PROCESSO Nº 00261.001722/2023-13

Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Fiscalização
Coordenação de Fiscalização

Nota Técnica nº 29/2024/FIS/CGF/ANPD

INTERESSADO: MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA - MJSP, GABINETE DO DIRETOR-PRESIDENTE DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

1. ASSUNTO

1.1. Ministério da Justiça e Segurança Pública (MJSP).

1.2. Confederação Brasileira de Futebol (CBF).

2. REFERÊNCIAS

2.1. Acordo de Cooperação entre o MJSP e a CBF para compartilhamento de dados pessoais visando ao aprimoramento do Projeto Estádio Seguro. O projeto prevê ações de combate ao racismo e à violência nos estádios brasileiros, com a aplicação do uso de tecnologias que permitam identificar torcedores que tenham se envolvido em ilícitos e possam, porventura, causar problemas nas praças esportivas.

2.2. Relatório de Impacto à Proteção de Dados (RIPD).

2.3. Protocolo de Execução nº 1/2023 – Projeto Estádio Seguro.

3. SUMÁRIO EXECUTIVO

3.1. Processo sei nº 00261.001722/2023-13;

3.2. Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD);

3.3. Ofício nº 111/2023/CGDI/AESP/GM/MJ (SEI-PR nº 4374407/SEI-ANPD nº 0048180);

3.4. Acordo {***/2023/GM} (SEI-PR nº 4374421/SEI-ANPD nº 0048181);

3.5. Despacho nº 970/2023/CGINT-DIOPI/DIOPI/SENASP (SEI-PR nº 4374524/SEI-ANPD nº 0048184);

3.6. Anexo Protocolo de Execução 1/20233 (SEI-PR nº 4374450/SEI-ANPD nº 0048182);

3.7. Relatório de Impacto à Proteção de Dados Pessoais (SEI-PR nº 4375287/SEI-ANPD nº 0048187);

3.8. Lei nº 13.675, de 11 de junho de 2018 – Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp); altera a Lei Complementar nº 79, de 7 de janeiro de 1994, a Lei nº 10.201, de 14 de fevereiro de 2001, e a Lei nº 11.530, de 24 de outubro de 2007; e revoga dispositivos da Lei nº 12.681, de 4 de julho de 2012;

3.9. Lei nº 8.159, de 8 de janeiro de 1991 – Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;

3.10. Lei nº 14.597, de 14 de junho de 2023 – Institui a Lei Geral do Esporte;

3.11. Decreto nº 9.489, de 30 de agosto de 2018 – Regulamenta, no âmbito da União, a Lei nº 13.675, de 11 de junho de 2018, para estabelecer normas, estrutura e procedimentos para a execução da Política Nacional de Segurança Pública e Defesa Social;

3.12. Portaria Ministerial nº 218, de 29 de setembro de 2021 – Dispõe sobre a Plataforma Integrada de Operações e Monitoramento de Segurança Pública - Córtex;

3.13. Decreto nº 11.348, de 1º de janeiro de 2023 – Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Justiça e Segurança Pública e remaneja cargos em comissão e funções de confiança;

3.14. Decreto nº 10.777, de 24 de agosto de 2021 – Política Nacional de Inteligência de Segurança Pública (PNISP);

3.15. Decreto nº 10.778, de 24 de agosto de 2021 – Estratégia Nacional de Inteligência de Segurança Pública (ENISP);

3.16. Decreto nº 10.046, de 9 de outubro de 2019 – Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

4. RELATÓRIO

4.1. Trata-se de processo instaurado por provocação da Diretoria de Operações Integradas e de Inteligência do Ministério da Justiça e Segurança Pública (DIOPI), por intermédio de seu encarregado, em que o órgão solicita apreciação e opinião técnica nos termos do §2º do art. 4º da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados.

4.2. O processo versa sobre o compartilhamento e o tratamento de dados pessoais visando ao aprimoramento do Projeto Estádio Seguro, que tem como objetivos gerais identificar sujeitos de interesse da justiça e segurança pública e promover ações de combate a atividades ilícitas cometidas no âmbito de eventos esportivos, com a aplicação de tecnologias para, por exemplo, verificar se o comprador de ingressos para jogos de futebol possui mandados de prisão em aberto, se há impedimentos estabelecidos pelo estatuto do torcedor, se houve o uso de documentos falsos ou outras situações correlatas (parágrafo 3.1.1., do Relatório de Impacto à Proteção de Dados Pessoais, primeira versão, SEI nº 0048187).

4.3. Em 21 de junho de 2023, por intermédio do Oficio nº 111/2023/CGDI/AESP/GM/MJ (SEI nº 0048180), o encarregado pelo tratamento de dados pessoais do MJSP encaminhou ao encarregado pelo tratamento de dados pessoais desta Autoridade Nacional de Proteção de Dados (ANPD) o Despacho nº 970/2023/CGINT-DIOPI/DIOPI/SENASP (SEI nº 0048184), que solicita apreciação e opinião técnica nos termos do §2º do art. 4º da Lei nº 13.709/2018 de três documentos relacionados ao projeto em comento: a minuta Acordo {***/2023/GM} (SEI nº 0048181), o Anexo Protocolo de Execução 1/20233 (SEI nº 0048182) e o Relatório de Impacto à Proteção de Dados Pessoais (SEI nº 0048187).

4.4. Em 29 de junho de 2023, por meio do Despacho GABPR (SEI nº 0048185), os autos foram encaminhados a esta Coordenação-Geral de Fiscalização (CGF) para conhecimento e adoção das providências consideradas cabíveis. Ato contínuo, em 25 de outubro de 2023, a Coordenação-Geral de Fiscalização, por meio do Informe nº 2/2023/CGF/ANPD (SEI nº 0048196), intimou o MJSP a se manifestar, dentro do prazo de 20 dias úteis, em relação às determinações constantes nas alíneas ‘a’ a ‘w’ da Nota Técnica nº 175/2023/CGF/ANPD (SEI nº 0048192).

4.5. Em 05 de janeiro de 2021, o MJSP enviou para análise da CGF a versão 2.0. do Relatório de Impacto à Proteção de Dados (SEI nº 0048206). No entanto, o órgão público federal deixou de encaminhar para esta autarquia federal os demais documentos relacionados ao procedimento fiscalizatório em andamento, com as devidas alterações determinadas na conclusão da Nota Técnica nº 175/2023/CGF/ANPD. Desse modo, foi enviado ao MJSP, em 08 de janeiro de 2024, o Ofício nº 1/2024/FIS/CGF/ANPD (Sei nº 0048207), solicitando o encaminhamento dos documentos mencionados, o que, finalmente, ocorreu em 14 de janeiro de 2024, quando chegaram à ANPD o Acordo de Cooperação nº 7/2023 (Sei nº 0048533), o extrato de Acordo de Cooperação publicado no Diário Oficial da União (Sei nº 0048535), a versão 2.0. do Relatório de Impacto à Proteção de Dados (Sei nº 0048538) e a minuta do Protocolo de Execução nº 1/2023 – Projeto Estádio Seguro (Sei nº 0048540).

4.6. Considerando que todos os documentos necessários para o exame do cumprimento das determinações exaradas por meio da Nota Técnica nº 175/2023/CGF/ANPD (SEI nº 0048192) encontram-se juntados ao procedimento fiscalizatório, passa-se à análise da conformidade do Projeto Estádio Seguro, à luz do disposto no art. 4º, §§ 1º e 3º, da LGPD, tendo como parâmetros a versão 2.0. do Relatório de Impacto à Proteção de Dados (Sei nº 0048538) e a minuta do Protocolo de Execução nº 1/2023 – Projeto Estádio Seguro (Sei nº 0048540).

4.7. É o relatório.

5. ANÁLISE

5.1. **Das determinações exaradas pela NOTA TÉCNICA nº 175/2023/CGF/ANPD** (SEI nº 0048192)**.**

5.1.1. A Nota Técnica nº 175/2023/CGF/ANPD (SEI nº 0048192), elaborada pela Coordenação Geral de Fiscalização da ANPD (CGF), para avaliar a legalidade e a legitimidade das operações de tratamento de dados pessoais relacionadas à execução do projeto Estádio Seguro, teve como escopo o acordo de cooperação técnica celebrado entre a CBF e o MJSP e seu respectivo plano de ação, o anexo protocolo de execução 1/20233 e o relatório de impacto à proteção de dados pessoais (RIPD).

5.1.2. A análise técnica da CGF concluiu, inicialmente, que a Lei nº 13.709/2018, Lei Geral de Proteção de Dados – LGPD, à luz do disposto nos §§ 1º e 3º do art. 4º da LGPD, reservou competência para que a ANPD possa emitir opiniões técnicas ou recomendações quanto ao tratamento de dados pessoais para fins de segurança pública, defesa nacional, segurança do estado e atividades de investigação e repressão de infrações penais. A competência regulatória se limitaria, no entanto, a aspectos do tratamento de dados pessoais relacionados ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular. Desse modo, a ANPD teria competência para solicitar às entidades públicas envolvidas os respectivos relatórios de impacto à proteção de dados pessoais.

5.1.3. Em seguida, a partir de exame minucioso de aspectos legais e procedimentais relacionados à observância do devido processo legal, dos princípios gerais de proteção de dados pessoais e dos direitos dos titulares, sob uma perspectiva do interesse público subjacente às finalidades do projeto Estádio Seguro, a Coordenação Geral de Fiscalização da ANPD concluiu que o Ministério da Justiça de Segurança Pública deveria realizar ajustes nos documentos encaminhados, de maneira a buscar a conformidade do projeto com as normas de proteção de dados pessoais aplicadas ao caso concreto. Desse modo, foram expedidas as determinações abaixo relacionadas:

> · ***Sobre a designação de operador constante do parágrafo 5.3.1 do RIPD:***
>
> *a) O MJSP deve ajustar o RIPD para esclarecer o papel do operador de dados, considerando o exposto no [item 5.17] ao [item 5.21] da Nota Técnica n 175/CGF/ANPD.*
>
> · ***Sobre o interesse público nas finalidades declaradas para tratamento dos dados pessoais:***
>
> *b) O MJSP deve ajustar o RIPD para deixar claro que o combate ao cambismo se refere às condutas tipificadas como crimes nos art. 166 e 167 da Lei nº 14.597/2023. Alternativamente, caso a presunção não seja verdadeira e o conceito de cambismo se refira a conduta diversa, o RIPD deve esclarecer as razões de interesse público que justificam o tratamento dos dados coletados para essa finalidade; explicitar a eventual competência do MJSP na consecução desse interesse; e justificar o tratamento de dados para essa finalidade com base no art. 4º, III, da LGPD, e não em outra hipótese legal.*
>
> · ***Sobre a observância aos princípios da adequação e necessidade:***
>
> *c) MJSP deve acrescentar ao RIPD os dados que serão tratados e como serão tratados, para o atendimento à finalidade (iii) [identificação de veículos furtados] nos mesmos moldes do realizado para as outras duas finalidades conforme descrito nos parágrafos 3.1.1. a 3.1.8. e 3.2.1. a 3.2.3. do RIPD.*
>
> *d) No que se refere à captura do registro facial do comprador ou beneficiário e envio pela EPD, o MJSP deve acrescentar ao RIPD a informação de que serão tratados dados biométricos e como serão tratados, inclusive atualizando os procedimentos descritos nos parágrafos 3.1.1. a 3.1.8. do RIPD.*
>
> *e) Sobre a coleta da data de nascimento, cumpre corrigir a expressão "com obrigatoriedade para indivíduos com idade ≥ 18 anos e ≤ 80 anos" no tópico "10. Plano de Ação" do Plano de Trabalho*

para que fique claro que apenas dados de maiores de dados serão repassados ao MJSP.

· ***Sobre a observância aos princípios da Transparência e do Livre Acesso:***

f) O MJSP, portanto, deve adequar o protocolo de execução para garantir o atendimento ao princípio da transparência, nos moldes do exposto no parágrafo 5.4.1. do RIPD, considerando as informações constantes nos parágrafos 2.2., 3.1.1., 3.4.2., 3.4.3. do RIPD, não só pela EPD como também pelo próprio MJSP e demais integrantes das forças de segurança pública que participarem do Projeto Estádio Seguro.

g) A EPD e o MJSP devem garantir que conste nos lugares de venda (on-line, nas bilheterias nos estádios ou nas revendedoras autorizadas), por escrito, informação de que os dados pessoais serão compartilhados com MJSP para fins de segurança pública com a finalidade de (i) recapturar indivíduos com mandado de prisão ou medidas penais restritivas; e (iii) evitar a venda de ingressos utilizando dados de pessoas falecidas, combatendo o cambismo.

h) A EPD e o MJSP devem garantir que conste nos estacionamentos e cercanias dos estádios onde houver câmeras, por escrito, informação de que os dados pessoais serão compartilhados com MJSP para fins de segurança pública com a finalidade de (ii) auxiliar na recuperação de veículos roubados ou furtados.

· ***Sobre a observância do princípio da Qualidade:***

i) O MJSP deve, por conseguinte, acrescentar ao RIPD esclarecimentos sobre como pretende garantir a exatidão, clareza, relevância e atualização dos dados tratados para essa finalidade.

· ***Sobre a Frequência do Tratamento e Tempo de Retenção:***

j) O MJSP deve ajustar o RIPD para deixar claro que somente serão repassados os dados de sujeitos de interesse (que acusem problema de falha na validação biométrica, suspeitos de usar documento falso ou outro tipo de ocorrência).

k) O MJSP deve ajustar o RIPD para deixar claro que os dados pessoais serão excluídos após o encerramento do evento esportivo e que não haverá compartilhamento em tempo real e com imagem dos dados e as informações relativas ao registro das passagens e movimentações de veículos registrados pelas câmeras do estacionamento do estádio após o encerramento do evento esportivo.

· ***Sobre o compartilhamento de dados pessoais:***

l) O MJSP deve esclarecer a possível contradição entre o previsto no parágrafo 3.2.4. do RIPD e o parágrafo 5.9. da minuta do ACT, em atenção ao exposto no [item 5.175] ao [item 5.176] desta Nota Técnica.

· ***Sobre a Análise dos Riscos:***

m) O MJSP deve adotar as providências indicadas como necessárias no quadro que segue o [item 5.133] desta Nota Técnica, com vistas a suprir as deficiências apontadas nas medidas de mitigação e tratamentos dos riscos R06, R07, R09, R10 e R11.

· ***Sobre o plano de trabalho:***

n) O MJSP deve ajustar o parágrafo 8.1. da minuta de ACT para garantir que, em seu nome, apenas servidores públicos possam ser designados como gestores e responsáveis.

o) O MJSP deve ajustar o eixo IV do Plano de Ação para excluir a coleta e o compartilhamento do número do telefone.

p) É preciso que o MJSP esclareça se a base será inteiramente gerida pela MJSP, se haverá compartilhamento dessas informações com as Entidades de Práticas Desportivas e em que condições.

q) Ainda, o MJSP deve ajustar a redação do eixo XI para que conste expressamente que a cooperação se dará pelo compartilhamento "da relação de associados e membros, sócio-torcedores, membros de torcidas organizadas e torcedores com acessos impedidos às áreas desportivas".

· ***Sobre o Protocolo de Execução:***

r) Recomenda-se seja revisada a redação do preâmbulo do protocolo de execução para correta referência aos parágrafos do ACT.

s) O MJSP deve alterar a redação do inciso I da Cláusula Quarta para que o tratamento fique restrito às finalidades declaradas nos parágrafos 2.1. e 2.2. do RIPD. Alternativamente, o MJSP deve ajustar o RIPD para deixar claro que existe esta quarta finalidade (inclusive alterando as informações que serão prestadas ao titular sob o princípio da transparência) e que somente serão mantidos os dados

de sujeitos de interesse (que acusem problema de falha na validação biométrica, suspeitos de usar documento falso ou outro tipo de ocorrência) ou relacionados a veículos furtados ou roubados.

t) O MJSP deve fazer constar no inciso II da Cláusula Quarta do Protocolo de Execução expressa menção ao dever de elaborar RIPD e submeter a proposta de compartilhamento de dados previamente à ANPD.

u) O MJSP deve ajustar a redação do inciso VI da Cláusula Quarta do Protocolo de Execução para garantir que, em seu nome, apenas servidores públicos possam ser designados como gestores e responsáveis.

v) O MJSP deve ajustar a redação do inciso I da Cláusula Sexta do Protocolo de Execução para que conste expressamente, ainda que por referência ao demais incisos da Cláusula Sexta, quais são os dados que serão fornecidos ao MJSP, no intuito de evitar alargamento irregular e indevido dos dados compartilhados sem fundamento legal ou a devida reflexão quanto aos riscos associados ao tratamento quando da elaboração do RIPD.

w) O MJSP deve indicar nova justificativa legal para o recolhimento e tratamento dessas informações e atualizar a referência legislativa no inciso XVII da Cláusula Sexta.

