



NOTA TÉCNICA

PL 3.443/2019

DISPÕE SOBRE A PRESTAÇÃO
DIGITAL DOS SERVIÇOS
PÚBLICOS NA ADMINISTRAÇÃO
PÚBLICA - GOVERNO DIGITAL



LAPIN

Realização:

Laboratório de Políticas Públicas e Internet (LAPIN)

Autoria:

Isabela Maria Rosal Santos (isabela@lapin.org.br)

José Renato Laranjeira de Pereira (joserenato@lapin.org.br)

Paulo Henrique Atta Sarmiento (paulo@lapin.org.br)

Thiago Guimarães Moraes (thiago@lapin.org.br)



Sobre esta nota técnica

A edição do **Projeto de Lei n. 3443/2019**, que propõe uma forma de regulação da Prestação Digital dos Serviços Públicos na Administração Pública (**Governo Digital**), se relaciona diretamente ao direito fundamental à privacidade e à proteção de dados pessoais, afetando o Estado Democrático Brasileiro.

A definição de conceitos de forma simplista e a falta de adequação ao sistema principiológico da arquitetura de proteção de dados pessoais são algumas das matérias que necessitam melhor reflexão, a fim de garantir adequada proteção à intimidade dos cidadãos brasileiros.

Com isso em vista, o Laboratório de Políticas Públicas e Internet - **LAPIN** editou esta nota técnica para apresentar suas considerações sobre o tema.

Quem somos nós

O **Laboratório de Políticas Públicas e Internet (LAPIN)** é um *think tank* com sede na capital federal brasileira, de composição multidisciplinar e cujo objetivo é apoiar o desenvolvimento de políticas públicas voltadas para a regulação das tecnologias digitais por meio da pesquisa e da conscientização da sociedade.

SUMÁRIO

I - Introdução	5
II - Das definições frágeis	6
III - Conformidade com a LGPD e o Marco Civil da Internet	9
IV - Cadastro Base do Cidadão	10
V - Conclusão	11

I - Introdução

O Projeto de Lei n. 3443/2019 dispõe sobre a Prestação Digital dos Serviços Públicos na Administração, o chamado "Governo Digital". A proposta pretende regulamentar o tratamento de dados pela Administração Pública, com destaque para sua interoperabilidade.

Não há dúvidas que uma regulação da Prestação Digital dos Serviços Públicos na Administração Pública seja assunto de extrema relevância para o país. Não obstante, exatamente essa importância exige análise cuidadosa antes da aprovação de uma legislação complexa que, **ao mesmo tempo que poderá trazer eficiência à máquina pública, corre o risco de trazer riscos à privacidade e à proteção de dados** dos cidadãos brasileiros se certas medidas e garantias não constarem no projeto de lei.

Por um lado, é louvável que o PL n. 3.443/2019 traga os seguintes alinhamentos com a pauta da proteção da privacidade e proteção de dados:

- A diretriz de adoção de **medidas de segurança, técnicas e administrativas que tornem os dados pessoais protegidos de acessos não autorizados** e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, desde a fase de concepção (*security by design*) - art. 3º, IV;
- A previsão das **definições de dados pessoais e dados pessoais sensíveis** em conformidade com a Lei 13.709/2019, a Lei Geral de Proteção de Dados (LGPD) - art. 4º, V e VI;
- A adoção de regras de boas práticas e governança, nos termos do art. 50 da LGPD - art. 4º, § 2º;
- A adoção das regras de atuação do setor público no âmbito da governança digital, nos ditos dos arts. 24 e 25 da Lei 12.965/2014, o Marco Civil da Internet (MCI) - art. 4º, § 3º.

Apesar dos esforços apresentados, como se verá a seguir, eles **não são suficientes para garantir a adequada proteção à privacidade e a proteção de dados** dos cidadãos, impactando o exercício de direitos previstos na Lei Geral de Proteção de Dados e do direito à autodeterminação informativa, incorporado ao

rol de direitos fundamentais pelo Supremo Tribunal Federal no julgamento da ADI 6387.

II - Das definições frágeis

O projeto de lei traz diversas definições em seu art. 4º, inclusive de tecnologias e técnicas. Contudo, pelo fato de envolverem ferramentas sofisticadas de computação, definir tecnologias como *blockchain* e inteligência artificial em uma lei poderá levar a uma série de dificuldades interpretativas que afetarão em muito sua aplicação, sem falar no fato de que tornará seus dispositivos rapidamente obsoletos.

Destaca-se, a esse respeito, a definição trazida para ***blockchain*** (art. 4º, X), como um "sistema que funciona como instrumento de registro em blocos, permitindo a transferência de informações criptografadas, **sem a existência de autoridade central de validação**"¹.

