

COALIZÃO
DIREITOS NA
REDE

PROTEÇÃO DE DADOS PESSOAIS E SISTEMA NACIONAL DE DEFESA DO CONSUMIDOR: ANÁLISE DO PLC 53/2018

Nota técnica produzida para o Departamento de Proteção e Defesa do Consumidor
Secretaria Nacional do Consumidor, Ministério da Justiça¹

Autores

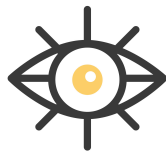
*Rafael A. F. Zanatta, Bárbara Simão e Juliana Oms
Instituto Brasileiro de Defesa do Consumidor*

1. Por que a Lei Geral de Dados Pessoais fortalece o Sistema Nacional de Defesa do Consumidor

A aprovação da Lei Geral de Proteção de Dados Pessoais (PLC 53/2018) representa um ciclo de renovação no Sistema Nacional de Defesa do Consumidor, fortalecendo os direitos individuais e difusos protegidos pela Lei 8.078/1990 (Código de Defesa do Consumidor) e ampliando as capacidades de coordenação de uma política nacional de defesa do consumidor no século XXI.

Na *United Nations Guidelines for Consumer Protection*, publicada pelas Organização das Nações Unidas em 2016, no capítulo que trata de "Princípios para boas práticas de negócios" (Item IV), recomenda-se que "empresas devem proteger a privacidade dos consumidores por meio de uma combinação do controle apropriado, segurança, transparência e mecanismos de consentimento relacionados à coleta e ao tratamento de dados pessoais". Os Estados-membros, como o Brasil, devem "desenvolver, fortalecer e manter uma política forte

¹ O presente documento foi elaborado pela Coalizão Direitos na Rede (www.direitosnarede.org.br) para o Departamento de Proteção e Defesa do Consumidor em julho 2018.



**COALIZÃO
DIREITOS NA
REDE**

de proteção de dados pessoais", tendo como um dos princípios básicos a proteção da privacidade e da proteção de dados pessoais.²

A aprovação de Lei Geral de Proteção de Dados Pessoais (LGPD) cumpre com os requisitos da ONU ao permitir um sistema harmônico de proteção de dados pessoais. Esse sistema harmônico, fruto de um trabalho que teve início em 2010 e que se fortaleceu em 2016 com a Comissão Especial de Tratamento e Proteção de Dados Pessoais, busca alinhar um sistema de proteção à privacidade já existente no Brasil, porém fragmentado em mais de 40 normas jurídicas do setor financeiro, de saúde, de crédito e telecomunicações.³

Há muitos anos, a doutrina brasileira de proteção ao consumidor reconhece que a proteção de dados pessoais é um direito fundamental, já reconhecido no art. 43 do Código de Defesa do Consumidor.⁴ Essa mesma doutrina apontava para as limitações do próprio Código de Defesa do Consumidor e a necessidade de uma legislação abrangente para criar um verdadeiro “sistema de governança” sobre a coleta e o uso legítimo de informações pessoais tanto pelo Poder Público quanto pelo setor privado. Nesse sentido, pela sua abrangência, pelo seu nível de detalhamento conceitual e pela identificação de princípios jurídicos próprios ao uso de dados pessoais, a Lei de Proteção de Dados Pessoais é superior ao nível jurídico que o Brasil se encontrava até sua aprovação, caracterizado por uma verdadeira “colcha de retalhos”⁵ de normas jurídicas.

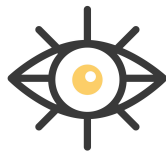
Em um sistema jurídico fragmentado, é difícil para o Sistema Nacional de Defesa do Consumidor (SNDC) realizar o adequado trabalho de prevenção e reparação de violação de direitos. O antigo sistema de proteção de dados pessoais ficava limitado aos parâmetros dados pelo art. 43 do Código de Defesa do Consumidor (Lei 8.078/1990), o art. 3º da Lei Geral de Telecomunicações (Lei 9.472/1997), as regras de sigilo bancário (Lei Complementar

² UNITED NATIONS, *United Nations Guidelines for Consumer Protection*. Geneva, 2016, p. 16: http://unctad.org/en/PublicationsLibrary/ditccplpmisc2016d1_en.pdf

³ MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. *Jota*, 14 de julho de 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018>

⁴ LIMBERGER, Têmis. Proteção dos dados pessoais e comércio eletrônico os desafios do século XXI, *Revista de Direito do Consumidor*, v. 17, n. 67, p. 215-241, jul./set. 2008. MENDES, Laura S. O direito fundamental à proteção de dados pessoais. *Revista de Direito do Consumidor*, v. 79, 2011, p. 45-81.