5.1.4. O MJSP, em resposta às determinações da Nota Técnica nº 175/2023/CGF/ANPD, encaminhou à CGF os seguintes documentos:

i. A versão 2.0. do relatório de impacto à proteção de dados referente ao projeto Estádio Seguro; e

ii. A minuta do protocolo de execução nº 1/2023.

5.1.5. O órgão público federal informou, ainda, que não foram realizadas as modificações apontadas pela ANPD no acordo de cooperação nº 007/2023 - Projeto Estádio, assim como em seu plano de ação, uma vez que o documento já havia sido assinado em 20 de setembro de 2023, o que impediu eventuais alterações em seu texto. No entanto, o MJSP afirmou que as determinações exaradas pela ANPD, na medida do possível, foram inseridas na minuta do protocolo de execução[1].

5.1.6. A presente análise, portanto, terá como objetivo verificar se a versão 2.0. do relatório de impacto à proteção de dados referente ao projeto Estádio Seguro e a minuta do protocolo de execução nº 1/2023 atenderam às determinações exaradas pela Nota Técnica nº 175/2023/CGF/ANPD. Em especial, devido os limites à aplicação da LGPD ao tratamento de dados pessoais para fins de segurança pública e atividades de investigação e repressão de infrações penais, serão analisadas apenas as questões atinentes ao devido processo legal, à observância dos princípios gerais de proteção de dados pessoais e à existência de mecanismos por meio dos quais os titulares de dados possam exercer seus direitos.

5.2. **Contexto do tratamento de dados pessoais no âmbito do projeto Estádio Seguro.**

5.2.1. Conforme o item 6.1. da versão 2.0. do RIPD, o tratamento de dados pessoais realizado no âmbito do projeto Estádio Seguro tem como objetivo *"(a)uxiliar as polícias estaduais na identificação de pessoas procuradas pela justiça, torcedores com ordem judicial de afastamento, bem como na verificação de envolvidos em atos de violência, racismo, xenofobia, LGBTfobia e violação das regras de segurança praticados no período que antecede, coincide e prossegue após a partida, além de identificar veículos roubados, furtados e proprietários desses bens procurados pela justiça".*

5.2.2. O projeto Estádio Seguro, segundo o MJSP, desse modo, apresentaria soluções práticas e inovadoras quanto à identificação de indivíduos de interesse da segurança pública, bem como veículos em situação irregular. O projeto possibilitaria, ademais, o estabelecimento de mecanismos para impedir a venda de bilhetes a partir do uso de informações falsas, inexistentes ou fictícias durante o processo de aquisição do ingresso. Essa abordagem auxiliaria na prevenção da entrada de pessoas com restrições judiciais nos estádios e garantiria a integridade e a segurança de todos os participantes e espectadores. O órgão público federal, assim, argumenta que o projeto em tela constituiria "*iniciativa essencial para enfrentar os desafios atuais da segurança pública, proteger os participantes e espectadores de eventos esportivos e contribuir para a construção de um Brasil mais seguro*".

5.2.3. Para a consecução desse objetivo, o MJSP pretende firmar, com fundamento no acordo de cooperação nº 07/2023, protocolos de execução com entidades de prática desportiva filiadas à Confederação Brasileira de Futebol. As entidades esportivas[2], desse modo, se comprometeriam a

encaminhar ao órgão público, a cada evento esportivo, um conjunto de dados pessoais dos torcedores, os quais seriam processados junto às bases de verificação de dados custodiadas pelo MJSP. Pretende-se, assim, que seja possível identificar pessoas de interesse da justiça e da segurança pública, como foragidos da justiça, garantindo-se maior segurança para os frequentadores do evento esportivo, em particular, e para a sociedade, em geral.

5.2.4. A operacionalização do projeto contará com um Centro Nacional de Inteligência para Segurança no Esporte, localizado em Brasília-DF e gerido pela Coordenação Geral de Inteligência (CGINT) do MJSP, que será composto por profissionais mobilizados pela Secretaria Nacional de Segurança Pública (SENASP)[3]. Além disso, nos Estados, o projeto disporá de salas de operações de inteligência em cada estádio cuja entidade desportiva tenha aderido ao projeto, as quais serão compostas por integrantes dos órgãos de inteligência da Polícia Militar, Polícia Civil, CGINT-MJSP, agências centrais de ISP e CIISPR das respectivas regiões[4].

5.2.5. Para a operacionalização do projeto, ademais, será criado um subsistema modular destinado às atividades de segurança pública em competições desportivas (Projeto Estádio Seguro), desenvolvido dentro da Plataforma Córtex, hospedada/mantida pela Diretoria de Operações Integradas e de Inteligência do MJSP. Por meio desse subsistema, as entidades esportivas participantes do projeto encaminharão ao órgão público federal os dados das bases de vendas de bilhetes com as informações fornecidas pelos torcedores. Esses dados serão cruzados, na API da Plataforma Córtex, com os dados provenientes das bases de verificação que indicam o status da pessoa, as quais se encontram custodiadas pelo MJSP.

5.2.6. Os titulares dos dados, assim, passarão por processo de identificação com o objetivo de gerar conhecimento que auxilie na prevenção de crimes envolvendo os frequentadores dos eventos desportivos. Com base nessa identificação, o Córtex emite o código de bloqueio para a *ticketeira* do estádio, que, durante a integração com o sistema de acesso, comunica a informação de bloqueio para o número do bilhete em questão. Além disso, o Córtex alimenta a lista prévia de indivíduos de interesse da segurança pública, automatizando os dados para identificação no momento do acesso do torcedor.

5.2.7. O MJSP ressalta, ademais, que os clubes organizadores não terão conhecimento do conteúdo representado por cada código, devido à sua natureza sigilosa exclusiva, mas apenas tomarão conhecimento da transcrição necessária para cada código[5]. Assim, os códigos encaminhados pelo MJSP determinarão o bloqueio da catraca associada ao ingresso vinculado ao CPF do indivíduo relevante para a segurança pública, mantendo-se a *ticketeira* e o estádio alheios à natureza específica da situação[6]. O MJSP, dessa maneira, assegura que as entidades privadas não terão acesso à API da Plataforma Córtex, medida que serviria para garantir a privacidade dos titulares e a segurança do próprio sistema.

5.2.8. A versão 2.0 do RIPD descreveu, ainda, os estágios de tratamento de dados pessoais, que se dividem da seguinte forma[7]:

a) *A etapa 1 (consciência situacional)*.

5.2.9. Consiste no processo de identificação prévia do sujeito de interesse da justiça e segurança pública (indivíduos procurados, torcedores impedidos e pessoas desaparecidas, por exemplo), com base no registro de venda dos bilhetes. A fase ocorre antes do início do evento esportivo. Nesse momento, ocorre o cruzamento da base de dados da venda dos bilhetes, encaminhados pelos clubes de futebol, com as bases de dados em posse do MJSP, no âmbito da Plataforma Córtex. O MJSP garante que apenas profissionais das agências de inteligência estaduais e da Secretaria Nacional de Segurança Pública (SENASP), envolvidos obrigatoriamente na operação e previamente oficializado pelo gestor máximo das respectivas instituições, terão permissão para acessar e visualizar a lista prévia contendo os indivíduos identificados como de interesse para a segurança pública no respectivo evento.

5.2.10. Na etapa de consciência situacional, a aplicação da Plataforma Córtex mostrará dados pessoais, como_número do documento, nome do indivíduo de interesse, natureza/status (pessoa procurada, torcedor impedido e pessoa desaparecida), número do pedido, número do bilhete, portão de acesso, tipificação, estado de custódia, município de custódia, órgão do judiciário, número do processo e

link do mandado público para que possa ser baixado. Nessa etapa, não há verificação de dados de veículos, visto que seu cadastramento prévio pelas entidades desportivas não é obrigatório.

b) *A etapa 2 (alertas gerais – estádios)*.

5.2.11. Permite que os profissionais de segurança alocados nas praças dos eventos esportivos possam efetuar a abordagem dos sujeitos de interesse da justiça. Assim, quando um bilhete é vinculado aos dados pessoais de determinado sujeito de interesse da justiça, é enviado um código de bloqueio à catraca do estádio, a qual é automaticamente travada. Essa ação permite a abordagem do titular.

5.2.12. Os agentes de inteligência presentes na sala de operações de inteligência terão acesso, por meio da interface da Plataforma Córtex, a informações como o número do documento, nome do indivíduo de interesse, natureza (pessoa procurada, torcedor impedido e pessoa desaparecida), data e hora do acesso, portão de acesso, número do bilhete, tipificação e informações para o encerramento da ocorrência. Durante o evento, os agentes de inteligência também terão acesso às placas dos veículos que entraram nos estacionamentos dos estádios equipados com radares de tecnologia OCR, o que permitirá o tratamento desses dados por meio da API do Córtex.

5.2.13. Os sujeitos de interesse da justiça, após as abordagens, serão encaminhados ou convidados a entrar na sala de triagem da inteligência, onde suas identidades serão confirmadas.

c) *A etapa 3 (identificação de autoria*).

5.2.14. Consiste na verificação precisa da identidade das pessoas de interesse previamente apontadas, com vistas a identificar os autores de condutas lesivas à segurança pública durante o evento, como ações discriminatórias, como atos de racismo, xenofobia, LGBTfobia, além daqueles que se envolvem em atos violentos resultantes em lesões corporais ou morte. A implementação efetiva dessa terceira medida, coordenada pelo MJSP, está condicionada ao monitoramento por imagem das catracas e com identificação biométrica dos espectadores pelas entidades desportivas, em atenção ao art. 148 da lei nº 14.597, de 14 de junho de 2023 - Lei Geral do Esporte.

5.2.15. Desse modo, o MJSP esclarece que os dados biométricos coletados permitirão a sua comparação por meio de uma ferramenta tecnológica adequada com imagens provenientes de televisões, câmeras de vigilância dos estádios e das redes sociais. Nesse sentido, o órgão público federal considera "*relevante destacar que, considerando a possibilidade de ocorrência de delitos relacionados ao contexto esportivo no futuro, essa base de dados armazenadas pelo MJSP torna-se essencial para facilitar a identificação de torcedores envolvidos em diversos tipos de delitos ocorridos no contexto do evento esportivo*".

5.2.16. O MJSP, por fim, destacou que os dados pessoais dos titulares maiores de idade (não serão tratados dados de indivíduos menores de idade) serão armazenados, no *data center* do Ministério, por um *prazo máximo de 20 anos*, conforme estabelecido pelo art. 109, Inciso I, do Código de Processo Penal. A retenção dos dados teria como objetivo facilitar a identificação de torcedores envolvidos em diversos tipos de delitos ocorridos no contexto do evento esportivo no futuro.

5.3. **Dos agentes de tratamento.**

5.3.1. A Lei Geral de Proteção de Dados Pessoais definiu o controlador e o operador como os agentes de tratamento responsáveis pelas operações realizadas com dados pessoais. Embora ambos os agentes de tratamento sejam responsáveis pela observância da legislação, em especial quanto à proteção dos direitos garantidos aos titulares de dados, eles possuem competências distintas, a depender do seu papel no tratamento dos dados.

5.3.2. O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI, LGPD). Cabe ao controlador definir as diretrizes e o modo como as operações de tratamento serão realizadas. De maneira mais específica, pode-se afirmar que o controlador é o agente de tratamento responsável por definir os propósitos da atividade de tratamento e os meios pelos quais os objetivos do tratamento deverão ser alcançados.

5.3.3. O papel de controlador de proteção de dados nos órgãos da administração direta federal pertence à União Federal, órgão com personalidade jurídica de direito público. No entanto, uma vez que o

tratamento de dados pessoais pelo Poder Público é vinculado às finalidades públicas específicas de cada órgão ou entidade, conforme definido pelo *caput* do art. 23 da LGPD, o Estado não deve ser entendido como uma "unidade informacional"[8]. Ademais, em virtude do princípio da desconcentração administrativa, cada órgão ou entidade pública é competente para exercer o papel de controlador em relação ao tratamento de dados pessoais que sejam necessários para o exercício de suas competências legais ou para o cumprimento de atribuições legais de serviço público, nos termos definidos pelo art. 23 da LGPD.

5.3.4. No caso em análise, portanto, percebe-se que o Ministério da Justiça e Segurança Pública exerce o papel de controlador no âmbito do tratamento de dados pessoais necessários para a consecução dos objetivos do projeto Estádio Seguro. A competência do MJSP, no papel de controlador, é deixada clara logo no item 1. do RIPD (SEI nº 0048206), em que consta a identificação dos agentes de tratamento e do encarregado. Além disso, consta que a Ouvidoria-Geral do Ministério da Justiça e Segurança Pública desempenhará a função de encarregado de dados.

5.3.5. O operador, por sua vez, é a pessoa natural ou jurídica, de direito público ou direito privado, que realiza o tratamento de dados em nome do controlador (art. 5º, VII, LGPD). Dessa forma, ao operador cabe observar as instruções fornecidas pelo controlador, a quem caberá a verificação do cumprimento de suas instruções e das normas de proteção de dados.

5.3.6. Conforme explicado nos itens 5.18. a 5.20. da Nota Técnica nº 175/2023/CGF/ANPD, a definição legal de operador não deve ser entendida como uma norma de distribuição interna de competências e responsabilidades. Por esse motivo, empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta não devem ser considerados operadores, tendo em vista que este agente de tratamento será sempre uma pessoa distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos.

5.3.7. A partir da leitura do parágrafo 5.3.1. do RIPD, versão 1.0., poderia presumir-se que a Coordenação-Geral de Inteligência (CGINT), órgão interno da DIOPI, desempenharia o papel de operador do projeto. Por esse motivo, solicitou-se ao MJSP que esclarecesse a questão, uma vez que o órgão não poderia desempenhar, concomitantemente, os papéis de controlador e operador no âmbito da mesma operação de tratamento de dados.

5.3.8. A versão 2.0 do RIPD, desse modo, deixou de identificar a Coordenação-Geral de Inteligência (CGINT) como operadora do tratamento de dados realizado no Projeto Estádio Seguro. A CGINT passou a ser apresentada apenas como unidade administrativa responsável pelo projeto (itens 10. e 10.1). Ao longo do documento, ademais, foram identificadas outras competências da unidade administrativa supracitada, como a realização de auditorias na Plataforma Córtex (item 20.4) e a gestão do Centro Nacional de Inteligência para Segurança no Esporte (item 24.2).

5.3.9. Nota-se, contudo, que a informação quanto à identificação do *encarregado de dados* não está suficientemente clara. O encarregado de dados é o indicado pelo controlador para atuar como canal de comunicação entre o agente de tratamento, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Ao encarregado de dados compete (i) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; (ii) receber comunicações da autoridade nacional e adotar providências; (iii) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e (iv) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

5.3.10. Na versão 2.0 do RIPD, conforme já destacado, indica-se a Ouvidoria do Ministério da Justiça e Segurança Pública como a encarregada de dados. Porém, quem assina o documento na condição de encarregado é o Diretor do Departamento de Projetos e de Políticas de Direitos Coletivos e Difusos da Secretaria Nacional do Consumidor. Ao se entrar no sítio do MJSP, na aba referente ao tratamento de dados pessoais[9], também consta como encarregado de dados do órgão público federal o Diretor do Departamento de Projetos e de Políticas de Direitos Coletivos e Difusos (SENACON). O Ouvidor-Geral do MJSP, por sua vez, aparece apenas como o suplente do encarregado.

5.3.11. Observa-se, portanto, que há uma contradição sobre qual autoridade pública exercerá o papel de encarregado de dados do MJSP. Essa aparente contradição deve ser corrigida, pois pode gerar no titular de dados confusão sobre a quem deve se dirigir em caso de necessidade de exercício de direitos no que se refere ao tratamento de seus dados pessoais no âmbito do projeto.

