Retirada de pauta do PL do Governo Digital (PL 3.443/2019) da Sessão Plenária de 05/11/2019[1]

E Solicitação de Audiência Pública para melhor debater os temas deste Projeto de Lei

O Laboratório de Políticas Públicas e Internet da Universidade de Brasília, LAPIN/UnB, mediante a presente **NOTA TÉCNICA**, requer a **retirada de pauta do PL 3.443/2019 da sessão deliberativa Plenária de 05/11/2019 e solicita que uma ou mais audiências públicas sejam realizadas** antes de aprovação do projeto de lei, pelos motivos doravante expostos.

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

Em uma rápida análise, é louvável que o PL 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.

Muito embora os esforços apresentados, eles **NÃO SÃO SUFICIENTES** para garantir a adequada proteção à privacidade e proteção de dados. Há **inúmeros pontos críticos** no PL 3.443/2019, que necessitam de melhor reflexão. Em uma **lista não exaustiva**, destacamos:

---

[1] Autores: José Renato Laranjeira de Pereira (josedepereira@hotmail.com) e Thiago Moraes (moraest@protonmail.com).

1. Embora as diretrizes do art. 3º prevejam o *security by design*, **nenhum dos dispositivos prevê** esforços na adoção de medidas técnicas e organizacionais para garantir a proteção da privacidade de cidadãos desde a fase de concepção do produto ou serviço, o ***privacy by design***;
2. Embora as **definições de dados pessoais e dados pessoais sensíveis** existam, elas **raramente são utilizadas** no decorrer do texto do projeto de lei. Ao contrário, o texto usa um termo não definido, *dados cadastrais*, que traz o risco de causar uma dissonância com as proteções necessárias previstas em legislações conexas, como a LGPD;
3. Algumas **definições precisam ser melhor elaboradas**. Como exemplo, citamos **inteligência artificia**l (art. 6º, XI), uma tecnologia consideravelmente complexa para ter sido resumida apenas como uma "técnica que permite a uma máquina simular tarefas próprias ao raciocínio humano".[2] Uma **definição imprecisa poderá trazer problemas para a própria eficiência da gestão pública**, caso incorpore sistemas falhos que se apresentem como inteligência artificial.
4. O **art. 6º, III,** traz uma previsão preocupante, ao afirmar 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". O texto é **extremamente vago** e cria uma **postura avessa a princípios como *security by design* e *privacy by design***, ao colocá-los como exceção e não como regra. Além disso, colide com outros princípios da LGPD, como o da **adequação** (art. 6º, II), que determina que o tratamento de dados deve ser compatível com as finalidades informadas ao titular no momento de sua coleta;
5. Apesar de o art. 11 apresentar a louvável iniciativa de prever a **fiscalização e o controle do cumprimento do PL**, tais medidas seriam feitas pelo próprio aparato estatal brasileiro, sem a participação da sociedade civil, principal interessada no processo de tratamento de dados pessoais. Tal previsão vai de encontro com a tradição de

[2] A título de comparação, no contexto europeu, um grupo de especialistas foi formado para chegar a uma definição compreensiva do fenômeno. Em uma tradução não oficial, a definição para inteligência artificial trazida foi: "*"Sistemas de inteligência artificial (IA) são sistemas de software (e possivelmente também hardware) projetados por seres humanos que, dados 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 anteriores.*"

transparência que prevê a participação popular em assuntos relacionados à internet e à proteção de dados, como ocorreu tanto no MCI quanto na própria LGPD;

6. O art. 30 é bastante **ambicioso** ao propor a instituição de um **Cadastro Base do Cidadão**, que centralize todos os dados públicos em uma única base. Como se pode imaginar, tal projeto deve ser realizado com extremo cuidado: um ponto único de acesso também significa **um ponto único 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 Informação**.[3] Esses incidentes de segurança poderão expor dados pessoais de milhares de cidadãos brasileiros, o que, **além de comprometer a privacidade desses indivíduos, afetará a imagem internacional do serviço público brasileiro;**
7. Ainda sobre o art. 30, **nenhum dos dispositivos prevê regras para garantir a conformidade à 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). Ademais, não é descrito como o compartilhamento de dados entre órgãos do governo se alinham a princípios da LGPD, como **adequação (art. 6º, II)** e **transparência** (art. 6º, VI) Referência a esses dispositivos **deveria ser explícita**.

Dado o exposto, o LAPIN requer a **retirada imediata do PL 3.443/2019 da sessão deliberativa Plenária de 05/11/2019** e **solicita que uma ou mais audiências públicas sejam realizadas** para melhor debater os temas ora expostos. 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.

[3] ABNT NBR ISO/IEC 27002:2013.