PARECER n. 00173/2024/GJU - 1/PFE-CVM/PGF/AGU

NUP: 19957.004475/2023-07
INTERESSADOS: COMISSÃO DE VALORES MOBILIÁRIOS - CVM
ASSUNTOS: DIREITO ADMINISTRATIVO E OUTRAS MATÉRIAS DE DIREITO PÚBLICO

EMENTA: DADOS PESSOAIS NÃO SENSÍVEIS. AUSÊNCIA DE PARÂMETROS JURÍDICOS PARA O ESTABELECIMENTO DA PROTEÇÃO MAIS ADEQUADA.

Considerando que o item 3.14 da Ferramenta [1] do Framework de Privacidade e Segurança da Informação, ao fazer referência a "dados sensíveis" não se limita a dados pessoais, na medida em que também se refere a dados organizacionais ou institucionais "que se divulgados ou acessados sem autorização, podem causar danos significativos à organização ou às partes interessadas envolvidas", indaga-se, por meio do Ofício Interno nº 4/2024/CVM/STI/DGOV (2189769), "*quais são os parâmetros jurídicos que devem ser considerados na criação de critérios de classificação de dados sensíveis não vinculados a pessoas?*".

Em atendimento, insta, de plano, observar que a presente consulta deriva de reposta apresentada por Anderson Araújo, coordenador da unidade de metodologia do Departamento de Privacidade e Segurança da Informação (DEPS/SGD/MGI), que instado sobre o tema, esclareceu ainda que tais "dados são geralmente protegidos por leis de privacidade, de sigilo fiscal, de propriedade intelectual ou de segredo comercial e industrial, entre outros regulamentos de segurança e de proteção de dados", concluindo, ao final que, "não se trata necessariamente de dados pessoais sensíveis, definidos pela LGPD como dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

O Brasil, no entanto, ainda não possui regulamentação específica para os dados não pessoais, exceto indiretamente no caso, por exemplo, de regimes previstos para os segredos no que se refere à concorrência desleal e aos crimes contra a inviolabilidade dos segredos[2]. Neste sentido, pode-se identificar, especialmente no contexto da legislação que trata sobre segredo industrial (*e.g.* Lei n° 9.610/1998[3], Lei n° 9.279/1996[4], Lei n° 9.609/1998[5]), alguns fundamentos para a proteção de informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços. Outros exemplos de normativos que atribuem sigilo a dados são, dentre vários, a Lei Complementar n° 105/2001 (sigilo bancário), a Lei n° 9472/1997 (comunicações) e a própria Lei n° 6385/1976 que, em seu art. 9°, § 2°, garante o sigilo das apurações em curso perante a CVM.

Não é do que se trata a presente consulta. Ao que parece, a área técnica indaga acerca da possível existência de regulamentação genérica sobre dados não pessoais sensíveis, ao escopo de que se fizesse possível o estabelecimento de algum critério de classificação mediante parâmetros jurídicos, para fins de mensurar a atribuição da proteção adequada. Todavia, no atual cenário nacional inexiste qualquer normativo em tal sentido, cabendo, inclusive, observar a ausência de submissão dos dados não pessoais à Lei Geral de Proteção de Dados (Lei n° 13.709/2018).

Não obstante, impende destacar, apenas tangenciando a matéria no país, a Lei nº 12.965/2014 (marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, regulamentada pelo Decreto nº 8.771/2016, que, dentre outras matérias, trata das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, bem como, indica procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, aponta medidas de transparência na requisição de dados cadastrais pela administração pública e estabelece parâmetros para fiscalização e apuração de infrações.

Estabelecido o contexto normativo relacionado à consulta, importa, neste ponto, deixar claro que em sentido oposto à proteção dos dados pessoais, cujo fundamento se assenta nos direitos humanos; no que se refere a dados não pessoais, vigora uma tendência de plena liberdade, onde os regulamentos, em contrapartida, são criados para tornar os dados não pessoais mais acessíveis e o compartilhamento mais seguro[6].

Para que fique claro: ao se cogitar acerca do estabelecimento de parâmetros para a proteção de tais dados, não se pode perder de perspectiva que a regra é publicidade, tendo em conta que os critérios técnicos apropriados à sua classificação deverão considerar a magnitude do risco envolvido em caso de vazamento.

Ao escopo de ilustrar a recomendação ora aduzida, importa destacar o Regulamento UE 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo ao regime para o livre fluxo de dados não pessoais na União Europeia (RLFD). Aplicável desde 28 de maio de 2019, o regulamento visa assegurar que os dados eletrônicos, que não sejam dados pessoais, possam ser livremente tratados em toda a União Europeia, proibindo restrições relativas ao local onde os dados podem ser armazenados ou tratados, conforme as condições que estipula.