5.4. **Do devido processo legal.**

5.4.1. ***Sobre o interesse público nas finalidades declaradas para o tratamento dos dados pessoais***

5.4.1.1. O art. 23 da LGPD limita o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI) ao atendimento de suas finalidades públicas, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. O tratamento de dados pessoais de torcedores pelas entidades de prática esportiva e o seu compartilhamento com o MJSP seria, conforme o controlador, *compatível* com as atribuições legais dos órgãos de segurança pública que compõe a sua estrutura, nos termos indicados pelo art. 23 da LGPD. Para corroborar este entendimento, foi apresentada competência específica da Secretaria Nacional de Segurança Pública, exarada no inciso XIV do art. 24 do Decreto nº 11.348/2023, logo a seguir:

> Decreto nº 11.348/2023
>
> Art. 24. À Secretaria Nacional de Segurança Pública compete:
>
> (...)
>
> **XIV - coordenar ações de prevenção à violência e à criminalidade.**

5.4.1.2. As atividades de tratamento de dados pessoais, no contexto do projeto Estádio Seguro, pelo Ministério da Justiça e Segurança Pública, estariam baseadas, ademais, pelo disposto na Lei nº 13.675/2018, que instituiu o Sistema Único de Segurança Pública (SUSP) e ampliou os objetivos da Política Nacional de Segurança Pública e Defesa Social. Em especial, foram citados os seguintes artigos, com os destaques feitos pelo MJSP:

> Art. 6º São objetivos da PNSPDS:
>
> [...]
>
> I - fomentar a integração em ações estratégicas e operacionais, em atividades de inteligência de segurança pública e em gerenciamento de crises e incidentes;
>
> [...]
>
> **VII - promover a interoperabilidade dos sistemas de segurança pública;**
>
> [...]
>
> **X - integrar e compartilhar as informações de segurança pública, prisionais e sobre drogas;**
>
> [...]
>
> XVII - fomentar ações permanentes para o combate ao crime organizado e à corrupção;
>
> [...]
>
> art. 9º É instituído o Sistema Único de Segurança Pública (Susp), que tem como órgão central o Ministério Extraordinário da Segurança Pública e é integrado pelos órgãos de que trata o art. 144 da Constituição Federal, pelos agentes penitenciários, pelas guardas municipais e pelos demais integrantes estratégicos e operacionais, que atuarão nos limites de suas competências, de forma cooperativa, sistêmica e harmônica.
>
> [...]
>
> § 2º São integrantes operacionais do Susp:
>
> I - polícia federal;
>
> II - polícia rodoviária federal;
>
> III – (VETADO);
>
> **IV - polícias civis;**
>
> **V - polícias militares;**
>
> VI - corpos de bombeiros militares;

> VII - guardas municipais;
>
> VIII - órgãos do sistema penitenciário;
>
> IX - (VETADO);
>
> X - institutos oficiais de criminalística, medicina legal e identificação;
>
> **XI - Secretaria Nacional de Segurança Pública (Senasp);**
>
> **XII - secretarias estaduais de segurança pública ou congêneres;**
>
> XIII - Secretaria Nacional de Proteção e Defesa Civil (Sedec);
>
> XIV - Secretaria Nacional de Política Sobre Drogas (Senad);
>
> XV - agentes de trânsito;
>
> XVI - guarda portuária.

5.4.1.3. A atuação da Diretoria de Operações Integradas e de Inteligência, por meio da Coordenação Geral de Inteligência, ademais, estaria fundamentada em dispositivos do Decreto nº 10.777/2021, Política Nacional de Inteligência de Segurança Pública – PNISP. O apoio às Instituições de Segurança Pública, na exata abrangência que se faz necessário para identificar ameaças, riscos e oportunidades, tanto ao País como à sua população, por sua vez, estaria de acordo com o disposto no Decreto nº 10.778/2021, Estratégia Nacional de Inteligência de Segurança Pública - ENISP. Nesse sentido, foram destacados os seguintes objetivos e diretrizes constantes na PNISP:

> 7. OBJETIVOS
>
> a) acompanhar e avaliar conjunturas de interesse da segurança pública, além de subsidiar o processo decisório e a ação do Estado;
>
> b) identificar fatos ou situações que representem ameaças, riscos ou oportunidades que possam impactar na atuação dos órgãos que integram o Susp;
>
> (...)
>
> e) consolidar a integração dos órgãos de inteligência de segurança pública;
>
> (...)
>
> 8. DIRETRIZES
>
> 8.1 Produzir conhecimento para o enfrentamento da criminalidade organizada e violenta.
>
> A produção de conhecimento pela atividade de inteligência de segurança pública tem como finalidade precípua o enfrentamento à criminalidade.
>
> (...)
>
> 8.2 Aperfeiçoar as inteligências cibernética, financeira e de sinais
>
> Consiste em capacitar profissionais e aprimorar, permanentemente, as técnicas e os meios necessários ao desenvolvimento da atividade de inteligência de segurança pública essenciais à detecção, ao acompanhamento, ao processamento, à produção, ao compartilhamento e à preservação de dados e informações obtidos nas esferas cibernética, financeira e de sinais.
>
> (...)
>
> 8.3 Fomentar a integração da atividade de inteligência de segurança pública
>
> Uma característica importante da atividade de inteligência de segurança pública é o seu alcance.
>
> Um conhecimento completo, abrangente, preciso e oportuno, cujos dados possam ser extraídos de todas as fontes possíveis, com análise do máximo de variáveis implicadas, é o objetivo a ser atingido.
>
> (...)
>
> 8.4 Subsidiar ações de preservação da ordem pública, da incolumidade das pessoas e do patrimônio e do meio ambiente.
>
> A atividade de inteligência de segurança pública exerce papel primordial no processo decisório, com o fornecimento de informações de interesse da segurança pública em todos os seus níveis.
>
> (...)
>
> 8.6 Garantir a proteção aos profissionais de inteligência

5.4.1.4. O controlador, por derradeiro, indicou os desafios, os eixos estruturantes e os objetivos estratégicos previstos na ENISP que, a seu ver, reconheceriam a "*importância da atividade de inteligência*

ao elencar desafios e objetivos estratégicos com destaque ao combate à criminalidades organizada e violenta e ao uso e modernização de ferramentas tecnológicas de ponta", com os destaques abaixo:

> 6. DESAFIOS (...)
>
> 6.1 Fortalecimento da atuação integrada e coordenada dos órgãos e das entidades responsáveis pela atividade de inteligência de segurança pública.
>
> (...)
>
> 6.3 Maior utilização de tecnologias de ponta, especialmente no campo da inteligência tecnológica (...)
>
> 6.4 Intensificação do uso de tecnologias da ciência de dados (...)
>
> (...)
>
> 7. EIXOS ESTRUTURANTES (...)
>
> 7.1 Atuação em rede (...)
>
> 7.2 Tecnologia
>
> O investimento em tecnologias de ponta deve estar sempre presente nas pautas de discussões. O avanço tecnológico no tratamento e na análise de dados permeia e impacta fortemente a atividade de inteligência de segurança pública e potencializa a resposta do trabalho de assessoramento.
>
> O ambiente profissional da atividade de inteligência de segurança pública ainda deve favorecer o compartilhamento de ideias, recursos e experiências, para que se estabeleçam as condições para a inovação e o uso de melhores práticas.
>
> 8. OBJETIVOS ESTRATÉGICOS (...)
>
> 2. identificar e gerenciar os principais processos a serem executados pelos integrantes do Sisp;
>
> (...)
>
> 12. ampliar a capacidade da segurança pública na obtenção de dados por meio da inteligência tecnológica;
>
> (...)
>
> 16. ampliar a capacidade de obtenção e análise de grande quantidade de dados estruturados e não estruturados;
>
> (...)
>
> 28. estabelecer temas prioritários para produção de conhecimento referente à corrupção, à criminalidade organizada, à criminalidade violenta e aos ilícitos interestaduais e transnacionais;

5.4.1.5. Observa-se que o tratamento de dados pelo Poder Público, nos termos do art. 23 da LGPD, tem como pressupostos o atendimento a uma finalidade pública, a persecução do interesse público e a execução pelo ente público de suas competências legais ou cumprimento de suas atribuições. A finalidade pública será atendida quando o poder público realizar o tratamento de dados pessoais dos administrados nos restritos termos da lei, para a execução de políticas públicas previstas na norma ou para o cumprimento de suas atribuições legais, zelando pela proteção de dados da pessoa natural e pela garantia de seus direitos personalíssimos[10].

5.4.1.6. De acordo com Barroso (Barroso, 2015)[11], ao se analisar a incidência do princípio da supremacia do interesse público em determinada relação jurídica, deve-se primeiramente distinguir o interesse público primário do interesse público secundário. O interesse público primário pode ser compreendido como a própria razão de ser do Estado, ou seja, caracteriza-se como os interesses de toda a sociedade, como a promoção da justiça e do bem-estar social. O interesse público secundário, por sua vez, pode ser entendido como a vontade da pessoa jurídica de direito público em determinada relação jurídica.

5.4.1.7. O interesse público primário, assim, que desfrutaria de supremacia em um sistema constitucional e democrático, uma vez que ele não é passível de ponderação, constituindo o próprio parâmetro para a ponderação com outros direitos e garantias fundamentais. O interesse público secundário, por outro lado, ao entrar em aparente colisão com outros bens jurídicos protegidos, deve ser ponderado com base nas condições fáticas e de direito presentes no caso concreto.

5.4.1.8. A execução de competências legais ou atribuições pelo Poder Público, com o objetivo de assegurar o interesse público, desse modo, tem como escopo a investidura legal atribuída aos entes estatais para o cumprimento de um determinado dever, que precede a existência de um poder estatal. Assim, enquanto a finalidade pública impõe aos órgãos e entidades da Administração que o tratamento de dados pessoais seja direcionado à execução de uma política pública ou de missão institucional prevista na norma, o interesse público subjacente e inafastável (interesse público primário) é a preservação dos direitos e das garantias fundamentais do administrado, por se tratar de demanda do bem comum da coletividade[12].

5.4.1.9. A análise das atribuições legais das unidades administrativas do MJSP envolvidas na execução do projeto, portanto, permite concluir que o tratamento de dados pessoais para os propósitos informados, no âmbito do projeto Estádio Seguro, se encontra dentro das competências legais do órgão federal. Do mesmo modo, entende-se que as medidas propostas no projeto Estádio seguro visam, em última análise, a proteção da vida dos frequentadores de eventos esportivos contra ameaças de violação por parte de terceiros (sujeitos de interesse da justiça). Nesse sentido, é razoável presumir que a presença de indivíduos foragidos da Justiça em eventos esportivos pode representar um risco à incolumidade física dos demais cidadãos presentes, o que tornaria legítimo a utilização de ferramentas tecnológicas que permitissem a sua identificação. Dessa forma, o interesse público na ação estatal, à princípio, estaria consubstanciado na dimensão positiva do direito à vida, ou seja, vincular-se-ia à obrigação estatal de desenvolver medidas ativas na proteção da vida dos indivíduos[13].

5.4.1.10. Entende-se, desse modo, que o tratamento dos dados pessoais coletados para a realização do projeto Estádio Seguro está associado a finalidades de interesse público, conforme definido no *caput* pelo art. 23 da LGPD.

5.4.1.11. O MJSP, ademais, argumenta que os arts. 2º, inciso XVI, 144, 146 e 148, 166 e 167 da Lei nº 14.597, de 14 de junho de 2023, Lei Geral do Esporte (LGE), autorizam o tratamento de dados pessoais de torcedores, inclusive por meio da utilização de tecnologia de reconhecimento facial, para a execução do projeto Estádio Seguro. Observe-se, nesse sentido, os dispositivos citados:

> **Lei nº. 14.597, de 14 de junho de 2023**:
>
> Art. 2º São princípios fundamentais do esporte:
>
> (...)
>
> XVI - **segurança.**
>
> (...)
>
> Art. 144. A organização esportiva que administra a competição e a organização de prática esportiva **mandante da partida**, prova ou equivalente, implementarão, na sistematização da emissão e venda de ingressos, **sistema de segurança contra falsificações, fraudes e outras práticas que contribuam para a evasão da receita decorrente do evento esportivo.**
>
> (...)
>
> Art. 146. **O espectador tem direito a segurança nos locais onde são realizados os eventos esportivos antes, durante e após a realização das provas ou partidas.**
>
> (...)
>
> Art. 148. **O controle e a fiscalização do acesso do público** a arena esportiva com capacidade para mais de 20.000 (vinte mil) **pessoas deverão contar com meio de monitoramento por imagem das catracas e com identificação biométrica dos espectadores**, assim como deverá haver central técnica de informações, com infraestrutura suficiente para viabilizar o monitoramento por imagem do público presente e o cadastramento biométrico dos espectadores.
>
> **Parágrafo único. O disposto no caput deste artigo deverá ser implementado no prazo máximo de até 2 (dois) anos a contar da entrada em vigor desta Lei.**
>
> (...)
>
> Art. 166. Vender ou portar para venda ingressos de evento esportivo, por preço superior ao estampado no bilhete:
>
> Pena - reclusão, de 1 (um) a 2 (dois) anos, e multa.

> Art. 167. Fornecer, desviar ou facilitar a distribuição de ingressos para venda por preço superior ao estampado no bilhete:
>
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
>
> Parágrafo único. A pena será aumentada de 1/3 (um terço) até a metade se o agente for servidor público, dirigente ou funcionário de organização esportiva que se relacione com a promoção do evento ou competição, de empresa contratada para o processo de emissão, distribuição e venda de ingressos ou de torcida organizada e se utilizar dessa condição para os fins previstos neste artigo. (Grifos no original).

5.4.1.12. A Lei Geral do Esporte (LGE), no entanto, não definiu regras, procedimentos ou critérios para que as entidades esportivas compartilhem os dados pessoais coletados com órgãos de segurança pública, inclusive para a consecução das finalidades supramencionadas. Assim, em que pese o art. 149, inciso I, da LGE ter definido que a organização esportiva responsável pela realização do evento deverá solicitar ao poder público competente a presença de agentes públicos de segurança, que seriam responsáveis pela segurança dos espectadores dentro e fora dos estádios e dos demais locais de realização de eventos esportivos, a legislação não apontou norma específica que instituísse o uso compartilhado dos dados pessoais dos torcedores com o Poder Público, especialmente para finalidades de segurança pública.

> **Lei nº 14.597, de 14 de junho de 2023**
>
> Art. 149. Sem prejuízo do disposto nos arts. 12, 13 e 14 da Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), a responsabilidade pela segurança do espectador em evento esportivo será da organização esportiva diretamente responsável pela realização do evento esportivo e de seus dirigentes, que deverão:
>
> I - solicitar ao poder público competente a presença de agentes públicos de segurança, devidamente identificados, responsáveis pela segurança dos espectadores dentro e fora dos estádios e dos demais locais de realização de eventos esportivos;

5.4.1.13. A LGE, na verdade, estabeleceu dois tipos de obrigação no que se refere ao tratamento de dados pessoais de torcedores. O art. 148 da LGE, por um lado, determina que o controle e a fiscalização do acesso do público a recinto esportivo com capacidade superior a 20.000 (vinte mil) pessoas deverão ser feitos por meio sistemas de monitoramento por imagem das catracas e com a identificação biométrica dos expectadores. Para isso, as arenas esportivas deverão dispor de centrais técnicas de informações, com infraestrutura suficiente para viabilizar o monitoramento por imagem do público presente e o cadastramento biométrico dos torcedores. Trata-se de uma obrigação legal imposta aos organizadores do evento esportivo.

5.4.1.14. O art. 158, inciso XII, da LGE, por outro lado, estabelece que o cadastramento biométrico se impõe como uma obrigação a todos os espectadores acima de 16 (dezesseis) anos de idade. O cadastramento biométrico, nos termos do parágrafo único do art. 158, torna-se, portanto, condição necessária para o acesso e a permanência do espectador no recinto esportivo, independentemente da forma de seu ingresso, sem prejuízo de outras condições previstas em lei. Trata-se, assim, de uma exigência legal imposta pela Lei Geral do Esporte aos espectadores de eventos esportivos.

> **Lei nº 14.597, de 14 de junho de 2023.**
>
> Art. 158. São condições de acesso e de permanência do espectador no recinto esportivo, independentemente da forma de seu ingresso, sem prejuízo de outras condições previstas em lei:
>
> (...)
>
> XII - para espectador com mais de 16 (dezesseis) anos de idade, estar devidamente cadastrado no sistema de controle biométrico para efeito do art. 148 desta Lei.
>
> Parágrafo único. O não cumprimento das condições estabelecidas neste artigo implicará a impossibilidade de acesso do espectador ao recinto esportivo ou, se for o caso, o seu afastamento imediato do recinto, sem prejuízo de outras sanções administrativas, civis ou penais eventualmente cabíveis.

5.4.1.15. Deve-se sublinhar, igualmente, que as normas da LGE indicadas pelo MJSP referem-se apenas ao tratamento de dados biométricos dos torcedores pelas entidades esportivas organizadoras do evento, sem que seja feita qualquer menção à coleta de atributos biográficos dos torcedores, como é pretendido pelo MJSP.

5.4.1.16. O projeto Estádio Seguro, desse modo, alargaria o escopo de tratamento de dados pessoais autorizado pela Lei Geral do Esporte, indo além da autorização legislativa, pois seria demandado aos clubes de futebol que encaminhassem ao MJSP dados pessoais biográficos dos torcedores, os quais foram coletados em contexto de relação comercial entre os titulares e as entidades esportivas. A utilização desses dados pessoais, a partir do seu uso compartilhado, resultaria em uso secundário para finalidade distinta para a qual eles foram coletados, visto que seriam utilizados em contexto bastante distinto, ou seja, para segurança pública.

5.4.1.17. O uso secundário de dados pessoais está associado ao princípio da finalidade[14] uma vez que a finalidade específica que legitima a coleta de dados pessoais restringe qualquer tratamento adicional, incluindo o seu uso compartilhado com terceiros. Assim, para que um controlador possa compartilhar os dados pessoais com outro agente, que realizará o tratamento para um propósito distinto daquele para o qual ele foi inicialmente coletado, sem o consentimento expresso do titular, é necessário que a nova finalidade seja compatível com a finalidade inicial.