⁵ ZANATTA, Rafael A. F. A Proteção de Dados entre Leis, Códigos e Programação: os limites do Marco Civil da Internet, in: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. *Direito e Internet III: Marco Civil da Internet*. São Paulo: Quartier Latin, 2015, p. 451.



**COALIZÃO
DIREITOS NA
REDE**

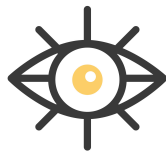
105/2001), as regras de proteção da vida privada da pessoa natural prevista no Código Civil (Lei 10.406/2002, art. 21), os direitos dos consumidores em cadastro positivo (Lei 12.414/2011) e os princípios de proteção de dados pessoais previstos no Marco Civil da Internet (Lei 12.965/2014). Esse sistema fragmentado, em geral, conta com os seguintes **problemas e lados negativos**:

- Sofre com a falta de harmonização conceitual de dados pessoais (o que são dados pessoais);
- Estabelece princípios gerais de dever de sigilo e respeito à privacidade (*e.g.* telecomunicações e regras bancárias), porém não possui regras mais detalhadas sobre o que deve ocorrer em caso de vazamentos de dados e incidentes de segurança;
- Não possui um regime harmonizado de responsabilização civil e não garante a devida segurança jurídica para os fornecedores e para os consumidores;
- Limita-se, em razão do Marco Civil da Internet, a garantir os direitos de transparência e “consentimento livre e informado” somente às relações de consumo com serviços de aplicações de Internet (*e.g.* Netflix), não se aplicando a todo o “universo off-line”, gerando uma situação bastante peculiar de um certo nível de proteção aos dados pessoais no nível on-line e quase completa desproteção de dados pessoais no mundo off-line, como no caso de farmácias⁶ ou sistemas de transporte.⁷

A Lei Geral de Proteção de Dados Pessoais (PLC 53/2018) aprovada pelo Congresso Nacional - primeiro, no dia 29 de maio, na Câmara dos Deputados e, depois, no dia 10 de julho no Senado Federal -, busca solucionar esses problemas e lados negativos por meio de uma ampla definição de conceitos na legislação (o que são “dados pessoais”, o que são “dados sensíveis”, o que são “dados anonimizados”, o que é “tratamento”, e assim por diante) e por meio de um sistema de princípios e regras bem calibrados.

⁶ MARCHETTI, Bruno, A distopia do 'me fala o CPF' nas farmácias do Brasil, Revista Vice, 15 de fevereiro de 2018. Disponível em: https://www.vice.com/pt_br/article/9kzbx5/por-que-farmacias-insistem-para-ter-seu-cpf

⁷ AFFONSO, Carlos. A privacidade saiu dos trilhos no metrô de São Paulo, TecnoFront, 18 de abril de 2018. Disponível em: <https://tecfront.blogosfera.uol.com.br/2018/04/18/a-privacidade-saiu-dos-trilhos-no-metro-de-sao-paulo/>



**COALIZÃO
DIREITOS NA
REDE**

Como notado por acadêmicos do campo de direito e tecnologia,⁸ as vantagens dessa abordagem seriam:

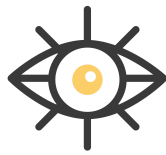
- Unificar as normas jurídicas, tornando-as harmônicas sobre o uso de dados pessoais, independentemente do setor econômico (regras transversais);
- Garantir maior flexibilidade ao autorizar várias hipóteses para o tratamento de dados pessoais que não somente o consentimento, tais como “legítimos interesses”, fortalecendo uma ideia de “integridade contextual”⁹ da privacidade (a ideia de que as expectativas legítimas de privacidade são sempre dependentes de seu contexto, sendo ele tecnológico e informacional);
- Estabilização das normas de direito do consumidor com as regras de proteção de dados pessoais, aumentando a confiança da sociedade na coleta e uso dos dados pessoais;¹⁰
- Aumento da segurança jurídica e capacidade de maior cooperação internacional para garantia dos direitos assegurados na própria Lei Geral de Proteção de Dados Pessoais;