Ao contrário do que determina o texto legal, apesar de sistemas *blockchain* terem ficado famosos por sua descentralização no registro de transações de criptomoedas como o Bitcoin, existem hoje diferentes modelos da tecnologia, inclusive que possuem sim um ente centralizador responsável pela validação de operações. São as ***blockchains privadas***, usadas principalmente por empresas e governos ao redor do mundo, onde o elemento da confiança permite a centralização de decisões em um só ente dentro do sistema².

A confusão conceitual presente no Projeto de Lei também causa preocupação considerando que muito se tem discutido a respeito da funcionalidade de *blockchains* na efetividade do exercício do direito à proteção de dados. Michelle Finck, em relatório oficial elaborado para o Parlamento Europeu, chamou atenção para as barreiras existentes em *blockchains* para o exercício de direitos do titular de dados como acesso, correção e eliminação (art.

¹ A União Europeia, na [Declaração da Parceria Europeia sobre Blockchain](#), adotou definição genérica de *blockchain* visando principalmente possibilitar infraestrutura para o desenvolvimento da Administração Pública baseada em tecnologias de *blockchain*.

² BUTERIN, Vitalik. **On Public and Private Blockchains**. Ethereum Blog. Disponível em <<https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains>>. Acesso em 11 ago 2020.

18, Lei Geral de Proteção de Dados - LGPD), bem como a incompatibilidade com a minimização de dados e o princípio da finalidade (art. 6º, LGPD)³.

Na mesma linha, o projeto traz o conceito de **inteligência artificial** (art. 4º, XI), delimitado como "técnica que permite a uma máquina simular tarefas próprias ao raciocínio humano".

Ocorre que inteligência artificial é uma tecnologia extremamente complexa, cuja conceituação tem sido objeto de debate há décadas. Defini-la em apenas uma linha é um indicativo da falta de compreensão a respeito de seu funcionamento. A título de comparação, no contexto europeu, um grupo de especialistas foi formado para alcançar uma definição compreensiva do fenômeno. Em uma tradução não oficial, a definição para inteligência artificial trazida foi:

(...) sistemas de *software* (e possivelmente também *hardware*) projetados por seres humanos que, dado um objetivo complexo, agem na dimensão física ou digital, percebendo seu ambiente através da aquisição de dados, interpretando os dados estruturados ou não estruturados coletados, raciocínio no conhecimento ou no processamento das informações, derivados desses dados e na decisão das melhores ações a serem tomadas para alcançar o objetivo especificado. Os sistemas de IA podem usar regras simbólicas ou aprender um modelo numérico e também podem adaptar seu comportamento analisando como o ambiente é afetado por suas ações anteriores⁴.

Como se vê, trata-se de um conceito complexo, e **uma definição imprecisa poderá trazer problemas para a própria eficiência da gestão pública.**

Mesmo previsões positivas, como a determinação de se adotar **medidas de segurança, técnicas e administrativas** que tornem os dados pessoais protegidos

³ FINCK, Michelle. **Blockchain and the General Data Protection Regulation**. European Parliament. Jul 2018. Disponível em <https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU%282019%29634445>. Acesso em 11 ago 2020.

⁴ Tradução livre. European Commission: **A definition of Artificial Intelligence: main capabilities and scientific disciplines**, 8 abr 2019. Disponível em <<https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>>. Acesso em 11 ago 2020.

de acessos não autorizados e de situações acidentais ou ilícitas, desde a fase de concepção (*security by design*) são esvaziadas, porque não há previsões para garantir a privacidade de cidadãos desde a fase de concepção do produto ou serviço (***privacy by design***), apesar de mencionar o desenvolvimento de aplicativos para a avaliação continuada das políticas públicas (arts. 2º, IV e 4º, §3º).

Vale dizer que, no entanto, existe uma contradição aos princípios de *privacy by design* e *security by design* na previsão do art. 6º, III, que estipula que os dados "que não estejam sob sigilo ou sob restrição de acesso nos termos da Lei nº 12.527, de 18 de novembro de 2011, serão disponibilizados, obrigatoriamente, em formato aberto e estruturado, amplamente acessível e utilizável por pessoas e máquinas assegurados os direitos à segurança e à privacidade". **Ao colocar a disponibilização como regra, os mencionados princípios *security* e *privacy by design* são entendidos como exceção, o que fere ainda outros princípios da LGPD, como a adequação e a finalidade.**

Deve-se também avaliar que definições precisas, como a de **dado pessoal** (art. 4º, V) e a de **dado pessoal sensível** (art. 4º, VI), não são utilizadas ao decorrer do texto do projeto de lei. Em movimento contrário à previsão de significados para os termos, o texto utiliza o conceito de **dados cadastrais** (art. 30, V e VI), que tem causado confusão em diferentes momentos por serem erroneamente categorizados como dados que não seriam pessoais. Isso geraria o risco de causar uma dissonância com as proteções necessárias previstas em legislações conexas, como a LGPD.