5.4.1.18. A LGPD, porém, não indica critérios claros quanto à forma para se definir a compatibilidade do uso secundário de determinado conjunto de dados pessoais que foram inicialmente coletados para propósitos distintos. Wimmer[15], ao citar Doneda e Viola, destaca que a questão poderia ser resolvida, nos casos concreto, pela aplicação do princípio da proporcionalidade, utilizando-se três critérios: (i) se a utilização do dado não seria abusiva; (ii) se tal uso secundário não ultrapassaria os limites de uso que os titulares pudessem razoavelmente cogitar no momento do fornecimento do dado; e (iii) se haveria interesses relevantes que pudessem sugerir a necessidade de maior elasticidade e tolerância com utilizações mais amplas de dados pessoais.

5.4.1.19. O art. 6(4) da GDPR, no âmbito da experiência europeia, oferece alguns critérios para a definição da compatibilidade no tratamento secundário de dados pessoais. Assim, a norma de proteção de dados pessoais europeia define que a análise da compatibilidade do tratamento deverá observar (i) a possível vinculação existente entre a finalidade inicial e a finalidade secundária; (ii) o contexto em que o dado pessoal foi inicialmente coletado; (iii) a relação entre o titular e o controlador; (iv) a natureza do dado pessoal coletado – dado comum ou sensível -; (v) as possíveis consequências na utilização pretendida do dado pessoal para o titular; e (vi) a existência de salvaguardas apropriadas[16]. De qualquer forma, entende-se que a ideia de ponderação na avaliação da compatibilidade do uso secundário de dados pessoais deve necessariamente perpassar pelas expectativas razoáveis dos titulares, a natureza dos dados pessoais coletados e os possíveis prejuízos aos titulares advindos do tratamento posterior.

5.4.1.20. A avaliação de compatibilidade, de todos os modos, é fundamental para se garantir a legalidade da operação de tratamento. Excepcionalmente, com base na experiência internacional, Wimmer afirma[17] que “seria possível superar a incompatibilidade de finalidades por meio do consentimento do titular ou com base em previsão legal específica, necessária e proporcional, observando-se o pleno respeito aos demais princípios e direitos associados à proteção de dados pessoais”.

5.4.1.21. A necessidade de existência de norma específica que fundamente o tratamento de dados pessoais de terceiros por autoridades públicas, nas áreas de inteligência e segurança pública, já foi verificada em decisões de tribunais internacionais. O Tribunal Europeu de Direitos Humanos (TEDH), no precedente *Rotaru vs Romênia*, em que o serviço de inteligência do governo europeu coletava dados pessoais de um determinado advogado, por exemplo, consignou que a coleta sistemática de informações e dados pessoais de terceiras pessoas, por autoridades públicas, mesmo quando tais informações encontrarem-se dispostas em meios de acesso público, podem representar uma interferência indevida no direito fundamental à vida privada do indivíduo, conforme definido pelo artigo 8º (1) da Convenção Europeia dos Direitos do Homem[18].

5.4.1.22. O TEDH definiu, ainda, que o tratamento de dados pessoais por autoridades públicas deve estar previsto em legislação específica, a qual deve estabelecer critérios mínimos, como o tipo de informação que pode ser tratada, as categorias de pessoas que podem ter seus dados coletados, as circunstâncias nas quais tais medidas podem ser tomadas, as pessoas autorizadas a ter acesso aos dados e os limites da retenção desses dados[19].

5.4.1.23. Pode-se verificar no ordenamento jurídico brasileiro, inclusive, a existência de normas específicas que autorizam o uso compartilhado de dados pessoais para fins de segurança pública e de atividades de investigação e repressão de infrações legais. A Lei nº 13.964/19, Lei Anticrime, por exemplo, que modificou a Lei nº 12.037/09, ao acrescentar que os dados contidos no Banco Nacional Multibiométrico e de Impressões Digitais podem ser acessados por autoridade policial e o Ministério Público, mediante autorização judicial. Observe-se que o legislador optou por estabelecer *reserva de acesso* aos dados pessoais sensíveis contidos na referida base de dados mesmo para autoridades policiais[20].

5.4.1.24. A Lei de Organização Criminosa, Lei nº 12.850/13, por sua vez, permite o acesso por delegados de polícia ou membros do Ministério Público a dados cadastrais de investigados mantidos pela Justiça Eleitoral. O Marco Civil da Internet, Lei nº 12.964/14, a seu turno, autoriza a disponibilização de registros de conexão ou de registros de acesso a aplicações de internet para fins de investigação ou instrução probatória[21].

5.4.1.25. O uso compartilhado dos dados pessoais, no contexto do projeto Estádio Seguro, sem o amparo de legislação específica, apenas com base em instrumentos administrativos ou congêneres, sem as salvaguardas necessárias, poderia infringir o princípio da boa-fé, nos termos do caput do art. 6º da LGPD, pois ampliaria a discricionariedade do Poder Público na coleta de dados pessoais para uso secundário, em prejuízo às expectativas razoáveis do titular.

5.4.1.26. A Lei Geral do Esporte, diante do exposto, não pode ser considerada como norma autorizativa para a transmissão de dados pessoais de torcedores, coletados pelos clubes de futebol, ao Ministério da Justiça e Segurança Pública para fins da consecução dos objetivos do projeto Estádio Seguro. Do mesmo modo, não se verifica uma relação de compatibilidade plena entre as finalidades para as quais os dados pessoais foram coletados pelas entidades esportivas e as finalidades do projeto Estádio Seguro, à luz dos critérios levantados nos itens 5.4.1.18 e 5.4.1.19. Enquanto no primeiro caso os atributos biográficos dos torcedores são coletados para a consecução de uma transação comercial entre o titular e o clube de futebol; no segundo, o tratamento visa objetivos exclusivos de segurança pública e atividades de investigação e repressão de infrações penais, que se encontram apenas de forma limitada sob o escopo da LGPD, no que tange a parte final do art. 4º, § 1º, da LGPD.

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
>
> III - realizado para fins exclusivos de:
>
> a) segurança pública;
>
> (...)
>
> d) atividades de investigação e repressão de infrações penais; ou
>
> § 1º 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***.

5.4.1.27. Não há uma relação direta entre titular e o novo controlador – Ministério da Justiça e Segurança Pública, tampouco entre a finalidade inicial e a finalidade secundária. O contexto em que o dado pessoal é inicialmente coletado, por uma entidade privada e para lazer, é estranho ao contexto da nova finalidade, promovida por um ente público para segurança pública, investigação ou repressão a infrações penais.

5.4.1.28. Observa-se, contudo, que o 4º, § 1º, da LGPD prevê a criação de norma específica que venha a regulamentar o tratamento de dados pessoais nas atividades exclusivas de segurança pública e atividades de investigação e repressão de infrações penais, de maneira a balancear os interesses públicos associados à segurança da população e a proteção da privacidade e demais garantias fundamentais afetadas pelas práticas de monitoramento e vigilância do Estado, ainda que realizadas de forma legítima. O legislador, portanto, optou que o tratamento de dados pessoais em matéria penal tivesse regulamentação própria, em função das peculiaridades das atividades de investigação criminal e manutenção da ordem, aplicando-se a LGPD apenas de maneira limitada.

5.4.1.29. Desse modo, em virtude da inexistência de regulamentação específica sobre a matéria, conforme determinado pelo art. 4º, § 1º, da LGPD, cabe ao MJSP assegurar que o tratamento de dados pessoais no âmbito do projeto Estádio Seguro seja realizado com o estrito cumprimento dos parâmetros definidos para a aplicação das normas de proteção de dados pessoais às exceções do art. 4º, inciso III, alíneas "a" e "d", da LGPD (devido processo legal, observância de princípios gerais de proteção de dados pessoais e garantia do exercício de direitos pelos titulares)[22]. Por esse motivo, a inexistência de legislação específica não confere ampla e irrestrita autorização aos órgãos de segurança para tratarem dados pessoais dos cidadãos para finalidades exclusivas de segurança pública e atividades de investigação e repressão de infrações penais sem quaisquer tipos de limites. Além das restrições apontadas pelo art. 4º, § 1º, da LGPD, as atividades dos órgãos de segurança pública encontram-se limitadas por normas de regime administrativo próprio, baseados em princípios como a legalidade, a moralidade, a transparência e a motivação[23].

5.4.2. ***Sobre o compartilhamento de dados pessoais do MJSP com outras entidades.***

5.4.2.1. O art. 23 da LGPD, como já destacado, dispõe que o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da LAI deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. Para isso, as entidades do Poder Público, além da necessidade de indicar previamente um controlador, precisam informar as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

5.4.2.2. A lógica subjacente das normas de proteção de dados pessoais não possui natureza proibitiva, motivo pelo qual a LGPD não tem como objetivo impedir o fluxo e o tratamento de informações que identifiquem ou venham a identificar as pessoas naturais. Na verdade, a norma estabelece um sistema de regras, princípios e procedimentos, por meio dos quais os agentes de tratamento poderão realizar o tratamento de dados pessoais legitimamente, de maneira que os direitos e garantias fundamentais dos titulares sejam devidamente observados.

5.4.2.3. A LGPD, nesse sentido, ***não veda*** o compartilhamento de dados pessoais entre órgãos da Administração. O art. 26, caput, da LGPD, nesse caso, estabelece que o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais.

5.4.2.4. O Supremo Tribunal Federal (STF), nesse sentido, ao analisar a constitucionalidade do Decreto nº 10.046/2019 da Presidência da República, que dispõe sobre a governança do compartilhamento de dados entre órgãos do Poder Público, no contexto do exame conjunto da Ação Direta de Inconstitucionalidade (ADI 6649) e da Arguição de Descumprimento de Preceito Fundamental (ADPF 695), determinou que o compartilhamento de dados pessoais é possível, desde que observados alguns parâmetros.

5.4.2.5. O voto do Ministro-relator Gilmar Mendes, assim, destacou que o uso compartilhado de dados envolvendo órgãos e entidades governamentais deve cumprir integralmente os requisitos, as garantias e os procedimentos estabelecidos na Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) compatíveis com o setor público. Da mesma maneira, o STF consignou que o compartilhamento de informações pessoais em *atividades de inteligência* deve observar legislação específica e parâmetros fixados no julgamento da ADI 6.529, que limitou o compartilhamento de dados do Sisbin[24], e atender ao interesse público, entre outros.

5.4.2.6. O Guia de tratamento de dados pessoais pelo Poder Público, editado pela ANPD[25], por sua vez, define os principais requisitos que devem ser observados nos processos de compartilhamento de dados pessoais pelo Poder Público, os quais podem ser ajustados ou complementados com parâmetros e requisitos adicionais de acordo com o contexto e as peculiaridades de cada caso concreto.

5.4.2.7. O uso compartilhado de dados pessoais entre órgãos do Poder Público, conforme entendimento da ANPD, deve ser precedido por procedimento formal, em que constem os documentos e as informações pertinentes sobre a operação de tratamento, incluindo análise técnica e jurídica que exponham a motivação para a realização do compartilhamento e a sua aderência à legislação em vigor. Na análise do órgão, deve ficar claro o objeto e as finalidades da operação de tratamento, bem como a hipótese legal que a fundamenta, a sua duração, os requisitos de transparência e a forma como os titulares poderão exercer seus direitos. Do mesmo modo, o controlador deve indicador os requisitos de tratamento inerentes à operação de tratamento, quando for o caso, e os requisitos técnicos e administrativos de segurança dos dados.

5.4.2.8. Uma vez que na primeira versão do RIPD era indicada a existência de compartilhamento entre o MJSP e os órgãos e agentes de segurança pública de outras entidades federativas, a ANPD questionou a existência de procedimentos formais que cumprissem os requisitos legais e procedimentais necessários para se verificar a legitimidade do uso compartilhado de dados.

5.4.2.9. A versão 2.0 do RIPD, desse modo, indica que um dos objetivos do projeto Estádio Seguro é auxiliar as *polícias estaduais* na identificação de pessoas procuradas pela justiça, torcedores com ordem judicial de afastamento, bem como na verificação de envolvidos em atos de violência, racismo, xenofobia, LGBTfobia e violação das regras de segurança praticados no período que antecede. Da mesma maneira, informa-se que todas as ações previstas no projeto serão em apoio aos serviços de inteligência das Unidades da Federação, por meio da Plataforma Córtex, conforme as normas da Portaria Ministerial nº 218, de 29 de setembro de 2021.

5.4.2.10. O controlador, por conseguinte, explicou que a Plataforma Córtex se faz presente "em todas as forças de segurança estaduais, por meio de pactuação do Acordo de Cooperação entre a União com aqueles Órgãos da Segurança Pública", constituindo importante ferramenta para a segurança pública. O uso compartilhado de dados pessoais, por meio da Plataforma Córtex, no contexto do compartilhamento de informações de inteligência entre órgãos de segurança pública de entres federativos, estaria dentro das atribuições legais do Ministério da Justiça e Segurança, sendo previstos na Política Nacional de Inteligência de Segurança Pública PNISP (Decreto nº 10.777/21) e na Estratégia Nacional de Inteligência de Segurança Pública - ENISP (Decreto nº 10.778/21), conforme já explicado no item 5.4 desta Nota Técnica.

5.4.2.11. Consta, da mesma maneira, que profissionais das agências de inteligência estaduais, devidamente autorizados, terão acesso a dados de identificação dos sujeitos de interesse da justiça durante a fase de consciência situacional (etapa 1). Os agentes públicos estaduais, desse modo, "terão permissão para acessar e visualizar a lista prévia contendo os indivíduos identificados como de interesse para a segurança pública no respectivo evento".

5.4.2.12. Tem-se, por conseguinte, que os profissionais da segurança pública estaduais terão acesso ao subsistema modular Estádio Seguro na Plataforma Córtex. Esses profissionais, no entanto, conforme consta no item 14.0.1. da versão 2.0 do RIPD (SEI nº 0048206), deverão assinar um Termo de Compromisso de Manutenção de Sigilo (TCMS), visto que os documentos gerados serão classificados em algum grau de sigilo, nos termos da Lei nº 12.527/2011, Lei de Acesso à Informação – LAI.

5.4.2.13. A minuta do protocolo de execução, em sua cláusula quinta, inciso VI, alíneas "a" e "b", a seu turno, restringe o acesso ao subsistema modular Estádio Seguro na Plataforma Córtex a usuários devidamente identificados em cada acesso, os quais serão autenticados e autorizados mediante a assinatura de um Termo de Compromisso e Manutenção do Sigilo (TCMS) pelo agente público estadual. Assim, além dos membros da Coordenação Geral de Inteligência (CGINT) envolvidos na atividade de inteligência e monitoramento da execução do Projeto Estádio Seguro, terão acesso ao sistema os *agentes estaduais* que atuam em atividades de inteligência em segurança pública nos estádios de futebol, *desde que haja um instrumento de formalização vigente*, em conformidade com a política de governança de dados estabelecida pelo Ministério.

5.4.2.14. Observa-se, portanto, que haverá, no âmbito do projeto Estádio Seguro, o tratamento compartilhado, por órgãos e entidades públicos, de dados e informações contidos em bancos de dados pessoais. O uso compartilhado de dados pessoais, por meio da Plataforma Córtex, porém, será realizado apenas com agentes públicos de entidades federativas devidamente conveniadas, os quais deverão

assinar previamente Termo de Compromisso e Manutenção do Sigilo (TCMS), nos termos da Portaria Ministerial nº 218, de 29 de setembro de 2021, e de acordos de cooperação específicos firmados com órgãos de segurança de outras unidades da federação.

5.4.2.15. Além desses requerimentos, é importante destacar, conforme já exposto no item 5.177 da Nota Técnica nº 175/2023/CGF/ANPD, que os órgãos públicos que terão acesso ao subsistema modular Estádio Seguro, na Plataforma Córtex, por meio de seus agentes devidamente credenciados, precisarão comprovar a necessidade do tratamento dos dados pessoais, o que deverá ser precedido pela demonstração de que há, de fato, um devido processo legal e respeito aos princípios e direitos dos titulares, conforme previsão da legislação.

5.4.2.16. O Ministério da Justiça e Segurança Pública, nesse sentido, nos termos do inciso VIII, da cláusula quinta do protocolo de execução, deve responsabilizar-se por acompanhar minuciosamente a execução da parceria, bem como assegurar o cumprimento das cláusulas estabelecidas no instrumento contratual e na legislação aplicável, como a LGPD. Desse modo, cabe ao MJSP verificar se as entidades públicas estatais cumprem todos os requisitos legais e procedimentais necessários para a realização do tratamento de dados necessários à consecução das finalidades do projeto.