Uma das grandes inovações da Lei Geral de Proteção de Dados Pessoais é a criação de uma “autoridade nacional” (órgão da administração pública indireta responsável pelo cumprimento desta Lei) que poderá atuar em regime de cooperação institucional com o Sistema Nacional de Defesa do Consumidor e com a crescente comunidade internacional

⁸ MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. *Jota*, 14 de julho de 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018>

⁹ BIONI, Bruno. *Autodeterminação Informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet*. Faculdade de Direito da Universidade de São Paulo, 2016 (propondo a “reavaliação de tal paradigma normativo [autodeterminação informacional], investigando-se, de forma ambivalente, como a autodeterminação informacional poderia ser melhor operacionalizada e, por outro lado, como a proteção dos dados pessoais poderia ser normatizada substantivamente sob o relato normativo complementar da privacidade contextual”).

¹⁰ BIONI, Bruno. Brasil precisa ser competitivo em uma economia de dados, *Jornal Valor Econômico*, 19 de julho de 2018 (defendendo que “nenhuma das leis setoriais existentes foram desenhadas e são vocacionadas para lidar com o fenômeno altamente complexo de uma economia e sociedade cada vez mais movida por dados. É essa lei geral que fornecerá organicamente o conjunto completo de direitos e deveres de todos os atores desse ecossistema, conferindo segurança jurídica tanto ao cidadão, como, também, ao setor estatal e privado sobre como deve se dar o fluxo desses dados”).



**COALIZÃO
DIREITOS NA
REDE**

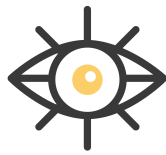
dedicada ao tema da proteção de dados pessoais.¹¹ No próximo tópico, detalharemos como essa cooperação institucional poderá ocorrer e quais os direitos básicos afirmados na legislação.

2. Os direitos básicos afirmados na legislação e o papel do diálogo institucional entre SNDC e Autoridade Nacional de Proteção de Dados Pessoais

O PLC 53/2018 enviado à sanção presidencial afirma que “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade” (art. 7º). Nessa relação entre a pessoa natural (o “titular dos dados pessoais”) e aquele que coletou seus dados (o “controlador”), a Lei é clara ao afirmar que o titular tem o direito de exercer, perante o controlador, nove direitos básicos. Tais direitos podem ser exercidos “a qualquer momento e mediante requisição” (art. 8º). São eles:

- *Confirmação da existência de tratamento*: toda pessoa tem o direito de saber se há ou não tratamento de dados pessoais por parte de um controlador;
- *Acesso aos dados*: uma vez identificado o tratamento, a pessoa tem direito de acessar os dados pessoais, tal como assegurado no Código de Defesa do Consumidor;
- *Correção de dados incompletos, inexatos ou desatualizados*: toda pessoa pode corrigir, gratuitamente, dados que não representem a realidade ou que estejam desatualizados;
- *Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade*: se uma pessoa percebe que há coleta de informações excessivas (como, por exemplo, a identificação de minha religião e anotação dessa informação em bancos de dados a partir dos meus hábitos de consumo de alimentos no iFood), há o direito de eliminação dessas informações;
- *Portabilidade dos dados a outro fornecedor de serviço ou produto*: apesar de depender de regulamentação do órgão controlador, o projeto de lei prevê o direito de

¹¹ BENNETT, Colin J.; RAAB, Charles. *The Governance of Privacy: Policy instruments in global perspective*. London: Routledge, 2017 (detalhando as formas de diálogo institucional e a complexidade da “caixa de ferramentas” da governança da privacidade em nível nacional e internacional).