Mais recente, o Regulamento UE 2022/868 do Parlamento Europeu e do Conselho, relativo à governança europeia de dados e que altera o Regulamento UE 2018/1724 (Regulamento de Governança de Dados), em vigor em 23 de junho de 2022 e aplicável desde setembro de 2023, faz algumas referências à avaliação do nível de proteção de tais dados no país terceiro, valendo-

se, para tanto, de critérios como a segurança pública e a defesa ou segurança nacional. Neste sentido, o seguinte excerto:

> (21) (...) A avaliação do nível de proteção assegurado no país terceiro em causa deverá, em especial, ter em conta o direito geral e setorial aplicável, incluindo em matéria de segurança pública, defesa, segurança nacional e direito penal, no que respeita ao acesso e proteção de dados não pessoais, acesso pelos organismos do setor público desse país terceiro aos dados transferidos, a existência e o funcionamento efetivo, no país terceiro, de uma ou mais autoridades de controlo independentes responsáveis por assegurar e impor o cumprimento do regime jurídico que garante o acesso a esses dados, os compromissos internacionais em matéria de proteção de dados, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos ou da participação do país terceiro em sistemas multilaterais ou regionais.

De extrema relevância ao escopo de auxiliar a área demandante quanto ao estabelecimento de critérios técnicos para avaliar o grau de proteção necessário aos dados não pessoais sensíveis, veja-se o seguinte excerto no que se refere, em especial, à imposição de maior rigor com relação aos dados altamente sensíveis, observada a proporcionalidade:

> (24) No que diz respeito à transferência para países terceiros, poderá ser necessário, a fim de criar confiança nos mecanismos de reutilização, impor condições mais rigorosas para certos tipos de dados não pessoais que possam ser identificados como altamente sensíveis em futuros atos legislativos específicos da União, se essa transferência puder comprometer objetivos de política pública da União, em conformidade com os compromissos internacionais. Por exemplo, no domínio da saúde, certos conjuntos de dados detidos por atores do sistema de saúde pública, tais como hospitais públicos, poderão ser identificados como dados de saúde altamente sensíveis. Outros setores relevantes incluem os transportes, a energia, o ambiente e as finanças. A fim de assegurar práticas harmonizadas em toda a União, esses tipos de dados públicos não pessoais altamente sensíveis deverão ser definidos pelo direito da União, por exemplo no contexto do espaço europeu de dados de saúde ou de outro direito setorial. Essas condições associadas à transferência desses dados para países terceiros deverão ser estabelecidas em atos delegados. As condições deverão ser proporcionadas, não discriminatórias e necessárias para proteger os objetivos legítimos de política pública da União identificados, tais como a proteção da saúde pública, a segurança, o ambiente, a moral pública, a defesa do consumidor, a privacidade e a proteção dos dados pessoais. As condições deverão corresponder aos riscos identificados em relação à sensibilidade desses dados, inclusive em termos de risco de reidentificação das pessoas. Essas condições poderão incluir condições aplicáveis à transferência ou disposições técnicas, como o requisito de utilizar um ambiente de tratamento seguro, restrições no que diz respeito à reutilização de dados em países terceiros ou às categorias de pessoas habilitadas a transferir os dados para países terceiros ou que podem aceder aos dados nos países terceiros. Em casos excecionais, tais condições poderão também incluir restrições à transferência de dados para países terceiros a fim de proteger o interesse público.

Ante o exposto, em que pese a ausência de parâmetros jurídicos a serem considerados na criação de critérios de classificação de dados sensíveis não vinculados a pessoas, recomenda-se, caso se entenda pertinente, a adoção de critério segundo o qual o rigor necessário à proteção do dado seja diretamente proporcional à magnitude do provável risco na hipótese de um incidente de segurança.

À consideração superior.

Rio de Janeiro, 14 de novembro de 2024.

Marilisa Wernesbach Grimberg
Procuradora Federal

---

[1] A Ferramenta do Framework é uma Planilha Eletrônica, criada no Microsoft Excel, (pacote office 365), com funcionalidades, design e recursos específicos, desenvolvida pela equipe da SGD, com a finalidade de facilitar a aplicação e acompanhamento da implementação de suas medidas. Com ela, os indicadores de maturidade em privacidade e segurança da informação poderão ser obtidos e acompanhados a partir do preenchimento de seus formulários diagnósticos. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/faq-framework

[2] Cf. Informação é poder – para lá da Propriedade Intelectual e dos Dados Pessoais, por Marcos Wachowicz, Giulia Michelotto, disponível em https://ioda.org.br/informacao-e-poder-a-propriedade-intelectual-e-os-dados-pessoais/

[3] Sobre direitos autorais.

[4] Sobre propriedade industrial.

[5] Sobre propriedade intelectual de programa de computador.

[6] Nesta linha o art. 9°, inciso I do Decreto n° 8.771/2016 preceitua:

Art. 9º Ficam vedadas condutas unilaterais ou acordos entre o responsável pela transmissão, pela comutação ou pelo roteamento e os provedores de aplicação que:

I - comprometam o caráter público e irrestrito do acesso à internet e os fundamentos, os princípios e os objetivos do uso da internet no País;

DESPACHO n. 00275/2024/GJU - 1/PFE-CVM/PGF/AGU

NUP: 19957.004475/2023-07
INTERESSADOS: COMISSÃO DE VALORES MOBILIÁRIOS - CVM
ASSUNTOS: DIREITO ADMINISTRATIVO E OUTRAS MATÉRIAS DE DIREITO PÚBLICO

De acordo com o **PARECER n. 00173/2024/GJU - 1/PFE-CVM/PGF/AGU.**

À análise superior.

São Paulo, 18 de novembro de 2024.

FELIPE MÊMOLO PORTELA
PROCURADOR FEDERAL
SUBPROCURADOR CHEFE / GJU-1
AGU/PGF/PFE/CVM