Sorria: o Estado brasileiro está de olho em você

A urgência de se assegurar uma política efetiva de proteção de dados por parte do Poder Público

---

Ana Frazão

Advogada. Professora de Direito Civil e Comercial da UnB. Ex-Conselheira do CADE.

Como se sabe, não são apenas as empresas e os agentes econômicos que colocam em risco a privacidade e os dados pessoais dos cidadãos. O Estado é também uma poderosa ameaça, sendo a história repleta de exemplos de como o acesso irrestrito e ilimitado a dados dos cidadãos pode se tornar uma vigorosa ferramenta de vigilância estatal, inclusive para efeitos da consolidação de regimes autoritários.

É por essa razão que a Lei Geral de Proteção de Dados - LGPD, acertadamente, tem o Poder Público como um dos principais destinatários de seus deveres, dedicando o Capítulo 4 especificamente para tratar do assunto. Entretanto, assegurar a eficácia do regime protetivo de dados perante o Estado não é simples, até diante do natural *tradeoff* entre proteção de dados, de um lado, e interesses públicos relevantes, como a segurança pública e a defesa nacional, de outro.

A própria LGPD, em seu art. 4º, III, excetua da sua aplicação os tratamentos de dados realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Ocorre que essa imunidade pode ser bastante perigosa, pois vários tratamentos de dados extremamente invasivos podem ser justificáveis a partir do "guarda-chuva" do art. 4º, III, da LGPD. Antecipando tais dificuldades, o §

1º, do art. 4º, da LGPD, prevê que "O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei."

Não é sem razão que, no tocante às questões penais, atualmente se encontra em discussão a chamada LGPD Penal, a fim de se buscar um equilíbrio entre a segurança pública e a persecução penal com a necessária proteção de dados.

Não obstante, questões de inteligência e outras afetas à segurança nacional e defesa do Estado continuam sendo exceções à aplicação do regime protetivo da LGPD, até porque, pelo que se sabe, foram expressamente excluídas do Anteprojeto da LGPD Penal, cujo art. 4º prevê que "Esta lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de defesa nacional e segurança do Estado."

Dessa maneira, assuntos vinculados à defesa nacional e à segurança do Estado parecem continuar sem qualquer limitação mais clara e, a depender da extensão com que tais exceções forem interpretadas, podem representar considerável amesquinhamento das garantias dos titulares de dados.

Com efeito, segurança nacional e proteção de dados seguem lógicas totalmente distintas, uma vez que a primeira requer sigilo e a segunda transparência e privacidade. Daí por que é realmente complicado encontrar um equilíbrio entre esses dois objetivos, ainda mais diante de um governo que utiliza a ideia de segurança nacional com considerável amplitude, sendo exemplos as constantes e indevidas tentativas de utilização da controversa Lei de Segurança Nacional. Aliás, não é demais lembrar que tramitam hoje no STF várias ADPFs contra a referida lei, o que foi provocado por inúmeros episódios recentes em a lei foi invocada para restringir a liberdade de expressão de cidadãos ou mesmo para justificar prisões arbitrárias.

Soma-se a isso a sanha investigatória do governo, revelada em várias iniciativas incompatíveis com o regime democrático, como a questão dos

dossiês antifascistas produzidos no âmbito do Ministério da Justiça. Tal circunstância, em razão da gravidade, justificou que o Supremo Tribunal Federal tivesse que dizer o óbvio: relatórios de inteligência não podem ser feitos para bisbilhotar dados sensíveis, como preferências ideológicas, de servidores e professores universitários[1].

Tais questões são ora mencionadas para contextualizar o problema e mostrar que, enquanto não houver o devido equacionamento do conflito entre segurança nacional e proteção de dados, os cidadãos brasileiros estão em situação de considerável vulnerabilidade, o que se reforça com o descaso do Estado em relação à LGPD e uma série de outras iniciativas que vão de encontro aos objetivos de um regime de proteção de dados.

Para chegar a tal conclusão, nem precisamos mencionar todos os obstáculos que foram arquitetados para impedir ou adiar a vigência da LGPD, ainda que ao elevado preço da insegurança causada à sociedade e ao mercado. Também não precisamos mencionar a demora na criação da ANPD e o fato de a autoridade ter sido arquitetada como um "braço" da Presidência da República.

