórios. Ter-se-á, assim, um retrato abrangente da "quebra de sigilo" dos dados pessoais e de relatórios de transparência das "duas pontas" – quem requer e quem concede o acesso. Possibilitar-se-á, assim, uma transparência e publicidade maior, permitindo que entidades de defesas de direitos difusos e coletivos monitorem, efetivamente, tais ações.

E.3. *Checks and balances*: um procedimento mais rígido para o tratamento dos dados pessoais pelo setor público

Uma das dificuldades em regular o setor público no tratamento de dados pessoais é que o procedimento pensado para o setor privado, baseado em autorizações individuais, dificultaria ou mesmo impediria o exercício das atividades administrativas e de fiscalização do Estado. No entanto, os princípios da transparência, da finalidade e da proporcionalidade deveriam, obviamente, ser aplicados ao Estado, como já o fez, parcialmente, algumas disposições do APL.

Creia-se, contudo, que existem ainda certas disposições muito permissivas que merecem uma melhor restrição. Acredita-se, por exemplo, que a interconexão e comunicação da base de dados entre setor privado e público e entre o próprio setor público deveria sempre contar com a autorização do órgão competente (Autoridade de Garantia: item "f" dessa contribuição), afastando-se a exigência, tão somente, de um informe específico. Nessa lógica, sugere-se um mecanismo de revisão no qual entes legitimados para defesa de interesses transindividuais possam interferir nesses procedimentos, recorrendo para impedir ou restringir autorizações concedidas que sejam consideradas excessivas ou arbitrárias.

Um exemplo pode esclarecer tal dinâmica:

Exemplo

O Ministério do Desenvolvimento Social solicita ao órgão competente autorização para comunicação com banco de dados pessoais da Secretaria Estadual de Educação para comprovar se os filhos dos beneficiários do Bolsa Família estão frequentando a escola (condição para concessão do benefício). O órgão competente julga se o pedido é pertinente e se os dados pessoais são realmente necessários. Assim que haja a concessão da autorização, o órgão competente publiciza a autorização de comunicação de banco de dados entre a Secretaria Estadual de Educação e o Ministério de Desenvolvimento Social. Desta forma, todo cidadão poderá consultar a listagem das autorizações concedidas pelo órgão competente e descobrir quais dados pessoais são utilizados por quais órgãos governamentais, para que finalidade e por quanto tempo. Se há abuso ou erro de julgamento por parte do órgão competente, entidades de defesa dos direitos transinvidividuais estariam capacitadas para agir em nome dos interesses da coletividade dos titulares dos dados pessoais, podendo recorrer da decisão. Assim, preservam-se para o setor público, de maneira coletiva, princípios como o da transparência, da finalidade, e da proporcionalidade sem impedir que o Estado cumpra suas funções regulares devido à necessidade de autorização de cada titular para cada uso.

Sugere-se ainda que, sempre que possível, o tratamento dos dados pessoais deva se dar por meio de dados anonimizados, uma vez que tal padrão de segurança minimizaria os riscos para a privacidade do cidadão, na medida em que, em tese, seria mais difícil de identificá-lo diretamente. Tal disposição está harmonizada com a sugestão da criação de uma nova hipótese de dispensa de consentimento dos dados anônimos para fins de implementação de políticas públicas (item a.2 dessa contribuição).

No exemplo acima, tem-se que a anonimização não seria possível. Contudo, a de-identificação dos dados pessoais seria possível para, por exemplo, a implementação de uma política pública de mobilidade urbana. Nesse caso, o necessário mapeamento do tráfego populacional não demandaria a identificação de cada cidadão em trânsito. Mas, tão somente, de estatísticas agregadas conquanto aos horários, vias e outras informações, simultâneas ou não, para exercer um melhor controle do tráfego e outras ações coordenadas para operacionalizar tal política pública.

Em resumo, pretende-se alcançar um significativo sistema de freios e contrapesos (*checks and balances)* para o tratamento dos dados pessoais envolvendo a administração pública, mediante inclusão de um ator imparcial nesse fluxo de dados pessoais. Em outros termos, um procedimento mais rígido que traga maior transparência e a possibilidade de se prevenir abusos e excessos e, por fim, como regra adoção dos dados anônimos para a minimização dos riscos para a privacidade dos cidadãos.

