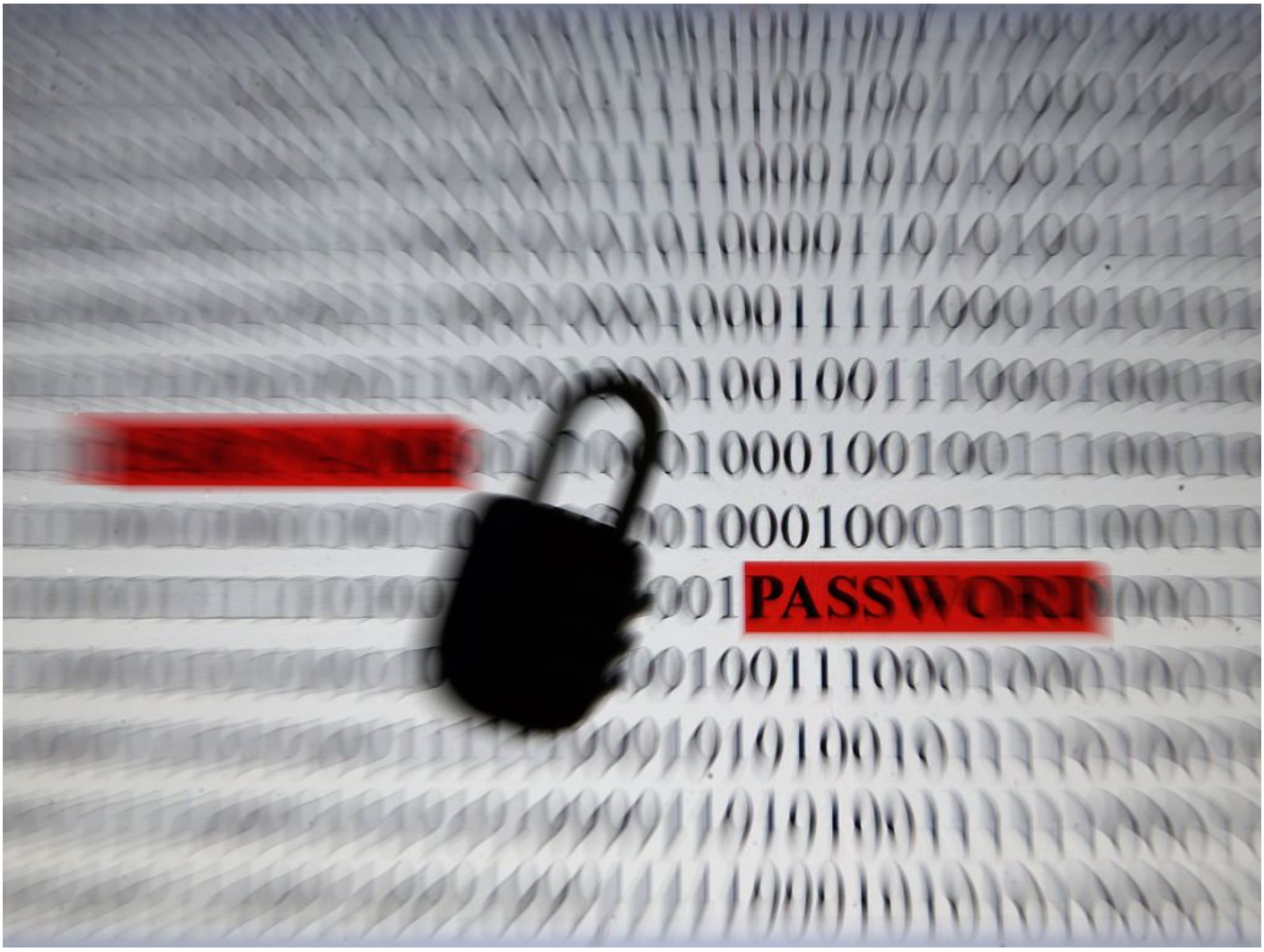
MÚLTIPLAS VOZES

Desafios da Proteção de Dados Pessoais no Brasil

LGPD é um avanço para a sociedade brasileira, mas o uso de dados para subsidiar políticas públicas exige responsabilidade e necessita de legislação específica para a segurança pública

João Araújo Monteiro Neto e Vasco Furtado
15 de setembro de 2020

MARCELLO CASAL JR/AGÊNCIA BRASIL



O uso de dados pessoais, como movimentações financeiras, no combate ao crime organizado, por exemplo, é um elemento-chave para o sucesso das investigações.