**COALIZÃO
DIREITOS NA
REDE**

portabilidade de dados pessoais de um fornecedor a outro (exemplo: possibilidade de mover dados do Netflix para GloboPlay);

- *Eliminação dos dados tratados com o seu consentimento:* o titular de dados pessoais poderá pedir a eliminação de dados pessoais após o fim da relação de consumo com o fornecedor;
- *Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados:* o titular dos dados pessoais tem o direito de saber quais são as entidades privadas (parceiros comerciais) que o controlador possui e como os dados são compartilhados (por exemplo, o direito de saber quem são os parceiros comerciais do WhatsApp e quais as empresas, dentro do grupo Facebook Inc., que poderiam receber os metadados gerados pela utilização do aplicativo);
- *Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa:* toda pessoa tem o direito de saber o que aconteceria caso ela opte por não consentir com a coleta de dados pessoais. Isso pode ter implicações, por exemplo, tanto na negativa de transmitir o CPF em uma farmácia quanto na discordância em transmitir certos tipos de dados em um aplicativo;
- *Revogação do consentimento:* toda pessoa poderá revogar seu consentimento, isto é, mudar de ideia e cancelar o elemento que dá sustentação ao contrato eletrônico que permite a coleta e transmissão de dados pessoais;

Os direitos básicos descritos acima, previstos no art. 8º do PLC 53/2018, podem ser exercidos tanto perante a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) quanto perante os órgãos de defesa do consumidor. O projeto de lei diz:

“Art. 8º O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

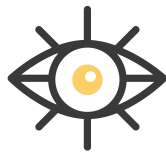
I - confirmação da existência de tratamento;

II - acesso aos dados;

(...)

1§ O titular dos dados pessoais, em relação aos seus dados, tem o direito de peticionar contra o controlador perante a autoridade nacional.

(...)



COALIZÃO
DIREITOS NA
REDE

8§ O direito a que se refere o 1§ deste artigo também poderá ser exercido perante os órgãos de defesa do consumidor”

Não há colisão da Autoridade Nacional de Proteção de Dados Pessoais com a Secretaria Nacional do Consumidor, com o Ministério Público Federal ou com outros órgãos responsáveis pela proteção dos direitos difusos no Brasil.

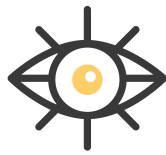
A Autoridade Nacional de Proteção de Dados Pessoais, tal como desenhada no PLC 53/2018, é órgão integrante da administração pública federal indireta, submetida a regime autárquico especial e vinculada ao Ministério da Justiça (art. 55). Sua estrutura de governança incorpora elementos de agências reguladoras e órgãos multissetoriais como o Comitê Gestor da Internet, pois há um **Conselho Diretor** (órgão máximo composto por 3 conselheiros com mandatos de quatro anos¹²) e, abaixo, um **Conselho Nacional de Proteção de Dados Pessoais e da Privacidade** (conselho de proposição de diretrizes estratégicas e formulação de estudos técnicos composto por 23 representantes titulares¹³). Como notado por acadêmicos da área, “a criação da Autoridade Nacional de Proteção de Dados é um dos pontos fortes da LGPD. O pressuposto essencial de seu funcionamento reside na sua expertise, independência, bem como em seu poder sancionatório e regulatório”¹⁴.

No desenho institucional formado pela Autoridade Nacional de Proteção de Dados Pessoais, cria-se um sistema de **cooperação** ao invés de um sistema de **competição** com o Sistema Nacional de Defesa do Consumidor.