5.4.2.17. Verifica-se, ademais, que durante a fase de consciência situacional, por meio de API[26] com a Plataforma Córtex, haverá o cruzamento dos dados pessoais encaminhados pelas entidades esportivas com bases de verificação disponibilizadas ao MJSP por outros órgãos públicos, como o Tribunal Superior Eleitoral (TSE), a Receita Federal do Brasil (RFB), o Departamento Nacional de Trânsito (DENATRAN) e do Serviço Federal de Processamento de Dados (Serpro). O MJSP, no entanto, não prestou maiores informações quanto à existência de acordos de cooperação ou de instrumentos legais que permitam o reúso dessas bases de dados para finalidades distintas daquelas para as quais os dados que as compõem foram inicialmente coletados.

5.4.2.18. A inexistência de instrumentos legais que indiquem a possibilidade de reutilização de dados pessoais coletados em função de obrigação legal, para finalidades de segurança pública, pode ensejar na inobservância da legítima expectativa dos titulares. Nesse sentido, o princípio da boa-fé no tratamento dos dados pessoais (art. 6º, *caput*, LGPD), de modo a garantir a transparência no uso conferido às informações repassadas pelos titulares e a lealdade no tratamento de dados, impõe às autoridades públicas uma regra de conduta que se vincula, em certa medida, às legítimas expectativas dos titulares de dados, como uma forma de se evitar qualquer tipo de abuso, lesão ou desvantagem[27]. Fica o MJSP alertado para que os instrumentos de formalização de compartilhamento de dados pessoais dessas entidades públicas - TSE, RFB, Serpro e Denatran - com o MJSP precisam estar atualizados ou adaptados aos termos da LGPD e orientações da ANPD, a exemplo do Guia de Tratamento de Dados pelo Poder Público.

5.4.2.19. No que se refere à possibilidade de tratamento compartilhado de dados pessoais com os clubes de futebol, o controlador afirma que não haverá a transmissão de dados ou de informações pessoais adicionais com a entidade privada esportiva responsável pela coleta inicial dos dados.

5.4.2.20. De acordo com o MJSP, haverá apenas o compartilhamento dos códigos de bloqueio das catracas, gerados pela Plataforma Córtex, após a identificação das pessoas de interesse da justiça, que serão encaminhados aos estádios, na fase de “alertas gerais”. Os códigos encaminhados pelo MJSP determinarão o bloqueio da catraca associada ao ingresso, que estará vinculado ao CPF do indivíduo de interesse, mantendo-se a *ticketeira* e o estádio alheios à natureza específica da situação (item 17.10 do RIPD 2.0, SEI nº 0048206). As entidades privadas, assim, não teriam acesso à API da Plataforma Córtex, medida que serviria para garantir a privacidade dos titulares e a segurança do próprio sistema.

5.4.2.21. O período de retenção dos códigos de bloqueio pelas entidades esportivas, por sua vez, deverá ocorrer nos termos dispostos no inciso XXIII da cláusula sétima do protocolo de execução, conforme abaixo:

> 7. CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DAS ORGANIZAÇÕES DE PRÁTICAS DESPORTIVAS MANDANTE DA PARTIDA, PROVA OU EVENTOS CORRESPONDENTES
>
> (...)

> XXIII - Realizar, de forma concomitante ao encerramento da partida, a efetiva eliminação de todos os códigos de bloqueio previamente fornecidos pelo MJSP, indispensáveis para o adequado funcionamento do mecanismo de travamento das catracas, essencial para a identificação de indivíduos de interesse da segurança pública;

5.4.2.22. Esse protocolo, segundo o MJSP, visa garantir que a API e os dados pessoais não sejam acessíveis a outras entidades e instituições públicas, de maneira a manter a confidencialidade e a integridade dos dados em conformidade estrita com as diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD).

5.4.2.23. Percebe-se, no entanto, que a redação do eixo XI do Plano de Trabalho do Acordo de Cooperação, não foi reajustada para que expressamente constasse no documento que a cooperação com as entidades esportivas para a criação da base nacional de torcedores se daria pelo compartilhamento "*da relação de associados e membros, sócio-torcedores, membros de torcidas organizadas e torcedores com acessos impedidos às áreas desportivas*". Na minuta do projeto de execução encaminhado pelo controlador, especialmente na cláusula sétima, item X, no entanto, consta obrigação para que as organizações de práticas desportivas cooperem na criação da base nacional de torcedores com ordem de afastamento dos estádios:

> 7. CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DAS ORGANIZAÇÕES DE PRÁTICAS DESPORTIVAS MANDANTE DA PARTIDA, PROVA OU EVENTOS CORRESPONDENTES
>
> (...)
>
> X - Cooperar para a criação de uma base nacional de torcedores com ordem judicial de afastamento dos estádios, visando estabelecer um sistema abrangente e integrado de informações, em especial junto ao Conselho Nacional de Justiça;

5.4.2.24. A obrigação supracitada, ademais, encontra-se em consonância com o disposto na cláusula quarta do mesmo instrumento legal, que trata sobre os objetivos do projeto Estádio Seguro:

> 4. CLÁUSULA QUARTA – DA CONSECUÇÃO FINALÍSTICA
>
> 4.1. A consecução finalística do Projeto Estádio Seguro é o fortalecimento da política nacional de combate ao desaparecimento de pessoas e o aprimoramento dos mecanismos de segurança pública empregados durante o acesso aos estádios e suas imediações, abrangendo os períodos prévio, durante e posterior aos eventos, com a finalidade de auxiliar as polícias estaduais na identificação de pessoas procuradas pela justiça, torcedores com ordem judicial de afastamento e na localização de pessoas desaparecidas, bem como na verificação de envolvidos em atos de violência, racismo, xenofobia, LGBTfobia e violação das regras de segurança, para além de identificação de veículo roubado, furtado e proprietário desse bem procurado pela justiça.

5.4.2.25. Diante do exposto, acredita-se que o MJSP tenha prestado informações detalhadas sobre o compartilhamento de dados com as entidades esportivas. O MJSP, contudo, não indicou qual seria a norma específica que justificaria a criação de eventual base de dados de torcedores impedidos de adentrar estádios de futebol.

5.5. **Da observação dos princípios gerais de tratamento de dados pessoais.**

5.5.1. *Do princípio da finalidade.*

5.5.1.1. Para que o tratamento de dados pessoais pelo Poder Público seja considerado legítimo, entretanto, não basta que a operação esteja vinculada a uma hipótese legal específica (obrigação legal, execução de políticas públicas etc.), mas ela precisa estar em consonância com os princípios gerais de tratamento de dados pessoais.

5.5.1.2. Os princípios gerais de tratamento de dados pessoais, inscritos no art. 6º da LGPD, além de incidirem diretamente no tratamento de dados pessoais, também podem ser considerados como vetores interpretativos para se definir o verdadeiro alcance das normas previstas na LGPD[28]. O princípio da finalidade, nesse contexto, pode ser considerado com o fundamento basilar da proteção de dados, uma vez que é requisito para a maioria dos outros requerimentos legais relacionados ao tratamento de dados[29].

5.5.1.3. O tratamento de dados pessoais, de acordo com o princípio da finalidade, deverá ocorrer apenas para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de

tratamento posterior que seja incompatível com as finalidades informadas ao titular. As finalidades para o tratamento de dados pessoais devem ser definidas desde o início da operação, a partir da coleta dos dados pessoais. Além disso, deve-se considerar ilegal o tratamento de dados para finalidades indefinidas e indeterminadas, pois essa situação impediria que o escopo do tratamento de dados fosse corretamente delineado pelo titular[30].

5.5.1.4. *O MJSP, desse modo, deve restringir a coleta, o tratamento e o armazenamento de dados pessoais, no âmbito do projeto Estádio Seguro, apenas às finalidades específicas informadas ao titular.* A menção à utilização dos dados para finalidades genéricas, como garantir a segurança do indivíduo ou para a realização de atividades de inteligência em segurança pública, devem ser evitadas, sob o risco de desrespeito ao princípio da finalidade.

5.5.1.5. O projeto Estádio Seguro, conforme a primeira versão do RIPD, analisada pela Nota Técnica nº 175/2023/CGF/ANPD, teria três *finalidades específicas* (i) recapturar indivíduos com mandado de prisão ou medidas penais restritivas; (ii) auxiliar na recuperação de veículos roubados ou furtados; e (iii) evitar a venda de ingressos utilizando dados de pessoas falecidas, combatendo-se o "cambismo", de modo a identificar ameaças, riscos e oportunidades, tanto ao país como à sua população.

5.5.1.6. A análise da Nota Técnica nº 175/2023/CGF/ANPD compreendeu que, na primeira versão do RIPD, a existência de base legal que justificaria o tratamento de dados pessoais para o combate ao "cambismo" não estava suficientemente clara no documento encaminhado à CGF.

5.5.1.7. Por esse motivo, determinou-se ao MJSP que ajustasse o RIPD, de modo a deixar evidente que o combate ao "cambismo" se referiria às condutas tipificadas como crimes nos art. 166 e 167 da Lei nº 14.597/2023. Como essa finalidade não estava inequivocadamente associada a uma atribuição legal do órgão público, o RIPD deveria, ao menos, esclarecer as razões de interesse público que justificariam o tratamento dos dados coletados para essa finalidade; explicitar a eventual competência do MJSP na consecução desse interesse; e justificar o tratamento de dados para essa finalidade com base no art. 4º, III, da LGPD, e não em outra hipótese legal.

5.5.1.8. A relação direta entre a finalidade de tratamento de dados pessoais para o combate ao "cambismo", isto é, a aquisição de ingressos para eventos esportivos por meios fraudulentos, e uma atribuição legal específica foi esclarecida no item 12.2. da versão 2.0. do RIPD. Nesse sentido, o documento passou a definir explicitamente que o tratamento de dados para a finalidade supramencionada estaria legitimado pelo disposto nos artigos 166 e 167 da Lei nº 14.597/2023[31]. O MJSP, por conseguinte, contextualizou a prática do "cambismo", ao explicar que ela está associada ao uso de CPF pertencente a indivíduos falecidos e a CPF inexistentes ou fictícios. Os "cambistas", desse modo, lucrariam com a venda de bilhetes, infringindo os artigos 166 e 167 da Lei nº 14.597/2023.

5.5.1.9. A versão 2.0. do RIPD, portanto, sanou a incompatibilidade apontada pela Nota Técnica nº 175/2023/CGF/ANPD, ao vincular a finalidade específica de combate ao "cambismo" a obrigação legal prevista em lei. Do mesmo modo, o MJSP procurou deixar evidente as razões de interesse público que fundamentariam o tratamento de dados para essa finalidade e a competência do órgão público na consecução dessa finalidade.

5.5.1.10. Nota-se, entretanto, que a versão 2.0. do RIPD, além das três finalidades supramencionadas, trouxe maior detalhamento dos propósitos para o tratamento de dados abrangido pelo projeto Estádio Seguro. Nesse sentido, a versão 2.0. do RIPD passou a identificar as seguintes finalidades específicas para o tratamento de dados pessoais:

i. Identificação e recaptura de indivíduos com mandado de prisão em aberto e aplicação de medidas judiciais;

ii. Localização de pessoas maiores de idade registradas como desaparecidas;

iii. Identificação de torcedores que estão sujeitos a medidas judiciais restritivas, tais como a proibição de frequentar estádios, com o objetivo de aplicar as referidas medidas judiciais;

iv. Identificação da utilização indevida de dados de pessoas falecidas para a retirada de bilhetes e sua posterior revenda a preços elevados (cambismo);

v. Combate à falsidade ideológica, por meio da identificação de inconsistências entre o CPF e a fotografia do torcedor, no intuito de prevenir que indivíduos procurados e impedidos adquiram ingressos utilizando CPF inexistentes e informações fictícias;

vi. Identificação e recuperação de veículos roubados ou furtados que adentrarem os estádios;

vii. Identificação e recaptura de proprietários de veículos procurados pela justiça; e

viii. Identificação de autores de delitos relacionados ao evento esportivo, como atos de violência, racismo, xenofobia, LGBTfobia e violação das regras de segurança praticados no período que antecede, coincide e prossegue após a partida.

5.5.1.11. As finalidades específicas para o tratamento de dados pessoais, conforme definidas na versão 2.0 do RIPD, portanto, encontram-se dentro das competências legais do órgão federal. Desse modo, entende-se que o tratamento dos dados pessoais relacionado ao projeto Estádio Seguro está associado a finalidades de interesse público, conforme definido no *caput* pelo art. 23 da LGPD.

5.5.2. *Dos princípios da adequação e da necessidade.*

5.5.2.1. O princípio da adequação (art. 6º, inciso II, LGPD) determina que as operações de tratamento de dados pessoais devem ser compatíveis com as finalidades informadas ao titular, de acordo com o contexto do tratamento. A adequação, desse modo, refere-se à justa expectativa que o titular tem quanto ao tratamento que é dispensado a seus dados pessoais, sendo vedado ao Poder Público o uso de dados pessoais além do esperado pelo titular.

5.5.2.2. O princípio da necessidade (art. 6º, inciso III, LGPD), por seu turno, disciplina que a coleta de dados pessoais deve se restringir ao mínimo necessário para a consecução das finalidades para as quais os dados foram coletados inicialmente. Os dados pessoais coletados pelo controlador, portanto, devem ser relevantes para o tratamento informado, se limitar ao estritamente necessário, bem como devem ser armazenados pelo menor tempo possível[32].

5.5.2.3. A versão 2.0 do RIPD mostra-se mais completa e descritiva que a sua primeira versão, uma vez que identifica todos os dados pessoais que serão coletados junto às entidades esportivas, relacionando-os à cada finalidade de tratamento, às bases de dados utilizadas para a verificação da identidade das pessoas de interesse e aos níveis de atualização dos dados pessoais coletados. Do mesmo modo, o documento esclarece a necessidade de cada conjunto de dados pessoais coletados, para a consecução dos objetivos de interesse público do projeto Estádio Seguro. A tabela abaixo, dessa maneira, indica de forma específica quais dados pessoais serão coletados, bem como a base de dados de origem da coleta, a entidade emissora e o nível de atualização da base de dados.

BASE DE ORIGEM	**ENTIDADE DE ORIGEM E ATUALIZAÇÃO**	**IDENTIFICAÇÃO DOS DADOS MÍNIMOS E NECESSÁRIOS REPASSADOS AO MJSP PELAS ENTIDADES DESPORTIVAS E AQUELES INTERNALIZADOS NA INFRA DO MJSP**
VENDAS DE BILHETES [somete para maior idade]	Entidade Desportiva - Ticketeira [Atualização a Cada Partida]	CPF (dado primário), nome completo, data de nascimento e foto, assento, setor e portão de acesso, número do pedido, número do bilhete*, tipo da compra, data e hora da compra.
ACESSO DE TORCEDOR [somete para maior idade]	Entidade Desportiva - Ticketeira [Em tempo real a Cada Partida]	Número do bilhete* registrado na catraca, data e hora do registro, número e localização da catraca. [dados e informações são utilizados para o tratamento na API do Córtex, todavia ele só se torna efetivamente visíveis na Plataforma Córtex (Figura 3, SEI MJ Nº 26132298) somente para os indivíduos de interesse da segurança pública].