Versão original	Sugestão de alteração
Capítulo IV – Comunicação e Interconexão	**Capítulo IV – Comunicação, Interconexão e o Tratamento dos Dados Pessoais pelo Estado**
Art. 23. A comunicação ou interconexão de dados pessoais entre pessoas de direito privado dependerá de consentimento livre, expresso, específico e informado, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.	**Art. 23.** A comunicação ou interconexão de dados pessoais entre pessoas de direito privado dependerá de consentimento livre, expresso, específico e informado, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.
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:	**Art. 24.** A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado e entre as próprias pessoas jurídicas e órgãos públicos sem o consentimento livre, expresso, específico e informado do titular, só será admitido mediante o seguinte procedimento:
I – nas hipóteses de dispensa do consentimento previstas nesta Lei;	
II – nos casos de uso compartilhado de dados previsto no inciso XVII do art. 5º, em que será dada publicidade nos termos	§ 1o A pessoa jurídica de direito público interessada na interconexão ou comunicação de dados pessoais deve fazer solicitação formal ao órgão

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. Parágrafo único. A autorização prevista no inciso III do caput poderá ser condicionada: I - à comunicação da interconexão aos titulares, nos termos do §1º do art. 6º; II - ao oferecimento aos titulares de opção de cancelamento de seus dados; ou III - ao cumprimento de obrigações complementares determinadas por órgão competente.	competente; § 2º A solicitação deve ser circunstanciada, explicando a necessidade de interconexão e comunicação, comprovando-se: a) a necessidade do tratamento dos dados para o cumprimento eficaz de uma finalidade dentro da sua competência; b) a impossibilidade de atender de maneira eficaz esta finalidade por outros meios que dispensem o tratamento de dados pessoais, em particular se forem sensíveis; c) que solicita o tratamento da menor quantidade de dados necessária para atender eficazmente a finalidade especificada; d) que os dados sejam, sempre que possível, anonimizados, de acordo com as obrigações previstas no artigo 11, inciso VII, justificando-se, de forma circunstanciada, a sua impossibilidade e/ou a adoção de outras medidas de segurança. § 3º O órgão competente julgará a adequação da solicitação mediante a análise dos princípios dispostos nessa legislação, atendendo-a parcialmente ou totalmente, bem como estabelecendo o período de validade para a autorização, os procedimentos para cancelamento posterior e medidas de segurança aplicáveis; § 4º Uma vez autorizado o estabelecimento de uma comunicação ou interconexão dos dados pessoais, tal decisão, com as razões que a embasaram, deve ser publicizada pelo órgão competente. § 5º Os legitimados para ações coletivas e ação civil pública poderão recorrer da decisão do órgão competente que poderá rever decisão anterior com base na avaliação de novos elementos providos

	por essas entidades.
	Art. 25. Os órgãos e entidades de direito público darão publicidade às suas atividades de tratamento de dados pessoais por meio de informações claras, precisas e atualizadas em veículo de fácil acesso, preferencialmente em seus sítios eletrônicos. (versão modificada do artigo 6°, §1°)
Art. 25. A comunicação ou interconexão entre órgãos e entidades de direito público será objeto de publicidade, nos termos do §1º do art. 6º, e obedecerá às regras gerais deste Capítulo.	§1° A comunicação, interconexão e o uso compartilhado dos dados pessoais deve atender uma finalidade específica para a execução de políticas públicas e/ou pertinente às atribuições legais desempenhadas pelos órgãos e entidades públicas, respeitando-se os princípios da finalidade, adequação e necessidade, e, sempre que possível, proceder a anonimização dos dados pessoais, de acordo, respectivamente, com o disposto no artigo 6°, incisos I, II e III, e obrigações estabelecidas pelo artigo 11, inciso VII.
Art. 26. O órgão competente poderá solicitar, a qualquer momento, aos órgãos e entidades públicos que realizem interconexão de dados e o uso compartilhado de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir recomendações complementares para garantir o cumprimento desta Lei.	**Art. 26.** O órgão competente poderá solicitar, a qualquer momento e mesmo após a concessão da autorização prevista no artigo 24, aos órgãos e entidades públicos que realizem interconexão de dados e o uso compartilhado de dados pessoais, um informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir recomendações complementares para garantir o cumprimento desta Lei.
	Art. 27. É vedado aos órgãos públicos e entidades públicas efetuar a transferência de dados pessoais constantes de base de dados que administram ou a que tenham acesso no exercício de dados pessoais constantes de base de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto os casos de execução terceirizada ou mediante concessão e permissão de atividade