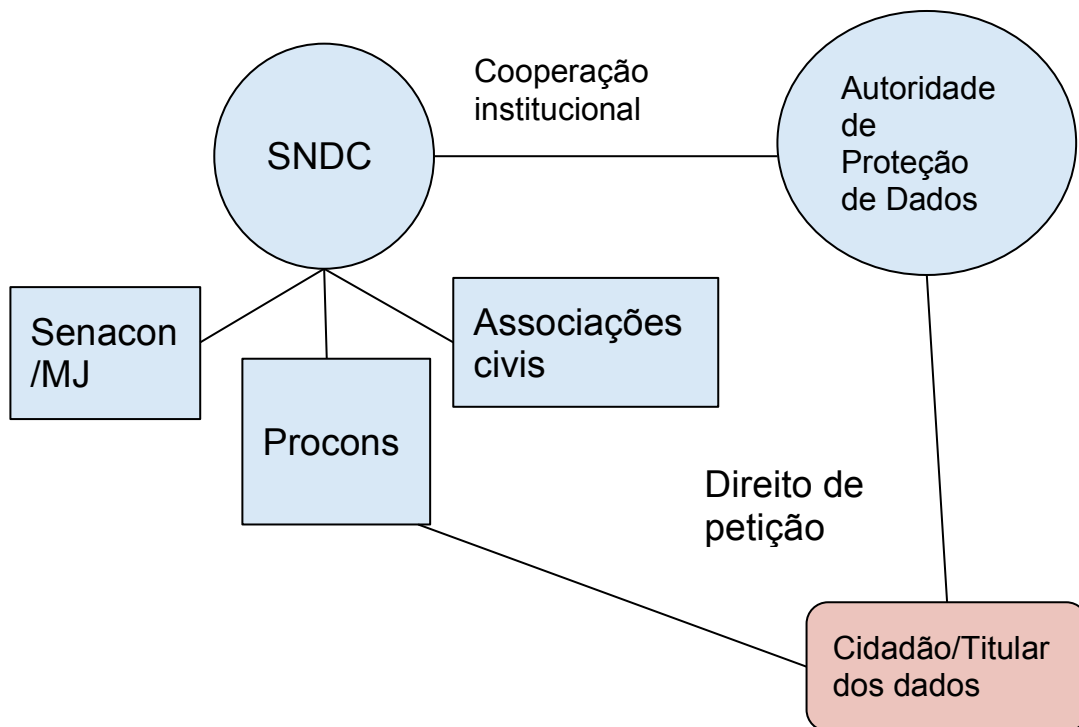
¹² O PLC 53/2018 estabelece que os mandatos dos primeiros membros do Conselho Diretor serão de 3 (três), 4 (quatro) e 5 (cinco) anos, conforme estabelecido no decreto de nomeação.

¹³ No Conselho, 6 representantes são do Poder Executivo Federal, 1 indicado pelo Senado, 1 indicado pela Câmara, 1 indicado pelo Conselho Nacional de Justiça, 1 indicado pelo Conselho Nacional do Ministério Público, 1 indicado pelo Comitê Gestor da Internet, 4 representantes da sociedade civil com atuação comprovada em proteção de dados pessoais e 4 representantes de entidade representativa do setor empresarial afeto à área de tratamento de dados pessoais (art. 58).

¹⁴ MENDES, Laura S.; DONEDA, Danilo. Lei de proteção de dados não pode morrer na praia, *Jornal Folha de São Paulo*, 20 de julho de 2018. Disponível em: <https://www1.folha.uol.com.br/opiniao/2018/07/laura-schertel-mendes-e-danilo-doneda-lei-de-protacao-de-dados-nao-pode-morrer-na-praia.shtml>



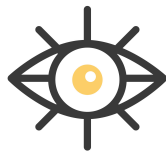
**COALIZÃO
DIREITOS NA
REDE**



O cidadão possuirá direito de petição para os Procons e para a Autoridade de Proteção de Dados Pessoais. Ao mesmo tempo, o sistema de cooperação institucional poderá ser fortalecido na seguinte forma:

- A Secretaria Nacional do Consumidor poderá contar com o apoio técnico da Autoridade Nacional de Proteção de Dados Pessoais para seu trabalho de prevenção e reparação de direitos em nível administrativo. Isso significa que a existência da ANPD **não irá bloquear** o trabalho prévio já desenvolvido pela Senacon, mas poderá fortalecer as capacidades de investigação da Secretaria Nacional do Consumidor e a construção de casos paradigmáticos na fronteira entre direitos dos consumidores e direitos digitais, como o “Caso Oi Phorm”¹⁵ e o “Caso Decolar.com”¹⁶;

¹⁵ Ver <http://www.justica.gov.br/news/ministerio-da-justica-multa-oi-por-monitorar-navegacao-de-consumidores-na-internet> (“O Departamento de Proteção e Defesa do Consumidor (DPDC) da Secretaria Nacional do Consumidor (Senacon/MJ) multou a TNL PCS S/A (Oi) em R\$ 3,5 milhões por infrações às normas de defesa do consumidor. A condenação foi motivada em razão do serviço Navegador disponibilizado aos consumidores do Velox, serviço de banda larga da Oi. Durante o processo administrativo foram constatadas violações ao direito à informação, à proteção contra a publicidade enganosa, além do direito à privacidade e intimidade”).