Esses pontos são bastante preocupantes porque mostram o pouco entusiasmo do Estado brasileiro com a criação de um ambiente institucional propício para a efetividade da LGPD. A lei entrou em vigor sem que tivesse sido estruturada a autoridade nacional e sem que houvesse arcabouço regulatório mínimo – já que aspectos cruciais da LGPD precisam da regulamentação da ANPD – que possibilitasse aos agentes de tratamento a ciência dos critérios e parâmetros básicos a serem observados para a obediência a vários dos deveres ali previstos.

Todo esse atropelo tem consequências importantes para o cumprimento de uma lei cuja eficácia não pode mais depender exclusivamente do modelo comando-controle por parte do Estado, mas deve contar com o convencimento e com as iniciativas voluntárias dos agentes de tratamento para tal objetivo. Ocorre que o *compliance* e as boas práticas de governança, por parte de agentes privados, dificilmente podem florescer no vazio institucional;

---

1 ADPF 722 MC, Relator(a): CÁRMEN LÚCIA, Tribunal Pleno, julgado em 20/08/2020, PROCESSO ELETRÔNICO DJe-255 DIVULG 21-10-2020 PUBLIC 22-10-2020.

pelo contrário, requerem as devidas sinalizações e incentivos por parte do Estado para que possam se tornar efetivos.

Não obstante, os problemas não param por aí. Se queremos falar da falta de cuidado do Poder Público com a proteção de dados pessoais, podemos mencionar os episódios recentes de vazamento de dados de vários órgãos públicos, dentre os quais o Ministério da Saúde, o que possibilitou o acesso indevido de dados sensíveis de milhões de brasileiros, incluindo altas figuras da República.

Como foi noticiado na imprensa, no caso específico do Ministério da Saúde, os dados foram vazados em razão de falhas de segurança banais, que podiam ter sido perfeitamente evitadas se tivesse havido um mínimo de cuidado por parte das autoridades envolvidas. Causou perplexidade também a reação das autoridades diante do vazamento pois, longe de haver qualquer plano de segurança para resolver os problemas com rapidez e mitigar os danos, o que se viu foi uma reação desorientada, incapaz de fazer frente ao problema ocorrido e ainda marcada pela falta de transparência sobre o que é feito para prevenir incidentes de segurança e o que é feito para remediá-los a tempo e modo.

Porém, não são apenas omissões e descuidos que vêm caracterizando a postura do Estado brasileiro a respeito dos dados de seus cidadãos. O mesmo Poder Público que não tem se esforçado para cumprir a LGPD e proteger os dados dos cidadãos brasileiros é o mesmo que vem avançando em iniciativas que são diametralmente opostas e representam ataques frontais aos direitos dos titulares de dados pessoais.

Nesse sentido, pode ser citada a utilização já disseminada de inteligência artificial pelo Estado para os mais diversos fins. Relatório do Transparência Brasil[2] mostra número considerável de ferramentas de inteligência artificial já em uso, inclusive para auxílio na tomada de decisões administrativas, mas sem observância dos devidos cuidados.

Outro exemplo de tentativa de violação dos direitos dos titulares de dados pessoais foi a Medida Provisória 954/2020, que pretendia autorizar o

---

2 https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_IA_PoderPublico.pdf

compartilhamento de dados pessoais das operadoras de telefonia com o IBGE. A iniciativa só não foi mais desastrosa porque foi devidamente contida pelo Supremo Tribunal Federal, em julgamento paradigmático no qual se reconheceu o direito fundamental autônomo à proteção de dados[3]. No julgamento, ficou muito claro que a Medida Provisória não atendia minimamente ao dever de definir apropriadamente como e para que os dados seriam utilizados nem as devidas salvaguardas para a proteção desses dados.