	pública que o exija e exclusivamente para fim específico e determinado. (antigo §3, do artigo 1°)
	§1° A terceirização, a que alude o *caput*, para fins de segurança pública, defesa, segurança do Estado, ou atividades de investigação e repressão de infrações penais, somente serão permitidas sob a tutela de pessoa jurídica de direito público, bem como mediante o processo de autorização do órgão competente disposto no artigo 24. (versão modificada do artigo 4°, parágrafo único)
Art. 27. Órgão competente poderá estabelecer normas complementares para as atividades de comunicação e interconexão de dados pessoais.	**Art. 28.** Órgão competente poderá estabelecer normas complementares para as atividades de comunicação e interconexão de dados pessoais.
Art. 5º Para os fins desta Lei, considera-se:	**Art. 5º** Para os fins desta Lei, considera-se:
XVII - uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos; e	XVII - uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, para uma ou mais modalidades de tratamento delegados por esses entes públicos, mediante autorização do órgão competente nos termos do 24.
TRANSFERÊNCIA INTERNACIONAL DE DADOS	TRANSFERÊNCIA INTERNACIONAL DE DADOS
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 as seguintes exceções:	**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 as
	seguintes exceções:
I - quando a transferência for necessária para a cooperação judicial internacional entre órgãos	I - quando a transferência for necessária

públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;	para a cooperação judicial internacional entre órgãos públicos de investigação, de acordo com os instrumentos de direito internacional e mediante a aplicação do quanto disposto no capítulo V; (capítulo de difusão de dados pessoais no curso de investigação criminal)
II - quando a transferência for necessária para a proteção da vida ou da incolumidade física do	II - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
titular ou de terceiro;	
III - quando órgão competente autorizar a transferência, nos termos de regulamento;	III - quando órgão competente autorizar a transferência, nos termos de regulamento;
IV - quando a transferência resultar em compromisso assumido em acordo de cooperação	IV - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional, mediante autorização do órgão competente nos termos do 24;
internacional;	
V - quando a transferência for necessária para execução de política pública ou atribuição legal do	V - quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, mediante autorização do órgão competente nos termos do 24.
serviço público, sendo dada publicidade nos termos do §1o do art. 6o.	Inclusão de capítulo e artigos
	CAPÍTULO V- O TRATAMENTO DE DADOS PESSOAIS NO CURSO DE INVESTIGAÇÃO CRIMINAL
	Art. 29. O tratamento de dados pessoais para utilização por autoridade policial para fins de investigação e repressão de delitos somente poderá ser feita mediante autorização judicial e quando o delito investigado tiver penalidade prevista no Código de Processo Penal superior a dois anos.
	§1°. Os dados cadastrais para finalidades investigativas submeter-se-ão a regime jurídico próprio previsto em legislação específica das Leis n° 9.613/98 e 12.850/2013.
	Art. 30. As autoridades de investigação e o setor privado devem elaborar relatórios públicos de transparência sobre a difusão

	de dados pessoais no curso de investigação criminal, cabendo ao órgão competente estabelecer a periodicidade e quais informações deverão compor tais relatórios.

F. O imprescindível "órgão competente"

A figura de um órgão fiscalizador da norma de proteção de dados pessoais é essencial para que haja o seu efetivo *enforcement*. Nesse sentido, o intitulado "órgão competente" - referenciado 34 (trinta e quatro) vezes no APL - deve ter assegurado a sua independência funcional e uma gama de poderes que torna viável a sua atuação. Mesmo que se discuta o desenho e o regime jurídico do "órgão competente", deve-se assegurar, desde logo, que ele tenha autonomia e poderes, assegurando-se a aplicabilidade e o cumprimento da nova legislação de proteção de dados pessoais. Deste modo, deve-se afirmar, na linha da Carta de Direitos Fundamentais da União Europeia, a independência de tal "órgão competente" e ainda retomar a primeira versão do APL de proteção de dados pessoais na qual os seus diversos poderes são elencados.