Ao fazer uso dessa miríade de definições que terminam esquecidas em meio aos outros dispositivos, o PL n. 3443/2019 acaba por criar uma arquitetura complexa em que diferentes técnicas não dialogam entre si, em uma colcha de retalhos normativa que afeta o desenvolvimento de um sistema de interoperabilidade de dados suficientemente protetivo à privacidade. Isso abre espaço para discutirmos sua relação tanto com a LGPD quanto com outro dispositivo de suma importância para regulação do ambiente digital no Brasil: o Marco Civil da Internet (MCI).

III - Conformidade com a LGPD e o Marco Civil da Internet

Em uma rápida análise, é louvável que o PL n. 3.443/2019 se alinhe com a pauta da proteção da privacidade e proteção de dados. A mencionada previsão das definições de dados pessoais e dados pessoais sensíveis está em conformidade com os critérios adotados pela LGPD. A atenção para o disposto na norma geral de proteção de dados também é evidenciada na previsão do art. 4º, §2º, do PL n. 3.443/2019, ao mostrar a necessidade de adotar regras de boas práticas e governança referidas no art. 50 da LGPD.

Entretanto, não há previsões para garantir a conformidade com diferentes previsões da LGPD, em especial aos **direitos dos titulares de dados** (arts. 17 a 22 da LGPD) e às regras quanto ao **tratamento de dados pessoais pelo poder público** (arts. 23 a 30 da LGPD).

Outro ponto omissivo do projeto diz respeito às especificações sobre o alinhamento do compartilhamento de dados entre órgãos do governo com os princípios da LGPD, como **adequação e transparência** (art. 6º, II e VI, LGPD). A alusão a esses princípios deveria ser explícita.

Por outro lado, também é notável a preocupação do PL n. 3443/2019 de adequar-se ao Marco Civil da Internet (MCI). O §3º do art. 4º do Projeto de Lei define expressamente que deverão ser adotadas as regras de atuação do setor público no âmbito da governança digital, conforme as previsões dos arts. 24 e 25 do MCI, que preveem um mecanismo de “governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica” (art. 24, I, MCI).

No entanto, o Projeto entra em contradição com esse direcionamento ao definir que as medidas de **fiscalização e controle do cumprimento do PL** seriam tomadas exclusivamente por órgãos estatais, **sem a participação da sociedade civil**, conforme seu art. 11. Essa centralização da atuação no Estado vai de encontro com a tradição participativa que prevê a atuação multissetorial em assuntos relacionados à internet, como ocorre desde as discussões sobre o MCI e que prosseguiu com a LGPD.

Isso mostra como ainda é necessário o aperfeiçoamento do Projeto de Lei para garantir sua compatibilização com direitos previstos no ordenamento jurídico brasileiro como a privacidade e a proteção de dados.

IV - Cadastro Base do Cidadão

O PL n. 3443/2019, em seu art. 2º, II, menciona como finalidade do Governo Digital disponibilizar, em **plataforma única e centralizada**, o acesso às informações e aos dados públicos. Apresenta, então, em seu art. 30, a previsão ambiciosa do **Cadastro Base do Cidadão**, que centralizaria todos os dados públicos em uma única base.

Essa centralização deve ser tratada com cautela - um único ponto de acesso também significa um único ponto de falha. Grupos mal-intencionados que pretendam realizar ataques de segurança poderão focar seus esforços em um único lugar para direcionar suas ações ilegais e ter acesso a todos os dados governamentais, **comprometendo os pilares CIDA** (Confidencialidade, Integridade, Disponibilidade, Autenticidade) da Segurança da Informação⁵.

Além disso, **nenhuma das disposições presentes no art. 30 prevê regras para garantir conformidade à LGPD**, em especial aos direitos dos titulares de dados (arts. 17 a 22, LGPD) e às regras quanto ao tratamento de dados pessoais pelo poder público (arts. 23 a 30, LGPD). Ademais, não é descrito como o compartilhamento de dados entre órgãos do governo se alinham a princípios da LGPD, como adequação e transparência (art. 6º, II e VI, LGPD) **Referência a esses dispositivos deveria ser explícita.**

Esses incidentes de segurança poderão **expor dados pessoais de milhares de cidadãos brasileiros**, o que, além de comprometer a privacidade desses indivíduos, afetará a prestação de serviços públicos e a imagem internacional do Estado brasileiro.

⁵ ABNT NBR ISO/IEC 27002:2013.

V - Conclusão

Dado o exposto, o LAPIN **recomenda que não se dê prosseguimento à deliberação do PL n. 3.443/2019 antes que os pontos aqui expostos sejam superados**. Apenas com insumos técnicos adequados, o Estado poderá ser capaz de promover eficiência pública ao mesmo tempo em que respeita os direitos e garantias fundamentais de seus cidadãos.