**COALIZÃO
DIREITOS NA
REDE**

- A Autoridade de Proteção de Dados Pessoais poderá contar com a participação da própria Secretaria Nacional do Consumidor no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, considerando que o Poder Executivo Federal poderá indicar representante do Ministério da Justiça ou da própria Secretaria Nacional do Consumidor. Nesse caso, a Senacon teria diálogo institucional interno, dentro da própria Autoridade, ao fazer parte do conselho multissetorial responsável por estabelecer as diretrizes estratégicas da futura Política Nacional de Proteção de Dados Pessoais;
- A Secretaria Nacional do Consumidor poderá estabelecer acordos de cooperação técnica com a Autoridade Nacional de Proteção de Dados Pessoais. Nesses casos, será possível aprofundar questões específicas de direitos dos consumidores no uso de novas tecnologias intensivas em dados pessoais (exemplo: assistentes domésticos dotados de serviços de Inteligência Artificial¹⁷). Será possível, também, realizar atividades em conjunto, como “hackatons”, seminários técnicos e guias para empreendedores que querem implementar as melhores práticas de proteção de dados pessoais aos seus consumidores, tal como feito, nos últimos anos, pela Federal Trade Commission nos Estados Unidos da América¹⁸;

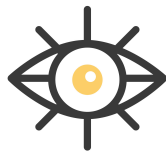
3. Fortalecimento da defesa de direitos difusos e cooperação internacional

A aprovação do PLC 53/2018 também irá fortalecer a tutela de interesses difusos e coletivos como um todo. O art. 12 da proposição dispõe expressamente que a defesa dos interesses dos usuários poderá exercida coletivamente em juízo. Este ponto é essencial, já que

¹⁶ Ver <http://defesadoconsumidor.gov.br/portal/ultimas-noticias/690-decolar-com-e-multada-por-pratica-de-geo-pricing-e-geo-blocking> (“Em decisão inédita no Brasil, o Departamento de Proteção e Defesa do Consumidor (DPDC), órgão do Ministério da Justiça, publicou hoje no Diário Oficial da União decisão que condenou a Decolar.com ao pagamento de multa de R\$ 7.500.000,00 (sete milhões e quinhentos mil reais) por diferenciação de preço de acomodações e negativa de oferta de vagas, quando existentes, de acordo com a localização geográfica do consumidor, técnicas conhecidas como geo pricing e geo blocking”).

¹⁷ EUROPEAN DATA PROTECTION SUPERVISOR, *Artificial Intelligence, Robotics, Privacy and Data Protection*. Document for the 38th International Conference of Data Protection and Privacy Commissioners, Outubro de 2016. Disponível em: https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf

¹⁸ Ver o trabalho da FTC nessa área em: <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/consumer-privacy>



**COALIZÃO
DIREITOS NA
REDE**

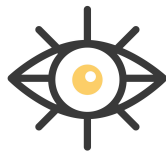
a proteção de dados pessoais possui - assim como a defesa do consumidor ou do meio ambiente - a característica de ser exercida por meio de instrumentos coletivos de tutela. Os danos, muitas vezes, são difusos e não mensuráveis individualmente. Não há como mensurar individualmente, por exemplo, o dano gerado por um teste de personalidade realizado em rede social, utilizado para finalidades indevidas, que possui impacto sobre o resultado de uma eleição em que determinado candidato tenha se aproveitado de características pessoais de usuários para direcionamento de propagandas políticas.

Trata-se, assim, de um dispositivo de defesa essencial para os usuários, considerando-se o contexto de desenvolvimento de novas tecnologias e da estratégia brasileira para a transformação digital que tem sido discutida e consolidada ao longo dos últimos anos. Ao prever mecanismos de tutela e uma Autoridade Nacional competente para fiscalização, a Lei traz segurança jurídica para o desenvolvimento de novos mercados no Brasil e adequa o país à níveis considerados adequados internacionalmente para cooperação econômica e transações que envolvam transferência e compartilhamento de dados.