Ressalta-se que principalmente após a revisão das *guidelines* sobre privacidade da Organização para Cooperação Econômica e Desenvolvimento/OECD (Privacy Framework, 2013) criou-se uma rede global de autoridades de garantias (GPEN). Por tal rede as autoridades de garantia agem cooperativamente e de maneira interoperável para uma *enforcement* efetivo a nível global. Nesse contexto, a não previsão do órgão competente poderá resultar em um alto custo para a efetividade da projetada lei geral de proteção de dados. Deve-se levar em consideração, sobretudo, que tal arranjo global permitirá superar questões problemáticas de jurisdição que poderiam prejudicar a proteção de dados pessoais sob a égide da legislação brasileira, mas que foram transferidos para outro país. Se esse outro país tiver uma autoridade de garantia, associada a essa rede global, facilitar-se-ia, em tese, a fiscalização dessas atividades de tratamento sujeitas à legislação nacional.

Por fim, deve-se dar nova redação ao artigo 50 para que o "órgão competente" também seja investido do poder de aplicar infrações ao setor governamental e não, somente, ao setor privado. De outra maneira, causar-se-ia uma completa distorção regulatória entre tais setores, vulnerando, por fim, a própria proteção de dados pessoais.

Versão original	Sugestão de alteração
CAPÍTULO VIII – SANÇÕES ADMINISTRATIVAS	CAPÍTULO VIII – SANÇÕES ADMINISTRATIVAS E DA INDEPENDÊNCIA DO ÓRGÃO COMPETENTE
Art. 50. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis por órgão competente:	**Art. 50.** O cumprimento dos direitos e obrigações estabelecidos nesta lei fica sujeitos à fiscalização[16] por parte do órgão competente, assegurando-se a sua independência com autonomia administrativa, orçamentária e financeira, cuja estrutura e atribuições serão

[16]Art. 8º, 3 da Carta de Direitos Fundamentais da União Europeia: "O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente".

estabelecidas nos termos do regulamento.

Art. 51. Compete ao órgão competente:

I - zelar pela observância desta lei, de seu regulamento e do seu regimento interno;

II - planejar, elaborar, propor, coordenar e executar ações da política nacional de proteção de dados pessoais;

III - editar normas e provimentos sobre matérias de sua competência;

IV - aprovar seu regimento interno;

V - receber, analisar, avaliar e encaminhar consultas, denúncias, reclamações ou sugestões apresentadas por titulares de dados pessoais, entidades representativas ou pessoas jurídicas de direito público ou privado, referentes à proteção de dados pessoais, nos termos do regulamento;

VI – aplicar, de ofício ou a pedido de parte, conforme o caso, sanções, medidas corretivas e medidas preventivas que considere necessárias, na forma desta lei;

VII – criar, manter e publicar, para fins de transparência, um registro de bancos de dados pessoais de caráter de categorias e setores que considere relevantes, nos termos de regulamento;

VIII - verificar se os tratamentos respeitam as normas legais e os princípios gerais de proteção de dados;

IX - promover o conhecimento entre a população das normas que tratam da matéria e de suas finalidades, bem como das medidas de segurança de dados;

X - vetar, total ou parcialmente, o tratamento de dados ou prover seu bloqueio se o tratamento se torna ilícito ou inadequado, nos termos de regulamento;

