ILICITUDE DA DEVASSA: TRATAMENTO DE DADOS PESSOAIS DE JURADOS EM FACE DOS PRINCÍPIOS DA CONVENÇÃO DE BUDAPESTE E DO ANTEPROJETO DA LGPD-PENAL NO BRASIL

ILLICIT OF THE THOROUGH INVESTIGATION: PROCESSING OF PERSONAL DATA OF JURORS IN THE FACE OF THE PRINCIPLES OF THE BUDAPEST CONVENTION AND THE DRAFT LGPD-PENAL IN BRAZIL

Rodrigo Oliveira de Camargo

Doutorando e Mestre em Ciências Criminais pela PUCRS. Bolsista Capes. Coordenador Estadual adjunto do IBCCRIM no Estado do Rio Grande do Sul e no Estado de Santa Catarina. Professor de Direito Penal e Processo Penal.

Link Lattes: http://lattes.cnpq.br/3857509102507710

ORCID: https://orcid.org/0000-0003-2340-9901

rodrigo@rodrigodecamargo.com.br

Resumo: A partir do reconhecimento de nulidade por ofensa à paridade de armas em razão do tratamento de dados pessoais, pelo Ministério Público, de integrantes da lista de jurados no Caso *Kiss*, propõe-se a verificação da licitude dessa conduta em face dos princípios estabelecidos pela Convenção de Budapeste e pelo Anteprojeto da LGPD-Penal. Analisando os princípios e categorias de titulares de dados apontados pelos textos observados, foi possível encaminhar o entendimento de que, para além do reconhecimento de ofensa à paridade de armas operado pelo Tribunal de Justiça do Estado do Rio Grande do Sul, a devassa de dados pessoais para a obtenção de informações para a formação do Conselho de Sentença não encontra amparo nos textos analisados, seja porque não se adequa aos princípios estabelecidos, seja em razão do fato de que a condição de jurado sequer constar na categoria de titulares de dados cuja norma autoriza o tratamento para fins de segurança pública e de investigação criminal.

Palavras-chave: Tratamento de Dados Pessoais – Jurados – Ilicitude – Convenção de Budapeste – LGPD-Penal.

Abstract: Based on the recognition of nullity for offense to the equality of arms due to the treatment of personal data, by the Public Prosecutor's Office, of members of the jury list in the Kiss case, we propose the verification of the lawfulness of this conduct in face of the principles established by the Budapest Convention and by the Draft LGPD-Penal. By analyzing the principles and categories of data subjects pointed out by the texts observed, it was possible to forward the understanding that, beyond the recognition of offense to the equality of arms operated by the Court of Justice of the State of Rio Grande do Sul, the search of personal data to obtain information for the formation of the sentence council does not find support in the texts analyzed, whether because it is not adequate to the principles established, or because of the fact that the condition of juror is not even in the category of holders of data whose norm authorizes the treatment for the purposes of public security and criminal investigation.

Keywords: Personal Data Processing – Jurors – Illicit – Budapest Convention – LGPD-Penal.

Por ocasião da apreciação dos recursos de apelação ofertados pelas defesas no caso do incêndio da boate *Kiss*, uma das maiores tragédias – factual e jurídica – recentes da história do Brasil, a 1ª Câmara Criminal do Tribunal de Justiça do Estado do Rio Grande do Sul, por maioria, anulou o julgamento realizado pelo Tribunal do Júri reconhecendo, dentre tantas outras, uma nulidade por ofensa à paridade de armas em razão do tratamento de dados pessoais, pelo Ministério Público, de integrantes da lista de jurados. Por ocasião do sorteio para a formação do Conselho de Sentença na data do júri, os representantes do órgão responsável pela acusação impugnaram 108 pessoas, motivando sua recusa com base em dados pessoais obtidos – e tratados – a partir do Sistema de Consultas Integradas, ferramenta a que tem à sua disposição livre acesso em razão de convênio firmado com o Poder Executivo do Estado do Rio Grande do Sul, por meio da Secretaria de Segurança Pública, visando o acesso ao seu banco de dados e que oferece enorme panorama de informações sigilosas sobre as pessoas.

O tema é instigante, diversas são as análises possíveis a partir deste único ponto, mas, aqui, a proposta é verificar a licitude da iniciativa do Ministério Público ante os princípios estipulados pela Diretiva 2016/680, também conhecida como Convenção de Budapeste, e do Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, daqui para a frente LGPD-Penal no Brasil, elaborado pela Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados.