Nesse sentido, a união Europeia determina que a transferência de dados pessoais para outros países apenas pode ocorrer quando eles possuírem salvaguardas apropriadas, que proporcionem remédios legais efetivos para a execução de direitos subjetivos dos usuários.¹⁹ A mesma necessidade de salvaguardas legais é também recomendada pela Organização para a Cooperação e Desenvolvimento Económico (OCDE). Em documento elaborado a pedido do governo brasileiro para uma revisão de seu Governo Digital, a OCDE inclusive reconhece a gestão de dados como um ativo estratégico para a digitalização do governo brasileiro e, ao mesmo tempo, a deficiência do Estado brasileiro na governança de dados. Defende expressamente a necessidade de um ambiente institucional bem definido, sendo essencial para isso a existência de uma lei geral de proteção de dados pessoais.²⁰ A Lei é capaz de gerar certezas institucionais, determinar melhores práticas de interoperabilidade de dados -

¹⁹ Assim dispõe o Art. 46 do Regulamento Geral de Proteção de Dados Europeu: “(...) a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.”,

²⁰ OCDE. *Revisão do governo Digital do Brasil: Rumo à Transformação Digital do Poder Público*. Projeto Governo digital, 2018, p. 20. Disponível em: <https://www.governodigital.gov.br/documentos-e-arquivos/digital-gov-review-brazil-portugues-pdf/view>



**COALIZÃO
DIREITOS NA
REDE**

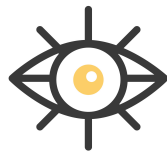
reconhecido como um dos gargalos na digitalização do governo - e define um novo ambiente de governança adequado para atender à necessidade de uma abordagem integrada da gestão dessa atividade.

4. Conclusões

Conforme exposto até aqui, recomenda-se que o Departamento de Proteção e Defesa do Consumidor (DPDC), da Secretaria Nacional do Consumidor, apoie a sanção do Projeto de Lei da Câmara 53/2018 (Lei Geral de Proteção de Dados Pessoais) em parecer ao Ministério da Justiça e Segurança Pública.

Dentre as razões a serem destacadas neste parecer, para além dos que já foram expostos até aqui, estão os seguintes:

- A Lei Geral de Dados Pessoais fortalecerá um sistema de cooperação e diálogo institucional entre Sistema Nacional de Defesa do Consumidor e a futura Autoridade Nacional de Proteção de Dados Pessoais;
- A Lei Geral de Dados Pessoais cria mecanismos de garantia de direitos, por parte dos consumidores e titulares de dados pessoais, que podem ser exercidos tanto perante a Autoridade Nacional de Proteção de Dados Pessoais quanto perante os órgãos do sistema brasileiro de defesa do consumidor;
- A legislação suprime lacunas existentes no sistema jurídico brasileiro, decorrentes da fragmentação das normas de proteção de dados pessoais em leis setoriais e da falta de harmonização conceitual em uma legislação unificada;
- A aprovação da legislação está de acordo com o sugerido pela Organização das Nações Unidas na mais recente resolução de proteção dos direitos dos consumidores, editada em 2016;
- A aprovação da legislação está de acordo com as recomendações da Organização para Cooperação e Desenvolvimento Econômico (OCDE), em especial com relação à garantia de um ambiente de confiança e segurança para as economias digitais, equilibrando a proteção dos direitos dos consumidores e dos direitos fundamentais



**COALIZÃO
DIREITOS NA
REDE**

com um ambiente jurídico propício aos investimentos e fortalecimento desses mercados no Brasil;

- A legislação tem o potencial de aprimorar a defesa dos consumidores no século XXI a partir da definição de conceitos mais precisos sobre “dados pessoais”, “dados sensíveis” e “dados anonimizados” e pelos novos direitos básicos assegurados no art. 8º e artigo 18, que passam a complementar o rol de direitos básicos assegurados no Código de Defesa do Consumidor.