LEITURA E REGISTRO DE PLACA	Entidade Desportiva - Ticketeira/Estádio [Em tempo real a Cada Partida]	Foto da placa do veículo (dado primário), local de acesso, sentido, horário do registro, latitude e longitude.
VERIFICAÇÃO (Pessoa) [somete para maior idade]	BNMP-CNJ 2.0 e 3.0 [Atualização Diária]	CPF (dado primário), Nome, Data de nascimento, Nome da mãe, Data de expedição do MP, Tipificação, Status da peça, Nº do processo, Fórum/Vara/UF, Data de validade do MP, Link da peça.
	BOPC-SINESP [Atualização Diária]	CPF (dado primário), Nome, Data de nascimento, Nome da mãe, Nº boletim de ocorrência, UF do desaparecimento, Município do desaparecimento, Delegacia de Registro, Data do desaparecimento, Hora do desaparecimento, Link da ocorrência.
	SIRC [Atualização Variável Dependente de Cada Cartório]	CPF (dado primário), Nome, Natureza [óbito], Data do registro.
	SERPRO [Atualização Diária] TSE [Atualização no Recadastramento]	CPF (dado primário) e Foto.
	RFB [Atualização Anual]	CPF (dado primário), Nome, Data de nascimento, Nome da mãe.
VERIFICAÇÃO (Veículo)	SENATRAN [Atualização Diária]	CPF (dado primário), Nome do proprietário, placa, chassi, renavam, nº do motor, registro de roubo e furto veicular.
	BOPC-SINESP [Atualização Diária]	CPF (dado primário), Registro de roubo e furto e Nome do proprietário.[33]

5.5.2.4. A versão 2.0. do RIPD, ademais, busca explicar que os dados pessoais coletados, a partir da comercialização dos ingressos, quando verificados com as bases de dados em posse do órgão público, por meio de processamento realizado na API da Plataforma Córtex, *"proporcionará os indicativos necessários para a identificação e a localização de indivíduos de interesse para a segurança pública*", conforme a tabela apresentada logo abaixo:

<table>
<tr><th colspan="2">INDICATIVOS</th><th>FINALIDADE</th></tr>
<tr><td colspan="2">Pessoa Procurada
[bloqueio realizado na catraca]</td><td rowspan="2">Identificação e recaptura de indivíduos com mandado de prisão em aberto e aplicação das medidas judiciais.</td></tr>
<tr><td>Origem dos Dados para Cruzamento: Base de Vendas de Maiores de Idade - Entidade Desportiva - Ticketeira [Atualização a Cada Partida]
Dado Primário: CPF.</td><td>Base(s) de Verificação: BNMP-CNJ 2.0 e 3.0 [Atualização Diária]
Dados BNMP: CPF, Nome, Data de nascimento, Nome da mãe, Data de expedição do MP, Tipificação, Status da peça, nº</td></tr>
</table>

Dados Secundários: nome completo, data de nascimento e foto. **Dados Complementares**: assento, setor e portão de acesso, número do pedido e do bilhete, tipo da compra, data e hora da compra, número do bilhete registrado na catraca, data e hora do registro, número e localização da catraca.	do processo, Fórum/Vara/UF, Data de validade do MP, Link da peça.	
Pessoa Desaparecida [bloqueio realizado na catraca]		Localização de pessoas maiores de idade registradas como desaparecidas.
Origem dos Dados para Cruzamento: Base de Vendas de Maiores de Idade - Entidade Desportiva - Ticketeira [Atualização a Cada Partida] **Dado Primário:** CPF. **Dados Secundários:** nome completo, data de nascimento e foto. **Dados Complementares:** assento, setor e portão de acesso, número do pedido e do bilhete, tipo da compra, data e hora da compra, número do bilhete registrado na catraca, data e hora do registro, número e localização da catraca.	**Base(s) de Verificação**: BOPC-SINESP [atualização diária] e SERPRO [atualização diária] **Dados BOPC-SINESP**: CPF, Nome, Data de nascimento, Nome da mãe, nº boletim de ocorrência, UF do desaparecimento, Município do desaparecimento, Delegacia de Registro, Data do desaparecimento, Hora do desaparecimento, Link da ocorrência.	
Torcedor Impedido [bloqueio realizado na catraca]		Verificação dos torcedores que estão sujeitos a medidas judiciais restritivas, tais como a proibição de frequentar estádios, com o objetivo de aplicar as referidas medidas judiciais.

Origem dos Dados para Cruzamento: Base de Vendas de Maiores de Idade - Entidade Desportiva - Ticketeira [Atualização a Cada Partida] **Dado Primário**: CPF. Dados Secundários: nome completo, data de nascimento e foto. **Dados Complementares**: assento, setor e portão de acesso, número do pedido e do bilhete, tipo da compra, data e hora da compra, número do bilhete registrado na catraca, data e hora do registro, número e localização da catraca.	**Base(s) de Verificação**: BNMP-CNJ 3.0 [Atualização Diária] **Dados BNMP**: Nome, CPF, Data de nascimento, Nome da mãe, Data de expedição do MP, Tipificação, Status da peça, nº do processo, Fórum/Vara/UF, Data de validade do MP, Link da peça.	
Pessoa Falecida [bloqueio realizado na venda]		No âmbito do combate ao cambismo, realiza-se a prevenção da utilização indevida de dados de pessoas falecidas para a retirada de bilhetes e sua posterior revenda a preços elevados. Tal medida encontra respaldo nos artigos 166 e 167 da Lei nº 14.597/2023. Além disso, essa abordagem visa evitar que indivíduos procurados e impedidos adquiram ingressos utilizando CPFs de pessoas falecidas, com o intuito de adentrarem nos estádios.
Origem dos Dados para Cruzamento: Base de Vendas de Maiores de Idade - Entidade Desportiva - Ticketeira [Atualização a Cada Partida] **Dado Primário**: CPF	**Base(s) de Verificação**: SIRC [Atualização Variável Dependente de Cada Cartório] **Dados SIRC:** CPF, Nome, Natureza [óbito], Data do registro.	
Divergência CPF e Fotografia [bloqueio realizado na venda]		No combate à falsidade ideológica, é realizada a identificação de inconsistências entre o CPF e a fotografia do torcedor. Essa medida visa prevenir que indivíduos procurados e impedidos adquiram ingressos utilizando CPF inexistentes e informações fictícias, com o intuito de ingressarem nos estádios.
Origem dos Dados para Cruzamento: Base de Vendas de Maiores de Idade - Entidade Desportiva - Ticketeira [Atualização a Cada Partida] **Dados Primários:** CPF e Foto.	**Base(s) de Verificação**: SERPRO [Atualização Diária] e TSE [Atualização no Recadastramento] **Dado SEPRO e TSE**: Foto.	
Proprietário Procurado [**NÃO** há bloqueio na cancela]		A identificação e recaptura de proprietários de veículos procurados pela justiça segue uma

Origem dos Dados para Cruzamento: Base de Leitura proprietário, em vez de utilizar diretamente o CPF. e Registro de Placa - Entidade Desportiva - Ticketeira e Estádio [Atualização a Cada Partida] **Dados Primários:** Foto da Placa do Veículo. **Dados Secundários:** Local de acesso, sentido, horário do registro, latitude e longitude.	**Base(s) de Verificação**: BNMP-CNJ 2.0 e 3.0 [Atualização Diária], SENATRAN [Atualização Diária] e RFB [Atualização Anual] **Dados BNMP:** CPF, Nome, Data de nascimento, Nome da mãe, Data de expedição do MP, Tipificação, Status da peça, nº do processo, Fórum/Vara/UF, Data de validade do MP, Link da peça. **Dados SENATRAN**: CPF e nome do proprietário, placa, chassi, renavam, nº do motor, registro de roubo e furto veicular	prática semelhante àquela empregada para pessoas procuradas. Nesse contexto, utiliza-se a placa do veículo como dado principal, o qual está vinculado ao CPF do proprietário, em vez de utilizar diretamente o CPF.
Veículo Roubado ou Furtado [**NÃO** há bloqueio na cancela]		Identificação e recuperação de veículos roubado ou furtado que adentrarem os estádios.
Origem dos Dados para Cruzamento: Base de Leitura e Registro de Placa - Entidade Desportiva - Ticketeira e Estádio [Atualização a Cada Partida] **Dados Primários:** Foto da Placa do Veículo. **Dados Secundários:** Local de acesso, sentido, horário do registro, latitude e longitude.	**Base de Verificação**: SENATRAN [Atualização Diária] e BOPC-SINESP [Atualização Diária] **Dados SENATRAN:** CPF e nome do proprietário, placa, chassi, renavam, nº do motor, registro de roubo e furto. veicular. **Dados BOPC-SINESP**: Registro de roubo e furto.	
Autores de Atos de Violência, Racismo, Xenofobia, LGBTfobia e Violação das Regras de Segurança [**NÃO** há bloqueio na cancela]		Identificação de autores de delitos relacionados ao evento esportivo praticado antes, durante ou após a partida de futebol.[34]
Origem dos dados para cruzamento: imagens provenientes de televisões, câmeras de vigilância dos estádios e das redes sociais (somente para maiores de idade).	**Base(s) de Verificação**: SERPRO [Atualização Diária], TSE [Atualização no Recadastramento] e RFB [Atualização Anual] **Dado SEPRO e TSE**: Foto e CPF. **Dados RFB**: Nome, CPF, Data de nascimento, Nome da mãe.	

5.5.2.5. O item 15.6 da versão 2.0. do RIPD, por conseguinte, procurou justificar a necessidade da coleta dos dados pessoais no âmbito do projeto, de maneira a indicar a compatibilidade do tratamento com os propósitos informados ao titular, conforme descrito a seguir:

> *a) **"CPF, nome completo, data de nascimento, foto**: esses elementos de identificação desempenham um papel fundamental na autenticação da identidade do portador do ingresso. Esta autenticação é essencial para garantir que a pessoa presente no evento é aquela que adquiriu o bilhete, assegurando a veracidade dos dados. No escopo do Projeto Estádio Seguro, essa autenticação está*

diretamente relacionada à segurança pública, uma vez que a correta identificação dos espectadores possibilita a prévia identificação e o acompanhamento, durante o acesso, de indivíduos de interesse para as autoridades de segurança. Ademais, esses dados propiciam a detecção do uso de CPF de pessoas falecidas ou informações fictícias para aquisição de ingressos, uma prática que demanda atenção especial.

b) ***Assento, setor e portão de acesso:*** *Essas informações, vinculadas exclusivamente aos indivíduos de interesse da segurança pública, complementam e contribuem para a estratégia operacional de inteligência em segurança pública. A identificação precisa do local de assento, setor e portão de acesso possibilita o eficiente monitoramento e a localização das pessoas de interesse durante o evento, promovendo uma abordagem mais assertiva e focada.*

c) ***Número do pedido e do bilhete, tipo da compra, data e hora da compra:*** *esses dados oferecem aos profissionais de inteligência, na sala de triagem, meios para verificar a autenticidade do bilhete, permitindo a comunicação com a entidade responsável pela venda de ingressos para esclarecimento de situações duvidosas. O tipo da compra, indicando o canal de aquisição, seja online, presencial ou por revendedores autorizados, garante a conformidade com métodos legítimos de obtenção de ingressos. A data e hora da compra, por sua vez, possibilitam o rastreamento temporal das transações, auxiliando na detecção de atividades suspeitas ou irregulares, bem como verificando qualquer inconsistência no acesso do torcedor ao estádio.*

d) ***Número do bilhete:*** *o número do bilhete assume um papel de suma importância ao estabelecer a conexão entre o CPF do indivíduo e o procedimento de bloqueio na catraca. Esse número é atribuído ao torcedor no momento da aquisição do bilhete e, juntamente com os demais dados, é encaminhado ao MJSP pela ticketeira, estando vinculado ao CPF do comprador ou beneficiário do bilhete. Quando o MJSP recebe da ticketeira a relação de dados dos torcedores para um evento específico e identifica, com base no CPF, a presença de um indivíduo procurado, impedido ou desaparecido, é gerado um código de bloqueio que é posteriormente repassado à ticketeira, conforme detalhado no presente relatório. Esse código de bloqueio é devolvido à ticketeira em conjunto com o número do bilhete, evitando a exposição da circunstância ao titular do CPF. Em outras palavras, o código de bloqueio é devolvido para a ticketeira juntamente com o número do bilhete, ao qual está vinculado o CPF pertencente a uma pessoa procurada, impedida ou desaparecida, evitando a exposição de tal informações para a ticketeira, ainda que eles possuam o vínculo CPF-Nº do bilhete em suas bases.*

e) ***BNMP-CNJ 2.0 e 3.0, BOPC-SINESP, SENATRAN, RFB, TSE, SERPRO e SIRC (Bases de Verificação integradas na infraestrutura do MJSP):*** *essas bases de verificação constituem um conjunto de informações relevantes para analisar a situação social, legal, restritiva e criminal dos torcedores, contribuindo para uma avaliação abrangente e embasada na segurança pública.*

1. Destarte, o BNMP-CNJ 2.0 e 3.0 assume destacada importância ao indicar, de maneira inequívoca, se determinada pessoa encontra-se com o mandado judicial em aberto ou, ainda, se está proibida de acessar recintos desportivos. Por sua vez, o BOPC-SINESP desvela-se como instrumento de fundamental importância para informar sobre a condição de desaparecimento de indivíduos, além de fornecer subsídios relativos a eventuais registros de roubo ou furto de veículos, quando aplicável.

2. No domínio do tráfego automotivo, o SENATRAN destaca-se ao efetuar a vinculação do CPF do proprietário do veículo à respectiva placa automotiva, conferindo, dessa maneira, a capacidade de identificar proprietários procurados, adicionando, ademais, informações acerca de registros de subtração veicular. Em paralelo, a Receita Federal do Brasil (RFB) desempenha papel crucial ao permitir que os dados individuais sejam enriquecidos com informações pertinentes à inteligência e aos processos investigativos, tais como endereço residencial e nome da mãe.

3. Por sua vez, o SERPRO e o Tribunal Superior Eleitoral (TSE), detentores de bases imagéticas correlacionadas aos dados dos titulares, constituem ferramentas singulares que possibilitam, juntamente com as demais bases (de venda, de acesso e de verificação) identificar os autores de atos de violência, racismo, xenofobia, LGBTfobia e violação das regras de segurança. Ademais, o SIRC destaca-se ao evidenciar a vital condição de um CPF, indicando se pertence a uma pessoa falecida, conferindo assim maior precisão na verificação da identidade.

f) Nº do bilhete registrado na catraca, data e hora do registro, número e localização da catraca: *o número do bilhete registrado na catraca, juntamente com a data e hora do registro, bem como ao número e à localização específica da catraca, concede aos profissionais de inteligência em segurança pública a capacidade de receber, em tempo real e na interface do Córtex, alertas que evidenciam a presença do indivíduo de interesse em um portão e catraca específicos naquele instante. Esses dados e funcionalidade possibilita um direcionamento preciso das ações de segurança pública, fortalecendo a eficácia das intervenções no controle de acesso ao evento.*

> ***g) Registro de veículos roubados ou furtados:*** *o registro de veículos roubados ou furtados nas bases de dados utilizadas no projeto é fundamental para identificar e prevenir a presença de veículos relacionados a crimes ou suspeitas de irregularidades acessando o estádio. Isso contribui diretamente para a segurança pública, pois a presença de veículos nessas condições pode indicar atividades criminosas, e seu controle é essencial para a segurança nos arredores do evento".*

5.5.2.6. O controlador explicitou, conforme a determinação da ANPD, que a coleta de dados pessoais limitar-se-á a pessoas maiores de idade, conforme consta em diversos trechos da versão 2.0. do RIPD, como nos itens 12.5., 15.2. e 15.5. A limitação da coleta consta, outrossim, na minuta do protocolo de execução, em especial nas cláusulas sexta, inciso III, e sétima, incisos I, II e IX. Além disso, foi retirado do projeto a obrigação de coleta e compartilhamento do número do telefone dos titulares, o que está de acordo com determinação da Nota Técnica nº 175/2023/CGF/ANPD.

5.5.2.7. Por conseguinte, embora o item 15. da versão 2.0. do RIPD, que trata da identificação dos dados pessoais coletados e processados no projeto, não tenha manifestamente destacado que serão tratados dados da biometria facial dos torcedores, outros trechos do documento fazem menção explícita ao uso dessa categoria de dado pessoal, indicando-se a base legal, a necessidade e os mecanismos de controle, prevenção e segurança associados ao tratamento dos dados pessoais sensíveis.

5.5.2.8. Os atributos biométricos, por definição legal, constituem dados pessoais sensíveis, que, nos termos do artigo 5º, inciso II, da LGPD, se referem ao 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.

5.5.2.9. A categoria de dado pessoal sensível faz referência aos dados pessoais que, em virtude do seu conteúdo, podem implicar em risco ou vulnerabilidade potencialmente mais gravosas para o exercício dos direitos e garantias fundamentais pelos seus titulares[35]. Por isso, o tratamento de atributos biométricos deve ser verificado com maior rigor, tendo em vista os maiores riscos para os direitos dos titulares.

5.5.2.10. As tecnologias de reconhecimento facial são um dos principais mecanismos utilizados para o tratamento de dados biométricos, especialmente com vistas ao desenvolvimento de sistemas de identificação que auxiliam no controle e monitoramento de pessoas para diversas finalidades. Os atributos biométricos, por sua vez, conforme definição do art. 2º, inciso II, do Decreto nº 10.046/2019, podem ser definidos como as características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar.

5.5.2.11. A análise técnica de atributos biométricos, desse modo, consiste em ferramenta tecnológica que permite a ***detecção*** (descobrir e localizar faces nas imagens e vídeos), a ***identificação*** (quem é a pessoa da imagem?), a ***verificação*** (a pessoal existe ou está cadastrada?) e a ***classificação*** (categorizar o indivíduo por meio de atributos como gênero, etnia, raça, idade, alegre, feliz, nervoso etc.) de indivíduos específicos ou grupos de pessoas de forma mais rápida e confiável, com base em um conjunto de dados reconhecíveis e verificáveis, que são únicos e específicos sobre seus titulares.

5.5.2.12. As tecnologias de reconhecimento facial permitem que indivíduos sejam automaticamente reconhecidos a partir da criação de uma representação digital e pesquisável da sua face, obtida por meio de fotos ou imagens previamente armazenadas, de maneira a facilitar processos de *verificação* e de *identificação* de determinada pessoa ou grupos[36].O tratamento de dados biométricos, com a utilização de tecnologia de reconhecimento facial, desse modo, possibilita aos controladores o desenvolvimento de sistemas de identificação que auxiliam no controle e monitoramento de pessoas para diversas finalidades, como segurança pública e o combate a fraudes financeiras[37]. Além disso, ao ser integrada a sistemas de vídeo e vigilância, a tecnologia de reconhecimento facial permite a identificação à distância, sem que as pessoas saibam que estão sendo monitoradas ou tenham que cooperar com o processo de identificação[38]. A utilização desses sistemas, sem que sejam garantidas as salvaguardas necessárias para a proteção de direitos assegurados aos cidadãos, pode levar a situações discriminatórias, bem como pode

gerar riscos ao exercício do direito à privacidade e, inclusive, de direitos políticos, como a livre manifestação em espaços públicos.