XI - reconhecer o caráter adequado do nível de proteção de dados do país de destino no caso de transferência internacional de dados pessoais, bem como autorizar uma transferência ou série de transferências para países terceiros

	que não contem com este nível adequado;
	XII - determinar ao responsável pelo tratamento de dados pessoais, quando necessário, a realização de estudo de impacto à privacidade, na forma de regulamento.
	XIII - fomentar a pesquisa acadêmica em torna do tema da proteção de dados pessoais, dada a sua autonomia financeira;
	XIV – estabelecer e fiscalizar os padrões técnicos para que os direitos e obrigações previstos nessa lei sejam implementados por meio de medidas técnicas e organizacionais para a proteção dos dados pessoais, levando-se em consideração desde fase de concepção do produto ou serviços até a sua execução;
	XV - desenvolver outras atividades compatíveis com suas finalidades.
	Art. 52. Os Estados, o Distrito Federal e os Municípios poderão criar suas próprias autoridades de proteção de dados pessoais, com competência concorrente e nas suas respectivas áreas de atuação administrativa.
	Art. 53. Sem prejuízo das sanções civis e penais cabíveis e de outras sanções administrativas a serem definidas em normas específicas, as infrações das normas previstas nesta Lei ficam sujeitas, conforme o caso, às seguintes sanções administrativas:
I – multa simples ou diária;	I – multa simples ou diária;
II – publicização da infração;	II – publicização da infração;
III – dissociação dos dados pessoais;	III – dissociação dos dados pessoais;
IV – bloqueio dos dados pessoais;	IV – bloqueio dos dados pessoais;
V – suspensão de operação de tratamento de dados pessoais, por prazo não superior a dois anos;	V – suspensão de operação de tratamento de dados pessoais, por prazo não superior a dois anos;
VI – cancelamento dos dados pessoais;	VI – cancelamento dos dados pessoais;
VII – proibição do tratamento de dados	VII – proibição do tratamento de dados

sensíveis, por prazo não superior a dez anos; e	sensíveis, por prazo não superior a dez anos; e
VIII – proibição de funcionamento de banco de dados, por prazo não superior a dez anos.	VIII – proibição de funcionamento de banco de dados, por prazo não superior a dez anos.
§ 1º As sanções poderão ser aplicadas cumulativamente.	§ 1º As sanções poderão ser aplicadas cumulativamente.
§ 2º Os procedimentos e critérios para a aplicação das sanções serão adequados em relação à gravidade e à extensão da infração, à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do infrator e aos prejuízos causados, nos termos do regulamento.	§ 2º Os procedimentos e critérios para a aplicação das sanções serão adequados em relação à gravidade e à extensão da infração, à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do infrator e aos prejuízos causados, nos termos do regulamento.
§ 3º Os prazos de proibição previstos nos incisos VII e VIII do caput poderão ser prorrogados pelo órgão competente, desde que verificada a omissão no cumprimento de suas determinações, a reincidência no cometimento de infrações ou a ausência de reparação integral de danos causados pela infração.	§ 3º Os prazos de proibição previstos nos incisos VII e VIII do caput poderão ser prorrogados pelo órgão competente, desde que verificada a omissão no cumprimento de suas determinações, a reincidência no cometimento de infrações ou a ausência de reparação integral de danos causados pela infração.
§ 4º O disposto neste artigo não prejudica a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.	**Art. 54.** Sem prejuízo das sanções cabíveis, o órgão competente, atuando de ofício ou a pedido de parte, deverá impor, aos responsáveis que incorram em infração às normas desta lei, as medidas corretivas que considere necessárias para reverter os efeitos danosos que a conduta infratora tenha causado ou para evitar que esta se produza novamente no futuro, fixando o valor da multa diária pelo seu descumprimento.
§ 5º O disposto nos incisos III a VII poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei no 8.112, de 11 de dezembro de 1990 e na Lei no 8.429, de 2 de junho de 1992.	§ 1º As decisões administrativas transitadas em julgado que apliquem medidas corretivas em favor do titular dos dados constituem título executivo extrajudicial.
	§ 2º Sempre que as medidas corretivas se dirigirem a um titular específico, é deste a legitimidade para executar a decisão.
	Art. 44. Em qualquer fase do processo administrativo é facultado à Autoridade de

	Garantia adotar medidas preventivas, de ofício ou a pedido de parte, quando houver indício ou fundado receio de que o representado, direta ou indiretamente, cause ou possa causar à coletividade lesão irreparável ou de difícil reparação no âmbito da proteção de dados pessoais, ou torne ineficaz o resultado final do processo, fixando o valor da multa diária pelo seu descumprimento.