A Convenção de Budapeste é um instrumento jurídico firmado por 46 dos 47 países do Conselho da Europa (exceção feita à Rússia), que estabelece as bases da política penal comum em face da delinquência relacionada à informática, promovendo uma

abordagem sob aspectos concretos para atuação no ciberespaço. Trata-se da referência legislativa internacional que pauta a política global no que guarda relação com a criminalização de condutas e desenvolvimento de ferramentas jurídicas no âmbito da investigação criminal, já que se propõe a superar os desafios em matéria de proteção de dados pessoais ante a evolução tecnológica e a globalização; o aumento da coleta e compartilhamento de dados pessoais; a necessidade de facilitação para transferência de dados para países terceiros e organizações internacionais e a profusão tecnológica que passou a permitir o tratamento de dados pessoais em escalas sem precedentes. Permite o tratamento de dados relacionados à infrações e condenações penais, onde também estão previstas disposições que regulam procedimentos, medidas cautelares e de segurança conexas ao tratamento de dados pessoais.

Este mesmo instrumento inspirou a redação do Anteprojeto LGPD-Penal no Brasil, elaborado pela Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados e que foi formada para demonstrar a necessidade e apresentar a estrutura e os principais conceitos para regular o tratamento de dados pessoais no âmbito da segurança pública e de atividades de persecução e repressão de infrações penais no Brasil. Fortificado em 12 capítulos e 68 artigos, abordam oito eixos de análise para disciplinar princípios, diretrizes e linhas mestras da proteção de dados e harmonizar os deveres do Estado na prevenção e na repressão de ilícitos criminais às observâncias das garantias processuais e prerrogativas fundamentais no que tange ao tratamento de dados pessoais e com a pretensão de complementar o microssistema legislativo de tratamento de dados para fins de segurança pública e de investigação criminal, hoje existente em leis esparsas e voltadas à regulamentação de quebras de sigilo no contexto processual penal.

Excepcionalmente, dados pessoais poderão ser tratados quando o tratamento for estritamente necessário; mediante a adoção de medidas técnicas e organizativas em razão dos maiores riscos que pendem sobre esses tipos de dados e somente nos casos autorizados por lei, se for necessário para a proteção dos interesses vitais do titular dos dados ou de um terceiro, se relacionado a dados manifestamente tornados públicos por seu titular. Uma das bases jurídicas que exclui a exigência do consentimento do interessado e legitima a obtenção e tratamento de dados pessoais por forças e corpos de segurança estatal – sobretudo nas atividades de investigação e coleta de elementos de autoria e materialidade da prática de uma infração penal – estão ancoradas no cumprimento de missão realizada em interesse público ou de poderes públicos, aqueles levados a efeito por autoridade competente investida. Para ser lícito, o tratamento de dados pessoais deverá ser necessário para a execução de uma missão de interesse público por uma autoridade competente para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Ao responsável pelo tratamento compete estabelecer uma distinção entre diferentes categorias de titulares de dados, tais como: (a) pessoas às quais existem motivos fundados para crer que cometeram ou estão prestes a cometer uma infração penal; (b) pessoas condenadas por uma infração penal; (c) vítimas de uma infração penal ou pessoas relativamente às quais certos fatos encaminhem à compreensão de que possam vir a ser vítimas de uma infração penal; e (d) terceiros envolvidos numa infração penal, tais como pessoas que possam ser chamadas a testemunhar em investigações penais relacionadas com infrações penais ou em processos penais subsequentes, pessoas que possam fornecer informações sobre infrações penais, ou contatos ou associados aos suspeitos ou condenados pela prática de uma infração penal. No contexto da LGPD-Penal no Brasil, esta categoria de titulares dos dados é ainda mais abrangente; para além daqueles previstos na Convenção de Budapeste, inclui: (e) as pessoas processadas pela prática de infração penal; e (f) as pessoas condenadas definitivamente pela prática de infração penal.

A obtenção do dado há de ser necessária para a investigação de um fato específico, jamais podendo admitir-se a procura especulativa, sem "causa provável", alvo definido, finalidade tangível ou com desvio de finalidade, para além dos limites autorizados, de elementos capazes de atribuir responsabilidade penal, o que configura a prática de *fishing expedition* (ROSA; SILVA; MELO E SILVA, 2019), já descartada pelos tribunais brasileiros (BRASIL, 2021). Assim, a coleta e tratamento de dados pessoais deve ser excepcional e subsidiária – somente se a finalidade do tratamento não puder ser obtida por outros meios – e, em ocorrendo, há de ser feita somente em dados adequados e necessários, sem excessos, para uma investigação concreta com fins explícitos e legítimos, os quais serão determinados no momento da coleta dos dados e que não excedam o tempo necessário em busca de ditos fins (MARTÍN, 2020, p. 411).