5.5.2.13. Os sistemas de reconhecimento facial, enquanto ferramentas de tratamento de dados pessoais sensíveis, portanto, devem estar adequados às disposições da LGPD. Desse modo, ainda que a norma de proteção de dados pessoais não vede a utilização de sistemas de reconhecimento facial para a identificação de terceiras pessoas, o uso dessa tecnologia deve ser feito em estrita consonância com as normas e princípios que limitam o tratamento de dados pessoais sensíveis pelos controladores, sempre com o objetivo de assegurar o exercício dos direitos e garantias fundamentais constitucionalmente protegidas.

5.5.2.14. O MJSP, desse modo, explicou que a coleta da biometria dos torcedores, por meio de sistema eletrônico de reconhecimento facial, ocorrerá no momento da compra do ingresso, "*podendo ocorrer concomitantemente com a captura da fotografia de um documento oficial ou mediante cadastro prévio presencial, onde a biometria facial é registrada e as informações declaradas são validadas pelas ticketeiras contratadas pelas organizações Desportivas*"[39].

5.5.2.15. O item 12. da versão 2.0. do RIPD, desse modo indica expressamente que o art. 148 da Lei nº 14.597/2023, Lei Geral do Esporte, é o fundamento legal autorizativo para a coleta da biometria facial dos torcedores. Assim, haveria uma obrigação legal para que as entidades de prática esportiva coletassem os dados biométricos para a consecução de finalidades específicas dispostas na norma. Tal obrigação legal, assim, estaria em conformidade com o art. 11, inciso II, alínea "a", da LGPD, segundo a qual o tratamento de dados pessoais sensíveis poderá ocorrer, sem o consentimento das pessoas naturais às quais se referem, caso seja necessário para o cumprimento de obrigação legal do controlador.

5.5.2.16. A tecnologia de reconhecimento facial, nesse contexto, seria utilizada como meio de autenticação da imagem vinculada ao CPF fornecido pelo torcedor maior de idade à entidade de prática desportiva (EPD), com vistas à mitigação dos riscos de "cambismo" e falsidade ideológica, o que fortaleceria a segurança e a integridade do processo de aquisição de ingressos. Além disso, a utilização da biometria facial proveniente das entidades esportivas possibilitaria a identificação dos indivíduos envolvidos em atos de violência, racismo, xenofobia, LGBTfobia e violação das regras de segurança durante os eventos esportivos[40].

5.5.2.17. O uso da biometria facial dos torcedores, para a consecução das finalidades supramencionadas, na visão do MJSP, seria, ademais, compatível com a Política Nacional de Inteligência de Segurança Pública (PNISP) e a Estratégia Nacional de Inteligência de Segurança Pública (ENISP), dada a necessidade de contribuição para o aprimoramento das atividades de Inteligência em Segurança Pública (ISP), seja na produção de conhecimento seja em ações de investigação de polícia judiciária.

5.5.2.18. O documento fez, entretanto, ressalvas quanto à utilização de tecnologia de biometria facial no contexto do projeto. Primeiramente, a utilização dessa tecnologia não se destinaria à obtenção de indicativos de abordagem em tempo real nos acessos ou entornos dos estádios. Em caso de verificação da necessidade de utilização de tecnologia para esse fim, o MJSP afirma que solicitará a aprovação de um protocolo de execução específico pela Autoridade Nacional de Proteção de Dados (ANPD). Em seguida, afirma-se que o identificador principal para gerar o indicativo de abordagem, assim como para o procurado, impedido, desaparecido, falecido e sujeito de identidade divergente, consiste no número de CPF[41]. A utilização da tecnologia de reconhecimento facial, desse modo, teria caráter secundário.

5.5.2.19. Entende-se, conforme o exposto, que o MJSP descreveu de forma detalhada a necessidade e a adequação dos dados pessoais coletados para a realização das finalidades do projeto Estádio Seguro. A utilização dos dados biométricos dos torcedores, por meio da utilização de sistema de reconhecimento facial, no entanto, deve ser feita nos termos estritos da legislação que autoriza a sua coleta e não devem, de forma alguma, ser empregados para finalidades distintas daquelas informadas aos titulares.

5.5.3. *Sobre a possibilidade de coleta excessiva de dados pessoais de torcedores (princípio da necessidade).*

5.5.3.1. Ainda que o projeto Estádio Seguro tenha como objetivo a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, não se pode conceber o acúmulo e a produção de

conhecimento despropositado sob a justificativa de proteger a sociedade de seus próprios cidadãos. Isso ocorre uma vez que a coleta e o armazenamento excessivos de dados pessoais para finalidades de segurança pública podem representar uma séria violação aos direitos de privacidade e proteção de dados pessoais dos titulares. Essa interferência nos direitos de personalidade dos titulares de dados é especialmente preocupante quando realizada de forma sistemática por autoridades públicas, com a utilização de sistemas que realizam o tratamento de dados biométricos, mesmo quando os dados pessoais coletados se referirem a atividades realizadas em espaços públicos[42].

5.5.3.2. O tratamento de dados pessoais para finalidades associadas a segurança pública e a atividades de investigação e repressão de infrações penais, com cada vez mais frequência, é realizado com o emprego de técnicas de tratamento de grandes volumes de dados estruturados ou não (*big data)* [43]. Essas técnicas permitem a identificação de tendências e padrões comportamentais de pessoas ou grupos sociais específicos, por meio de análises descritivas, preditivas e prescritivas, realizadas tanto por entidades privadas quanto por governamentais. Isso é possível uma vez que tais técnicas possibilitam a coleta e o armazenamento de grande volume de dados digitais, com diversos tipos de qualidade, os quais podem ser processados em altíssima velocidade, gerando modelos de análise com grande precisão[44].

5.5.3.3. O uso de técnicas de *big data* no tratamento de dados pessoais para finalidades de segurança pública e persecução penal, por sua vez, pode resultar em uma situação de "vigilância de arrastão" (*dragnet surveillance*[45]). A "vigilância de arrastão[46] é compreendida como *"um conjunto de técnicas de investigação que envolvem a coleta de dados e informações sobre um número elevado de pessoas (a maioria inocentes), e não apenas sobre aquelas pessoas contra as quais há indícios de envolvimento em atividades criminosas"*. Em função dessa prática, pessoas sem nenhum tipo de envolvimento em práticas criminosas – ou mesmo sob suspeita de estarem envolvidas em algum tipo de irregularidade – podem acabar inseridas em bancos de dados de autoridades púbicas de segurança[47].

5.5.3.4. Nesse sentido, é fundamental que os órgãos de segurança pública, quando realizarem o tratamento de dados pessoais no âmbito de suas atribuições legais, estabeleçam limites proporcionais ao que se refere à coleta e ao armazenamento de dados pessoais para fins de suas atividades. Deve-se, por exemplo, deixar claras as categorias de sujeitos cujos dados pessoais devem ser recolhidos, as condições para o tratamento dos dados pessoais e os prazos específicos para o ciclo de vida dos dados acumulados. Procura-se, desse modo, ponderar o respeito à privacidade, à proteção de dados pessoais e à presunção de inocência, bens jurídicos constitucionalmente assegurados, com a necessidade social premente da segurança pública.

5.5.3.5. Observa-se que a iniciativa do MJSP, de maneira geral, tem como objetivo a identificação de sujeitos de interesse da justiça e da segurança pública, *por meio do controle de acesso do público a eventos esportivos*, conforme delimitação feita pelo *caput* do art. 148 da Lei Geral do Esporte. Por esse motivo, a CGF determinou ao MJSP que ajustasse o RIPD no sentido de deixar claro que somente seriam repassados pelas entidades esportivas ao órgão público federal os dados pessoais de uma categoria de indivíduos específica, isto é, os sujeitos de interesse da justiça e segurança pública.

5.5.3.6. De acordo com a redação da versão 2.0. do RIPD[48], entretanto, é possível concluir que serão passíveis de tratamento pelo MJSP não apenas os dados pessoais de sujeitos de interesse da justiça e segurança pública. Conforme o documento, as entidades esportivas deverão encaminhar para o tratamento do MJSP os dados pessoais coletados de todos os que adquirirem ingressos (por de venda, fornecimento gratuito ou repasse de bilhetes) para os eventos esportivos, independentemente de seu efetivo comparecimento ao evento. O texto da cláusula sexta, inciso III, e da cláusula sétima, inciso II, da minuta do protocolo executivo permite que se chegue à mesma conclusão:

> CLÁUSULA SEXTA – DAS OBRIGAÇÕES DA CONFEDERAÇÃO BRASILEIRA DE FUTEBOL
>
> III - Incentivar as Organizações de Práticas Desportivas mandantes de partidas, provas ou eventos correspondentes a adotarem a integral informatização do processo de venda, fornecimento gratuito e repasse de bilhetes, bem como o sistema de acesso dos torcedores em competições realizadas em arenas esportivas com capacidade para mais de 20.000 (vinte mil) pessoas, ***inclusive nos casos de gratuidade, meia entrada, cortesias, associados, membros, sócio-torcedores e membros de torcidas organizadas, abrangendo indivíduos maiores de idade***;

> (...)
>
> CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DAS ORGANIZAÇÕES DE PRÁTICAS DESPORTIVAS MANDANTE DA PARTIDA, PROVA OU EVENTOS CORRESPONDENTES
>
> II - Implementar e/ou aprimorar os sistemas voltados à integral informatização do processo de venda, fornecimento gratuito e repasse de bilhetes, bem como o sistema de acesso dos torcedores em competições realizadas em arenas esportivas com capacidade para mais de 20.000 (vinte mil) pessoas, ***inclusive nos casos de gratuidade, meia entrada, cortesias, associados, membros, sócio-torcedores e membros de torcidas organizadas, abrangendo indivíduos maiores de idade***;

5.5.3.7. A coleta de dados pessoais, com fundamento no art. 148 da Lei Geral do Esporte, para as finalidades específicas do projeto, no entanto, limita-se aos *frequentadores do evento esportivo*. Desse modo, a coleta de dados pessoais de associados, membros, sócios-torcedores e membros de torcidas organizadas das entidades esportivas que não tiverem adquirido (por de venda, fornecimento gratuito ou repasse de bilhetes) ingressos para a partida mostra-se excessiva em relação à determinação legal, não é objeto do ACT e não deve ser realizada. A coleta dos dados pessoais dessas categorias de sujeitos junto às entidades esportivas, *sem que essas pessoas estejam diretamente associadas à participação em um evento esportivo*, ampliaria, portanto, o escopo de aplicação do art. 148 da Lei Geral do Esporte, e estaria em desconformidade com o princípio da necessidade, nos termos do art. 6º, inciso III, da LGPD.

5.5.3.8. A captação de dados pessoais, por meio do uso de imagens de câmeras de segurança, por outro lado, será legítima, desde que tenha como finalidade a prevenção da ocorrência de atos ilícitos no contexto da realização do evento esportivo e a identificação de indivíduos envolvidos em atividades ilegais, como as descritas nas finalidades específicas do projeto. Desse modo, as imagens dos indivíduos poderiam ser capturadas, para posterior tratamento, no âmbito do projeto Estádio Seguro, somente quando a ação estiver relacionada à realização do evento esportivo, permitindo-se as filmagens no interior do estádio, nas suas proximidades e no percurso entre um ponto de concentração de torcedores e o estádio. A utilização de tecnologia de reconhecimento facial, associada a sistemas de monitoramento por vídeo, no entanto, deverá estar submetida ao envido de RIPD específico para a Autoridade Nacional de Proteção de Dados Pessoais.

5.5.3.9. Observa-se, por conseguinte, no que se refere à possibilidade de coleta de dados pessoais apenas de sujeitos de interesse da justiça, que a identificação dessa categoria de indivíduos, conforme o contexto de tratamento de dados pessoais no âmbito do projeto, somente poderia ser devidamente verificada após o cruzamento dos dados pessoais de todos os frequentadores do evento esportivo com as bases de verificação da Plataforma Córtex.

5.5.3.10. A coleta dos dados pessoais de todos os frequentadores do evento esportivo, desse modo, torna-se necessária para que o órgão público possa identificar, após o processamento dos dados pessoais, com as suas bases de verificação, os sujeitos de interesse da justiça.

5.5.3.11. Assim, tendo em vista o melhor detalhamento contido na descrição da metodologia para a coleta e tratamento das informações pessoais, no âmbito do projeto Estádio Seguro, conforme o disposto no item 5.2.9 desta Nota Técnica, *entende-se que a limitação da coleta de dados pessoais apenas aos sujeitos de interesse da justiça impediria a consecução dos propósitos específicos do projeto Estádio Seguro*. Deve-se, porém, em virtude da impossibilidade de limitação do tratamento de dados pelo MJSP apenas aos sujeitos de interesse da justiça, sem que as finalidades legítimas do projeto Estádio Seguro sejam comprometidas, examinar o período de retenção dos dados pessoais coletados pelo órgão público, conforme disposto na versão 2.0 do RIPD.

5.5.3.12. Conforme já destacado, o armazenamento de dados pessoais coletados de forma sistemática por entidades públicas não apenas configura interferência no direito a proteção de dados pessoais, mas também pode representar uma ameaça ao exercício de outros direitos e garantias fundamentais dos titulares de dados, como a inviolabilidade da vida privada, a proteção de dados pessoais e a presunção de inocência.

5.5.3.13. Pela redação da versão 2.0. do RIPD, o MJSP reterá em seus sistemas todos os dados pessoais coletados no âmbito de realização do Projeto Estádio Seguro pelo prazo máximo de 20 anos; informa que o período de retenção foi baseado no artigo 109, inciso I, do Decreto-lei nº 3.689 de 03 de

outubro de 1941, Código de Processo Penal, e se aplicará a todos os dados pessoais coletados, independentemente da finalidade específica para a qual houve o seu recolhimento.

5.5.3.14. Percebe-se, nesse ponto, que parece ter havido equívoco do MJSP ao indicar o fundamento legal que justificaria a retenção de dados pelo prazo supracitado. O fundamento indicado para estabelecer o período de retenção dos dados pessoais, na verdade, deve estar se referindo ao artigo 109, inciso I, do Decreto-lei nº 2.848, de 7 de dezembro de 1940, Código Penal. Desse modo, a análise quanto ao limite temporal de retenção dos dados será feita com base no dispositivo do Código Penal, e não do Código de Processo Penal, conforme fora informado pelo controlador.

5.5.3.15. Embora a LGPD não tenha estabelecido um prazo determinado para que os agentes de tratamento descartem os dados pessoais coletados, a norma de proteção de dados pessoais estipula parâmetros para o término do tratamento e a eliminação desses dados. Assim, pode-se compreender que o legislador optou por limitar temporalmente o período de tratamento de dados pessoais por controladores e operadores, de maneira que os agentes de tratamento não possam armazenar os dados coletados indefinidamente[49]. Trata-se, portanto, de norma diretamente relacionada à aplicação do princípio da necessidade.

5.5.3.16. O art. 15 da LGPD, nesse sentido, determinou quatro hipóteses para o término do tratamento de dados pessoais, as quais podem ser organizadas como (i) esgotamento funcional da utilização dos dados; (ii) término do prazo; (iii) autodeterminação informacional; e (iv) ilegalidade[50]. No âmbito do projeto Estádio Seguro, não se vislumbra, à princípio, o término do tratamento dos dados pessoais coletados com fundamento nas hipóteses de autodeterminação informativa e de ilegalidade.

5.5.3.17. No caso da hipótese de autodeterminação informativa, o término do tratamento ocorre em virtude da revogação do consentimento pelos titulares. No entanto, uma vez que o fundamento legal para o tratamento de dados pessoais no âmbito do projeto em análise se baseia na execução de competências e atribuições legais do serviço público, nos termos do art. 23 da LGPD, por órgãos do Ministério da Justiça e Segurança Pública, o consentimento dos titulares não seria exigível. A inexigibilidade da solicitação prévia do consentimento do titular, para o tratamento de dados baseado no art. 23 da LGPD, assim, torna o exercício do direito à revogação do consentimento inaplicável ao caso concreto.

5.5.3.18. Quanto à hipótese de ilegalidade, no presente contexto e considerando as competências do MJSP, o término do tratamento ocorreria apenas após determinação expressa da Autoridade Nacional de Proteção de Dados, conforme as sanções previstas na Resolução CD/ANPD nº 4, de 24 da fevereiro de 2023 (Regulamento de Dosimetria e Aplicação de Sanções Administrativas). O término do tratamento com base nessa hipótese, no entanto, está condicionado a decisão administrativa impetrada pela ANPD, no âmbito de processo fiscalizador, quando houver necessidade de medida preventiva, ou de processo sancionador, nos termos da legislação aplicável.