A gestão pública baseada em evidências advindas de dados digitalizados tem se tornado uma boa prática de governos (van Ooijen et. al., 2019; van Veenstra et.al, 2017). Exemplos disso podem ser encontrados nas mais diversas áreas como no planejamento do transporte público, acompanhamento epidemiológico e mapeamento da criminalidade. Sistemas de monitoramento por vídeo câmeras, ferramentas analíticas e preditivas a partir de grandes volumes de dados (Big Data) e métodos de Inteligência Artificial são exemplos de como a tecnologia e o uso de dados podem contribuir para as atividades de segurança pública.

A despeito dessa perspectiva promissora, o uso de dados para subsidiar políticas públicas requer responsabilidades, em especial, no que se refere ao uso de dados pessoais. A recente promulgada Lei Geral de Proteção de Dados Pessoais – LGPD e de suas congêneres no mundo (e.g. a lei europeia - GDPR) foi um avanço das sociedades democráticas nesse sentido. Visa-se estabelecer

obrigações a serem seguidas por instituições públicas e privadas sobre como dados pessoais podem ser utilizados sem colocar em risco desproporcional, ou causar prejuízos a privacidade das pessoas.

O princípio fundamental que norteia esse tipo de legislação é de que dados pessoais sejam usados somente de maneira legítima, segura e específica a uma finalidade previamente acordada com o cidadão. Esse importante avanço para a proteção dos dados e da privacidade das pessoas requer um capítulo à parte em se tratando de segurança pública. Na LGPD brasileira é reconhecida a importância do uso de dados em atividades de manutenção da lei e da ordem, mas o parlamento brasileiro reconheceu igualmente que é fundamental que se discutam as especificidades desse cenário.

O próprio princípio básico da compactuação com o cidadão sobre o objetivo para o qual seus dados pessoais serão usados não se aplica plenamente a situações de manutenção da lei, visto que isso poderia se tornar um instrumento que protegeria autores de crimes. O uso de dados pessoais, como movimentações financeiras, no combate ao crime organizado, por exemplo, é um elemento-chave para o sucesso das investigações.

Entretanto, a má gestão ou utilização dos dados pessoais de forma indiscriminada podem gerar também riscos graves ao exercício de direitos e garantias fundamentais que funcionam como elementos estruturais da vida em uma sociedade democrática. A falta de regulamentação pode ocasionar situações de abuso como a criação indiscriminada de dossiês secretos sobre cidadãos, o uso de imagens de câmeras de segurança para usos indevidos (G1, 2018), ou até mesmo a criação de um sistema de super vigilância em massa que monitore o cidadão em cada uma de suas atividades.

A tecnologia já permite que, através de reconhecimento de dados biométricos, um rastreamento do cidadão seja feito toda vez que ele utilize um serviço público como um posto de saúde ou acesse um espaço público como um estádio de futebol. Em que situações, sob que pretextos, a partir de qual autorização, poderão as forças de segurança acessar esses dados individualizados? Os limites entre o uso dos dados pessoais em benefício da sociedade e de um estado de vigilância em massa danoso às relações sociais precisam ser claramente estabelecidos e evidenciam a necessidade de que a extensão da LGPD para Segurança seja prioridade.

Dentre os desafios enfrentados na construção dessa lei podem-se destacar dois grandes pontos: o aspecto ético necessário a balancear o acesso aos dados e a proteção dos direitos dos cidadãos; e a necessidade de estruturar um mecanismo de governança capaz de garantir o uso legal, seguro, transparente e responsável desses dados. Nesse contexto, a institucionalização de uma Autoridade Nacional de Proteção de Dados dotada de autonomia, independência, transparência, capacidade técnica e um modelo de operação multisetorial, nos moldes do aplicado ao Comitê Gestor da Internet no Brasil (CGI.br), é um elemento crucial na busca de se garantir a utilização adequada de dados pessoais nas atividades de segurança pública.