A atividade está orientada por princípios gerais previstos no Regulamento 2016/679 do Parlamento Europeu e do Conselho da União Europeia, que são o da legalidade; da necessidade e proporcionalidade da medida e no respeito aos interesses legítimos do indivíduo afetado, mas, a partir do Considerando 26 da Diretiva 2016/680, estabelece-se um rol específico aplicável ao tratamento de dados para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou execução de sanções penais. São eles: licitude e lealdade, limitação da finalidade, minimização, exatidão, limitação do prazo de conservação; integridade e confidencialidade; responsabilidade; proteção de dados por defeito e "desde o desenho".

Por licitude e lealdade, atribui-se a necessidade de que dados pessoais sejam tratados por uma autoridade competente se e na medida em que for necessário para o exercício de sua atribuição, cabendo-lhe especificar os objetivos do tratamento, os dados pessoais a tratar e as finalidades do tratamento. Lealdade ou transparência pressupõe um sistema de acesso sobre o tratamento que seja realizado de forma a assegurar ao afetado pelo tratamento condições de tomar conhecimento de sua realização e obter em face da autoridade informações precisas sobre as circunstâncias da obtenção, as finalidades, qual será o tipo de tratamento a que estarão sujeitos, o que será feito com o resultado do tratamento, se os resultados retroalimentarão novas pesquisas para produzir novos dados e se serão cedidos ou comunicados a terceiros.

A limitação de finalidade orienta que a coleta de dados ocorrerá com finalidade determinada, explícita e legítima, assegurando-se, ainda, o não tratamento posterior com finalidades alheias à original para fins incompatíveis com os da prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais; se dados pessoais forem tratados para finalidade distinta daquela para a qual foram recolhidos, este será permitido apenas se em conformidade com as disposições legais aplicáveis e se necessário e proporcional para a prossecução dessa outra finalidade. Minimização de dados significa que o tratamento se limita ao adequado e necessário para atingir os fins a que se destina e, na mesma medida em que o princípio da limitação do prazo de conservação, determina que os dados devem ser conservados apenas pelo período necessário para os fins aos quais se destina.

As autoridades competentes deverão assegurar que não sejam transmitidos nem disponibilizados dados pessoais incorretos, incompletos ou desatualizados, valor consagrado pelo princípio da exatidão, orientado a garantir a exaustividade e fiabilidade dos dados pessoais transmitidos ou disponibilizados. Este princípio aplica-se tendo em conta a natureza e a finalidade do tratamento em

causa, ganhando especial importância quando diante de processo judicial, já que muitas declarações que contêm dados pessoais são baseadas em percepções subjetivas e nem sempre verificáveis.

Já o princípio da integridade e confidencialidade impõe o emprego de segurança adequada ao tratamento de dados – vedação de tratamento não autorizado ou ilícito –, assim como de medidas técnicas apropriadas, orientadas a evitar a perda, destruição, inutilização ou danos acidentais aos dados pessoais. Aponta para o emprego de técnicas e gestão para evitar a violação de dados pessoais, o acesso ou a utilização desses dados e do equipamento utilizado por parte de pessoas não autorizadas, levando em conta as técnicas e tecnologias avançadas, os custos da sua aplicação em função dos riscos e a natureza dos dados pessoais a proteger. A propósito, decorre do princípio da responsabilidade o dever do responsável pelo tratamento de dados em aplicar medidas técnicas e organizacionais adequadas, além de estar em condições de demonstrar que o tratamento realizado se encontra em conformidade com a Diretiva 2016/680.

Finalmente, o princípio da proteção de dados por defeito e "desde o desenho" indica que, levando em consideração o custo de aplicação, a natureza, o âmbito, o contexto e os fins, o responsável pelo tratamento deve aplicar – seja no momento de determinação dos meios, seja no momento de execução do tratamento – procedimentos e técnicas voltadas a reduzir ao máximo o tratamento de dados pessoais, ocultar assim que possível os dados pessoais, dar transparência de forma a permitir que os interessados supervisionem o tratamento de dados, a melhorar o sistema de segurança, enfim, medidas concebidas para aplicar os demais princípios de proteção de dados.

Anteprojeto LGPD-Penal no Brasil, elaborado pela Comissão de Juristas, também indica as balizas e parâmetros aplicáveis a qualquer operação de tratamento de dados pessoais realizada por autoridades competentes em atividades de segurança pública e de persecução penal, equilibrando a proteção do titular contra mau uso e abusos, como acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações.