Com efeito, além de diversas violações aos princípios estruturantes da proteção de dados, o STF foi categórico também ao apontar que a Medida Provisória não apresentava mecanismo técnico ou administrativo apto a proteger os dados compartilhados de acessos não autorizados, de vazamentos acidentais ou de utilização indevida, seja na transmissão, seja no tratamento, razão pela qual descumpria as exigências constitucionais para a efetiva proteção dos direitos fundamentais dos brasileiros.

Igualmente não se pode esquecer do preocupante Decreto 10.046/2019, que prevê o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados, o que possibilita a reunião de um número imenso de dados, incluindo dados biográficos, biométricos e mesmo genéticos dos cidadãos, sob a alegação genérica de racionalização e eficiência da gestão pública.

O que mais impressiona nesse tipo de iniciativa estatal, além da violação a inúmeros pontos da LGPD – dentre os quais os princípios da finalidade, da necessidade e da minimicidade -, é o fato de o governo nem mesmo sopesar os riscos de um tratamento de dados com tal extensão, não se preocupando em apresentar para a sociedade uma política de proteção de dados minimamente clara.

Felizmente a OAB já ingressou com ação direta de inconstitucionalidade - a ADI 6649 - apontando as inúmeras inconstitucionalidades do decreto, inclusive do ponto de vista formal. Na petição inicial, a OAB reconhece a possibilidade de legítimo compartilhamento de dados para a execução de políticas públicas, mas ressalta ser imprescindível a

3 ADI 6387 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO DJe-270 DIVULG 11-11-2020 PUBLIC 12-11-2020.

adoção de medidas e procedimentos para salvaguardar os direitos e liberdades fundamentais dos titulares dos dados.

Não bastasse o quadro descrito, suficientemente preocupante, por mostrar uma estratégia de governo invasiva e despreocupada com a proteção dos dados pessoais dos cidadãos brasileiros, recentemente circulou na imprensa a existência de licitação, encabeçada pela União e pelo Ministério da Justiça (Pregão 003/2021), para adquirir aparelho Pegasus[4]. Trata-se de poderosa ferramenta de investigação da empresa israelense NOS Group, pois pode invadir telefones celulares à distância sem que seja rastreado o acesso.

Chama a atenção que não houve o envolvimento nem do Gabinete de Segurança Institucional nem da própria ABIN, o que motivou comentários de que o governo estaria tentando organizar uma inteligência paralela.

Em razão dos riscos desse tipo de tecnologia, o Senador Alessandro Vieira ingressou com ação popular para obstar a aquisição. Na petição inicial, assinada pelo advogado Renato Ribeiro de Almeida, argumenta-se que "tem-se a potencial adoção de um sistema que possibilitaria a espionagem, a partir de total anonimato, não sendo possível o conhecimento dos cidadãos sobre o destino e o uso dos seus dados, em completa violação ao princípio da autodeterminação informativa, garantido pela LGPD."

Mais uma vez, impressiona a falta de discussão pública e a ausência de qualquer cuidado em relação à adoção de uma tecnologia que é contrária a tudo o que a LGPD pretende proteger. Em outras palavras, enquanto a LGPD procura alinhar a tecnologia à proteção de dados, por meio de soluções como as de *privacy by design* ou *privacy by default*, esse tipo de aparelho, se colocado em uso, pode comprometer todo o regime protetivo, sujeitando qualquer brasileiro a uma extensa espionagem sem qualquer tipo de controle.

Trata-se de grave ataque não apenas aos direitos dos cidadãos brasileiros, mas sobretudo à democracia, possibilitando que o Estado possa assumir o verdadeiro papel de espião onipresente, de acordo com seu bel prazer e sem qualquer limite ou prestação de contas.

---

4 https://www.uol.com.br/tilt/noticias/redacao/2021/05/19/pegasus-conheca-o-software-da-crise-entre-carlos-bolsonaro-e-militares.htm

Por essas razões, já está mais do que na hora de ficarmos atentos às constantes tentativas de ataques estatais aos nossos dados pessoais. Ao contrário do que o título do artigo ironicamente sugere, atualmente não temos nenhum motivo para sorrir. Apenas para nos preocupar.

Publicado em 26/05/2021

Link: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/sorria-o-estado-brasileiro-esta-de-olho-em-voce-26052021