DataPrivacyBR Research

Contribuição à Audiência Pública nº 01/2023-CNM/CGPI/DPSP/SENASP/MJSP

Sobre a Data Privacy Brasil

A Data Privacy Brasil é uma organização que nasce da união entre uma escola e uma associação civil em prol da promoção da cultura de proteção de dados e direitos digitais no Brasil e no mundo. Para isso, com o apoio de uma equipe multidisciplinar, realizamos formações, eventos, certificações, consultorias, conteúdos multimídia, pesquisas de interesse público e auditorias cívicas para promoção de direitos em uma sociedade datificada marcada por assimetrias e injustiças. Por meio da educação, da sensibilização e da mobilização da sociedade, almejamos criar um ambiente digital mais seguro, justo e ético para todos.

Dentre outros trabalhos, já participamos como amicus curiae em dois julgamentos do STF, o da ADI 6387 e da ADI 6649 em conjunto com a ADPF 695, ambos com impactos significativos para o reconhecimento da proteção de dados e que guiam o uso de dados pelo poder público.

Como organização comprometida com direitos humanos e novas tecnologias, temos nos debruçado sobre o tema da segurança pública desde 2020, com o projeto Novas Fronteiras dos Direitos Digitais, contribuindo com uma nota técnica sobre o anteprojeto de lei da LGPD Penal e artigo em publicação do CNJ sobre reconhecimento de pessoas. Atualmente estamos realizando pesquisa empírica sobre parâmetros jurídicos de usos secundários de dados pessoais em câmeras corporais, motivo pelo qual apontamos aqui nossas preocupações sobre o tema.

Proteção de dados pessoais e segurança pública

A implementação de medidas de segurança pública sempre implica impactos aos direitos e liberdades fundamentais. Parte deste impacto é gerado pelo tratamento de dados pessoais feito pelas polícias e um erro neste processo pode prejudicar severamente a vida de um cidadão. Dada a gravidade e sensibilidade do processo desenvolvido pelas polícias que se faz necessária a proteção de dados pessoais desde o momento de concepção da medida. E embora ainda não exista uma lei de proteção de dados específica para a segurança pública, **a Lei Geral de Proteção de Dados (LGPD) traz parâmetros aplicáveis a este contexto na ausência de lei (art. 4º, §1º, da LGPD)**.

No que tange a proteção de dados, independente do contexto, deve-se considerar os seus princípios (art. 7º, da LGPD), são eles: (i) **finalidade, correspondente ao propósito legítimo do tratamento de dados pessoais**; (ii) adequação, referente a necessidade de se identificar se o meio para o tratamento é efetivo para alcance da finalidade; (iii) **necessidade, que trata da limitação aos dados estritamente necessários para o tratamento**; (iv) livre acesso, que é a consulta por parte do indivíduo sobre a forma e duração do tratamento, bem como sobre a integralidade de seus dados; (v) **qualidade dos dados: manutenção de dados claros, precisos e atualizados**; (vi) **transparência, isto é, informações claras e precisas sobre o tratamento e seus agentes de tratamento**; (vii) **segurança, aplicação de medidas técnicas e administrativas aptas a proteger os dados de acessos indevidos, bem como perdas ou alteração**; (viii) **prevenção: adoção de medidas para evitar dano resultante do tratamento de dados**; (ix) **não discriminação, o tratamento não pode ter fins discriminatórios ilícitos ou abusivos**; e (x) responsabilização e prestação de contas.

Proteção de dados como vetor para garantia da cadeia de custódia

Todos os princípios trazidos no item anterior são cabíveis ao cenário da segurança pública, e permitem garantir a eficiência de tratamento de dados pessoais. Ao se questionar sobre a finalidade e os meios adequados de atingi-la, bem como a implementação de medidas protetivas e de transparência, preserva-se a integridade da cadeia de custódia. Sem dados verdadeiramente necessários e úteis, e sem um processo lícito de

obtenção destes dados, a evidência é fragilizada e prejudica a cadeia de custódia. Ou seja, **desde o desenvolvimento da medida e dos equipamentos a serem utilizados, a proteção de dados precisa ser mobilizada**.

Apontamentos na nota técnica

Indicamos abaixo alguns comentários aos itens da nota técnica, com sugestões de melhorias no texto para garantia do direito fundamental à proteção de dados pessoais.

Item	Texto original	Comentários	Sugestão de texto
4.	[sem correspondência]	Na medida em que os metadados são informações contextuais a respeito de determinado documento digital e seus usos, é preciso limitar seu acesso àqueles estritamente necessários. A definição do conceito auxilia nesse processo, devendo haver previsão expressa na nota técnica	4.x Metadados: dados e registros gerados pelo sistema em que se faz o registro de um arquivo, informação ou comunicação e que não constituam o seu conteúdo em si, mas sejam capazes de garantir autenticidade e contexto ao documento eletrônico
4.	[sem correspondência]	O item 6.1.45 utiliza o termo "operador", podendo causar dúvidas sobre seu conceito. É necessário esclarecer quem é o operador e quem é o usuário para fins deste protocolo,	4.x: Operador: agente que efetivamente veste a câmera corporal 4.x: Usuário: quem acessa o sistema da câmera, de gestão das filmagens.

		uma vez que os termos podem não ficar evidentes. Isso é especialmente relevante na dogmática de proteção de dados pessoais, já que operador é uma "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII, LGPD)	
6.1.40	Todos os usuários devem ser obrigados a fazer login no sistema de gestão usando uma senha segura, a fim de minimizar a possibilidade de usuários não autorizados acessarem informações confidenciais ou sensíveis e, quando houver a integração com outros sistemas, é recomendável a implementação a autenticação por single sign-on.	É fundamental haver previsão de *logs* auditáveis para fins de responsabilização em casos de acessos indevidos, assim como potenciais edições ou exclusões de arquivos nos sistemas, tanto nas câmeras corporais quanto nos sistemas de gestão dos dados (*softwares*)	Acréscimo ao texto original: "Os sistemas de gestão de dados devem ser capazes de promover auditorias de eventos de logon, indicando se houve êxito no logon, tentativa falha e processos de logoff, garantindo maior aderência a políticas de privacidade e segurança da informação"
6.2.5	Liberação das câmeras das dock stations através de reconhecimento facial	Ainda que uma funcionalidade opcional, a escolha pelo uso de reconhecimento facial envolve dados biométricos, considerados dados	Acréscimo ao texto original: "Havendo escolha pela funcionalidade com reconhecimento facial, o órgão deverá produzir Relatório de Impacto à

		pessoais sensíveis nos termos na LGPD (art. 5º, II, LGPD). Isso exige uma série de procedimentos de segurança da informação, além de um Relatório de Impacto à Proteção de Dados Pessoais (art. 5º, XVII, LGPD), implicando em custo maior para os órgãos contratantes	Proteção de Dados Pessoais (art. 5º, XVII, LGPD) de modo a preservar garantias e direitos de titulares de dados”