Aponta como seus fundamentos a dignidade, os Direitos Humanos, o livre desenvolvimento da personalidade, e o exercício da cidadania pelas pessoas naturais; a autodeterminação informativa; o respeito à vida privada e à intimidade; a liberdade de manifestação do pensamento, de expressão, de informação, de comunicação e de opinião; a presunção de inocência; confidencialidade e integridade dos sistemas informáticos pessoais; e garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal, sendo seus princípios inspirados na LGPD e que devem guiar as etapas e as cadeias do tratamento de dados pessoais no âmbito da investigação. O tratamento de dados deve: (i) estar embasado em hipótese legal (licitude); (ii) ocorrer para fins legítimos, específicos, explícitos e informados ao titular, vedado tratamento posterior de forma incompatível (finalidade); (iii) ser realizado com pertinência às suas finalidades e com o mínimo suficiente para consecução dos objetivos do tratamento (adequação). Deve haver, ainda: (iv) compatibilidade do tratamento com seus objetivos e serem assegurados (proporcionalidade); (v) livre acesso às garantias de facilidade e gratuidade ao acesso às informações (livre acesso) de; (vi) formas claras, precisas e acessíveis (qualidade dos dados); (vii) sobre o tratamento que está sendo realizado nos dados dos titulares e sobre o seu responsável (transparência). Os dados devem: (viii) ser atualizados com exatidão, clareza, relevância (segurança); (ix) empregados medidas técnicas e administrativas para a sua não violação (prevenção); e (x) evitar a realização do tratamento para fins discriminatórios, ilícitos ou abusivos (não discriminação); cabendo (xi) a responsabilização e prestação de contas em caso de violação.

Estabelecido este panorama, cabe-nos enfrentar a nossa problemática central: em face do que estabelecem a Convenção de Budapeste e LGPD-Penal no Brasil, quais poderiam ser apontados como os pecados capitais da atividade desenvolvida pelo Ministério Público?

A primeira ilicitude – e não, nulidade – decorre de que jurados não constam na categoria de titulares de dados que as orientações internacionais autorizam o afastamento da garantia fundamental da proteção de dados pessoais para fins de segurança pública e persecução penal, de forma que dados pessoais de jurados jamais poderiam ter sido tratados por qualquer uma das partes, nem mesmo autoridades competentes em atividades de segurança pública e de persecução penal. Admitir tal hipótese seria admitir o tratamento de dados pessoais de juízes.

Ademais, o tratamento sobre a base de dados dos jurados não foi feito sobre nenhum fato específico. A atividade traduziu-se em flagrante pescaria probatória, de forma a que importavam quaisquer dados que pudessem justificar alguma recusa. O fato passaria a importar após a aquisição do dado, não antes, como exige o princípio.

Por outra perspectiva, também podemos apontar que o tratamento de dados pessoais dos jurados realizado pela acusação reside no terreno da ilicitude em decorrência do fato de que, em que pese anunciadas uma série de reuniões prévias com os pretendentes a compor o Conselho de Sentença, em momento algum foram-lhes asseguradas condições de tomar conhecimento de sua realização e obter em face da autoridade informações precisas sobre as circunstâncias da obtenção, as finalidades, qual seria o tipo de tratamento a que foram sujeitados, o que foi feito com o resultado do tratamento, se os resultados retroalimentariam novas pesquisas ou e se seriam cedidos ou comunicados a terceiros. Tampouco, se o tratamento limitou-se ao adequado e necessário para atingir os fins a que se destinava ou ao estritamente adequado e necessário para atingir os fins a que se destinava.

Neste cenário, pois, o Ministério Público incorreu em prática atentatória à principiologia estabelecida pela Convenção de Budapeste e delineada no Anteprojeto da Comissão de Juristas para a elaboração da LGPD-Penal no Brasil, justificando-se sob diversos aspectos, portanto, a decisão do Tribunal de Justiça do Estado do Rio Grande do Sul. Para além da ofensa ao princípio da paridade de armas, assim como reconhecido no acórdão, a licitude da própria atividade de tratamento de dados pessoais fica comprometida; além de jurados não figurarem na categoria de titulares de dados que podem ter seu direito fundamental afastado para fins de segurança pública e persecução penal, ela ocorreu em violação a diversos dos princípios que sustentam as exceções à regra de proibição do tratamento de dados pessoais.

Referências

BRASIL. Superior Tribunal de Justiça. Agravo Regimental na PET no RMS: 62.562 MT 2019/0374119-3, Rel. Min. Felix Fischer, T5 - Quinta Turma, *Diário da Justiça Eletrônico*, 15 abr. 2021.

MARTÍN, Joaquín Delgado. *Judicial-Tech, el proceso digital y la transformación de la justicia*: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer. 2020.

ROSA, Alexandre Morais; SILVA, Viviani Ghizoni; MELO E SILVA, Philipe Benoni. *Fishing expedition e encontro fortuito na busca e apreensão*. Florianópolis: EMais, 2019.

Autor convidado