Do ponto de vista ético, a nova legislação deve estabelecer de forma muito clara, não somente em que situações estão as forças de segurança autorizadas à tratar os dados pessoais, mas também indicar quais princípios devem orientar o tratamento desses dados. Nesse processo deve-se levar em conta os valores e princípios já estabelecidos tanto na LGPD, como em práticas legais aplicadas em outros países. Exemplos no mundo podem apoiar os legisladores. A Lei de Proteção de Dados do Reino Unido (Data Protection Act - 2018), no seu capítulo destinado ao uso de dados em atividades de segurança, estabelece seis princípios que devem orientar as atividades de segurança destacando-se a exigência de que o uso seja legal e justo, que os dados sejam adequados, relevantes e não excessivos e os dados pessoais sejam mantidos por um período não superior ao necessário. Ressalte-se que esses princípios guardam perfeita simetria com as regras gerais aplicadas à proteção de dados pessoais estabelecidas pela General Data Protection Regulation – GDPR na Europa como um todo.

O segundo desafio diz respeito à governança dos dados pessoais utilizados em atividades de segurança pública. As boas práticas internacionais sugerem a operação de uma estrutura de fiscalização capaz de garantir aspectos mínimos de segurança, transparência e responsabilização. É indispensável que os dados utilizados sejam protegidos de forma adequada e que sua confidencialidade, integridade e disponibilidade sejam garantidas. Veja por exemplo o que aconteceu no Equador, onde uma organização criminosa *hackeou* os dados de toda a população do país (EBC, 2019).

Por fim, deve-se possuir mecanismos, seja uma corte especial como nos EUA [1], ou uma autoridade autônoma, como na Europa [2], que fiscalizem o uso de dados pessoais em atividades de segurança que garantam níveis mínimos de transparência, respeitando-se o sigilo inerente as essas atividades, e a responsabilização dos agentes que violem os princípios e as regras legais a elas aplicadas. A estruturação desse mecanismo apresenta-se como um dos maiores desafios do processo de regulamentação do uso de dados pessoais no campo da segurança pública, mas é também, se observarmos o debate internacional que ocorre na área do uso de dados em atividades de inteligência (UNSRP, 2019; CCDCOE, 2019) o que possui maior impacto na legalidade e legitimidade dessas atividades (Wetzling et. al., 2019).

Assim, compreendendo a importância do uso de dados na segurança pública e a necessidade de proteção dos direitos e garantias do cidadão, entende-se prioritário e necessário o debate para criação de uma lei específica, que observe as melhores práticas internacionais e que inclua em seu processo de elaboração representantes dos mais variados setores da sociedade. Ela tem que ser capaz de estabelecer de forma clara balizas éticas e de governança capazes de garantir o uso legal, legítimo, seguro e responsável de dados pessoais em atividades de segurança pública.

João Araújo Monteiro Neto
Doutor em Direito pela Universidade de Kent, no Reino Unido, e professor do Curso de Direito do Centro de Ciências Jurídicas da Universidade de Fortaleza

Vasco Furtado
Professor e Diretor de Pesquisa e Inovação da Universidade de Fortaleza, e associado do Fórum Brasileiro de Segurança Pública

[1] Apesar da enorme crítica da sociedade civil e da academia que questionam os processos secretos e a falta de transparência de seu funcionamento, os EUA possuem uma Corte especial destinada a autorizar atividade de vigilância para ns de inteligência. A Corte FISA atua nos pedidos de vigilância fundamentos no The Foreign Intelligence Surveillance Act.

[2] Na Europa o papel de scalização do uso de dados pessoais compete as Autoridades Nacionais de Proteção de Dados Pessoais, como por exemplo a Agência Espanhola de Proteção de Dados Pessoais. No contexto mais amplo o European Data Protection Board emite orientações gerais destinadas a orientar as autoridades nacionais no cumprimento das GDPR