5.5.3.19. O término do tratamento de dados pessoais, entretanto, poderia ser fundamentado em duas outras hipóteses. Primeiro, poder-se-ia encerrar a operação de tratamento em virtude do exaurimento da finalidade específica para a qual os dados foram coletados ou quando os dados tratados deixarem de ser necessários para se alcançar os propósitos do tratamento. Em segundo, ocorreria o encerramento da operação de tratamento com o fim do prazo de retenção dos dados pessoais. Tal prazo pode ser definido, por exemplo, tanto em função de uma obrigação contratual pactuada entre as partes ou em virtude de uma obrigação legal específica.

5.5.3.20. Observa-se, no que se refere ao exaurimento dos propósitos de tratamento, que as finalidades estabelecidas para o tratamento de dados precisam ser capazes de justificar a retenção dos dados pessoais pelo controlador[51]. Além disso, percebe-se que, se um conjunto de dados pessoais foi coletado para um propósito específico e ele não mais for aplicável ao caso concreto, o tratamento desses dados deixa de ser necessário.

5.5.3.21. O MJSP, conforme visto, definiu oito finalidades específicas que justificariam o tratamento de dados pessoais, as quais foram descritas no item 5.5.1.10 desta Nota Técnica. Para o atingimento dessas finalidades, seriam coletados dados pessoais de *todos* os torcedores que adquirissem ingressos para eventos esportivos organizados pelas entidades cooperadas.

5.5.3.22. Ao se verificar de maneira detalhada as finalidades específicas informadas para o tratamento de dados pessoais, tem-se que a identificação das pessoas de interesse da justiça e segurança pública, propósito específico para a consecução das finalidades (i) a (vii)[52], é feita já na etapa de consciência situacional (etapa 1), momento em que é realizada a verificação dos dados pessoais coletados com a base de dados do órgão público.

5.5.3.23. Assim, com o envio de alertas gerais aos Estádios (etapa 2), para que os agentes de segurança presentes nos eventos esportivos possam realizar as abordagens dos sujeitos e veículos de interesse, ocorre o exaurimento das finalidades para as quais os dados pessoais foram coletados, constituindo-se em marco para o término do tratamento. Por conseguinte, a retenção dos dados pelo MJSP deixa de ser necessária para a consecução dos propósitos específicos do projeto.

5.5.3.24. Eventual conservação dos dados pessoais compartilhados pelas entidades esportivas, no âmbito do MJSP, somente seria legítima mediante a existência de previsão legal que justificasse a medida ou a incidência de uma das hipóteses legais do art. 16 da LGPD[53]. Assim, entende-se que, para o atingimento das finalidades específicas de (i) a (vii), a retenção de dados pessoais de *todos* os torcedores que compareceram ao evento esportivo, após o seu encerramento, não se justificaria nos termos apresentados pela versão 2.0. do RIPD.

5.5.3.25. Compreende-se, com base no exposto, que apenas os dados pessoais dos sujeitos de interesse da justiça e segurança pública que tenham sido devidamente identificados, após a verificação realizada por meio da Plataforma Córtex, seriam passíveis de retenção após o encerramento do evento, para a consecução das finalidades de (i) a (vii). Os dados pessoais dos demais torcedores, desse modo, devem ser descartados em virtude do exaurimento da finalidade para a qual eles foram coletados.

5.5.3.26. A única exceção para a conservação de dados pessoais, após o encerramento do evento esportivo, ocorreria para finalidade (viii), ou seja, a identificação de autores de delitos relacionados ao evento esportivo, como atos de violência, racismo, xenofobia, LGBTfobia e violação das regras de segurança praticados no período que antecede, coincide e prossegue após a partida.

5.5.3.27. A verificação da identidade dos sujeitos de interesse, para o atingimento desta finalidade específica, ocorre apenas durante a etapa de *identificação de autoria* (etapa 3), por meio da utilização de dados pessoais captados pelas imagens provenientes de televisões, câmeras de vigilância dos estádios e de redes sociais. Os dados pessoais coletados, incluindo-se dados da biometria facial dos torcedores, provenientes das entidades esportivas, seriam utilizados para a verificação da identidade de eventuais infratores, após o seu cruzamento com as bases de dados em posse do órgão federal, no âmbito da Plataforma Córtex, em particular as bases de dados do SERPRO, TSE e RFB, as quais seriam reprocessadas para finalidades de segurança pública (item 15.5 da versão 2.0. do RIPD).

5.5.3.28. Tem-se que a consecução dessa finalidade específica (viii) está associada não apenas à ação ostensiva das forças de segurança durante o evento esportivo, mas também à persecução de atividades de polícia judiciária, especialmente no âmbito de eventuais investigações de atividades criminosas ocorridas antes, durante e após o evento esportivo. Nesse sentido, a retenção dos dados pessoais necessários para a realização dessa finalidade, por maior prazo, seria justificável, uma vez que a sua eliminação logo após o fim do evento poderia prejudicar o atingimento do propósito para os quais eles foram coletados pelo MJSP.

5.5.3.29. A retenção dos dados pessoais provenientes de câmeras de vigilância dos estádios, capturados durante o evento, bem como os dados biométricos coletados para identificar autores de delitos relacionados ao evento esportivo, porém, deve ser temporalmente limitada para atender à necessidade de minimização do armazenamento de dados pessoais. Compreende-se que, da mesma forma que ocorre com as demais finalidades do projeto, os dados pessoais coletados não devem ser utilizados para constituir repositórios de informações contidas em bases de dados governamentais, para serem utilizados a qualquer momento. Tal tratamento é incompatível com a LGPD, em especial no que se refere à aplicação do princípio da finalidade.

5.5.3.30. A retenção de dados pessoais, dessa maneira, mesmo quando justificável, não pode ocorrer por período indeterminado ou estipulado de maneira desproporcional em relação à finalidade a ser alcançada. A Lei Geral do Esporte, norma que fundamenta o recolhimento de dados dos torcedores

pelas entidades esportivas, não estabeleceu qualquer prazo para a retenção dessas informações. O MJSP, nos termos do inciso II do art. 15 da LGPD, por sua vez, procurou estabelecer um limite temporal para o tratamento de todos os dados pessoais coletados, vinculando-o a prazo prescricional descrito no Código de Processo Penal.

5.5.3.31. O MJSP, desse modo, definiu prazo máximo de 20 anos para o armazenamento de todos os dados pessoais compartilhados pelas entidades privadas, com base no artigo 109, inciso I, do Decreto Lei nº 2.848/1940 (Código Penal), independentemente da finalidade específica para a qual os dados foram coletados, bem como da categoria de sujeito à qual os dados se vinculam.

> **Decreto-lei nº 2.848, de 7 de dezembro de 1940, Código Penal**
>
> Art. 109. A prescrição, antes de transitar em julgado a sentença final, salvo o disposto no § 1o do art. 110 deste Código, regula-se pelo máximo da pena privativa de liberdade cominada ao crime, verificando-se: (Redação dada pela Lei nº 12.234, de 2010).
>
> I - em vinte anos, se o máximo da pena é superior a doze;

5.5.3.32. O prazo de retenção máxima de 20 anos se aplicaria, portanto, de maneira genérica, a todos os dados pessoais coletados pelo órgão público, independentemente da finalidade para a qual eles foram coletados. Tal situação resulta em coleta massiva e sistemática de dados pessoais, inclusive sensíveis, de sujeitos indeterminados, sem que exista norma específica que defina os limites de armazenamento.

5.5.3.33. A utilização de prazo prescricional do art. 109, inciso I, do Código Penal, sem qualquer tipo de contextualização ou de justificativa quanto a sua necessidade ou pertinência, ademais, é desproporcional para as finalidades específicas do projeto Estádio Seguro. Como exemplo da desproporcionalidade do prazo de retenção pretendido, pode-se citar a finalidade de tratamento para o combate ao "cambismo". De acordo, com o art. 167 da Lei Geral do Esporte, o prazo de reclusão do tipo penal associado a esta prática varia de 2 (dois) a 4 (quatro) anos, podendo ser acrescido em até 1/3, em determinadas circunstâncias. Pelas normas de prescrição dispostas no art. 109 do Código Penal, não se aplicaria ao caso exposto o prazo prescricional máximo inserido no inciso I do art. 109, utilizado pelo MJSP para determinar o prazo de retenção de todos os dados coletados, mas deveria ser utilizado prazo menor, conforme o exposto:

> Art. 109. A prescrição, antes de transitar em julgado a sentença final, salvo o disposto no § 1º do art. 110 deste Código, regula-se pelo máximo da pena privativa de liberdade cominada ao crime, verificando-se: (Redação dada pela Lei nº 12.234, de 2010).
>
> I - em vinte anos, se o máximo da pena é superior a doze;
>
> II - em dezesseis anos, se o máximo da pena é superior a oito anos e não excede a doze;
>
> III - em doze anos, se o máximo da pena é superior a quatro anos e não excede a oito;
>
> IV - em oito anos, se o máximo da pena é superior a dois anos e não excede a quatro;
>
> V - em quatro anos, se o máximo da pena é igual a um ano ou, sendo superior, não excede a dois;
>
> VI - em 3 (três) anos, se o máximo da pena é inferior a 1 (um) ano.

5.5.3.34. O prazo de 20 anos de retenção, para a consecução dessa finalidade específica, assim, se mostra claramente excessivo, motivo pelo qual está em desacordo com o art. 6º, inciso II, da LGPD. Por esse motivo, entende-se que o prazo de retenção dos dados pessoais deve estar vinculado a cada finalidade específica para a qual o dado foi coletado. A imposição de prazo genérico, sem qualquer tipo de justificativa, torna a prática irregular à luz da LGPD.

5.5.3.35. Como exemplo da delimitação do prazo de retenção de dados pessoais para finalidades de segurança pública e persecução penal, pode-se citar o art. 13 da Lei nº 12.965/2014, Marco Civil da Internet (MCI). O dispositivo, ao tratar sobre o período de guarda de registros de conexão por administradores, estabelece o prazo de 1 (um) ano, nos termos de regulamento, para o arquivamento de dados e informações pessoais de usuários da rede de computadores.

5.5.3.36. O MCI, ademais, estabelece condições para que autoridade policial ou administrativa ou o Ministério Público possa requerer prazo de guarda superior à regra geral, caso se verifique a necessidade de sua utilização para atividades relacionadas à segurança pública. Desse modo, o legislador procurou

sopesar o direito de privacidade dos usuários da internet e o interesse público associado, entre outros valores constitucionalmente protegidos, à segurança pública.

5.5.3.37. No caso em análise, como visto, a Lei de Geral do Esporte não faz qualquer tipo de determinação quanto ao prazo de retenção dos dados pessoais coletados pelas entidades esportivas. Do mesmo modo, não foram especificadas condições para o seu compartilhamento com autoridades públicas para a sua utilização em finalidades relacionadas à segurança pública. A lacuna legislativa, salvo melhor juízo, não poderia ser superada com fundamento no artigo 109, inciso I, do Código Penal, conforme deseja o MJSP, em virtude da sua desproporcionalidade em relação às finalidades para as quais o tratamento de dados é realizado.

5.5.3.38. Diante do exposto, entende-se que a retenção dos dados pessoais coletados para a consecução das finalidades (i) a (vii), após o encerramento do evento esportivo, excede a necessidade para a qual eles foram coletados, exceto no caso dos dados pessoais vinculados a pessoas de interesse da justiça e segurança pública que tenham sido identificadas após a etapa de consciência situacional.

5.5.3.39. Considera-se, por outro lado, legítima a retenção das imagens dos torcedores captadas por câmeras de vigilância, assim como dos dados biométricos compartilhados pelas entidades esportivas, para a identificação de autores de delitos relacionados a fatos ocorridos no contexto do evento esportivo, desde que o prazo de conservação dos dados pessoais seja limitado temporalmente, bem como seja proporcional em relação à finalidade para a qual eles foram coletados.

5.5.3.40. Verifica-se, por fim, que o prazo de retenção de dados pessoais estipulado em 20 anos, conforme o prazo prescricional do artigo 109, inciso I, do Código Penal, é genérico, pois desconsidera as diversas finalidades para as quais os dados pessoais foram coletados, bem como é desproporcional, uma vez que se mostra excessivo em relação aos propósitos de tratamento relacionados ao projeto Estádio Seguro.

5.5.3.41. Nesse sentido, para os dados pessoais de frequentadores do evento esportivo que não sejam de interesse da segurança pública, recomenda-se, até que sobrevenha a legislação específica prevista no art. 4º, §1º, que as imagens captadas dos torcedores por câmeras de vigilância, assim como os dados biométricos compartilhados pelas entidades esportivas, coletadas para finalidade específica (viii) sejam mantidas por, no máximo, 30 (trinta) dias após o encerramento do evento esportivo, ressalvadas as situações em que autoridade policial ou administrativa ou o Ministério Público requeira ao MJSP a guarda por prazo superior, caso se verifique a necessidade de sua utilização no âmbito de investigações de atividades criminosas ocorridas antes, durante e após o evento esportivo. Desse modo, estabelece-se um equilíbrio provisório entre o direito de privacidade dos frequentadores do evento esportivo e o interesse público associado à segurança pública.

5.5.3.42. Alternativamente, quando essas informações forem armazenadas pela própria entidade de prática desportiva, nos mesmos termos do MCI, podem ser disponibilizadas ao MJSP mediante autorização judicial. Trata-se de um modelo já conhecido, proposto pelo legislador, de equilíbrio entre valores constitucionais como a vida, a segurança, a vida privada e a proteção de dados.

5.5.4. *Do princípio da transparência e dos direitos dos titulares.*

5.5.4.1. A LGPD estabeleceu uma estrutura legal que empodera os titulares de dados pessoais, fornecendo-lhes direitos a serem exercidos perante os agentes de tratamento. Esses direitos devem ser garantidos durante toda a existência do tratamento dos dados pessoais do titular realizado pelo órgão ou entidade. Os direitos a serem garantidos aos titulares de dados estão segregados tanto nos princípios estabelecidos pelo artigo 6º da LGPD, quanto em direitos específicos dos titulares constantes dos demais artigos da referida Lei.

5.5.4.2. O princípio da finalidade, por exemplo, ao mesmo tempo em que torna explícito o objetivo final do tratamento, também confere ao titular a previsibilidade de seu resultado, inviabilizando o tratamento posterior dissociado da finalidade original. Desse modo, no âmbito do Poder Público, permite-se que o titular possa verificar se a operação de tratamento dos dados guarda, de fato, relação direta com a missão institucional do órgão ou ente público detentor da base de dados sobre a qual está fundamentada a execução de política pública ou a obrigação legal investida por lei, que justifica a interferência no direito a proteção de dados pessoais[54].

5.5.4.3. O princípio da transparência (art. 6º, inciso VI, LGPD), por sua vez, estabelece uma série de garantias ao titular quanto ao acesso a informações sobre o tratamento de dados pessoais pelo controlador. O exercício do direito de acesso, previsto no art. 9º da LGPD, por exemplo, depende do nível de transparência do controlador em relação às operações de tratamento realizadas e da qualidade dos dados aos quais é dado o acesso. Assim, sem que sejam indicadas corretamente as finalidades específicas de determinada operação de tratamento, não é possível aferir se a coleta de dados está em conformidade com a norma de proteção de dados pessoais.

5.5.4.4. O art. 9º da LGPD, nesse sentido, determinou aos agentes de tratamento que, ao realizarem o tratamento de dados pessoais sensíveis, assegurem o direito de acesso facilitado às informações sobre o tratamento, que devem ser disponibilizadas de maneira clara, adequada e ostensiva sobre: (i) finalidade específica; (ii) forma e duração, observados o segredo comercial e industrial; (iii) identificação do controlador; (iv) informações de contato do controlador; (v) informações acerca do uso compartilhado de dados pelo controlador e a finalidade; (vi) responsabilidades dos agentes que realizarão o tratamento; e (vii) direitos do titular, com menção explícita aos direitos do art. 18 da norma[55].

5.5.4.5. Para o exercício dos direitos dos titulares, a seu turno, a Lei prevê um conjunto de ferramentas, que, no âmbito público, traduzem-se em mecanismos que aprofundam obrigações de transparência ativa e passiva, bem como criam meios processuais para provocar a Administração Pública.

5.5.4.6. O titular tem, dessa maneira, o direito de ser informado sobre o tratamento dos seus dados, o que envolve a solicitação de informações sobre a finalidade, a duração e a forma de tratamento dos dados, assim como solicitar informações sobre como os seus dados estão sendo ou foram compartilhados com outros agentes. Por sua vez, o Poder Público deve informar as hipóteses em que, no exercício de suas competências, realizará o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônico[56].

5.5.4.7. O MJSP, dessa maneira, no item 18.3. da versão 2.0. do RIPD, estabelece aos administradores dos estádios e às entidades esportivas obrigações de transparência quanto ao tratamento dos dados pessoais dos torcedores. Do mesmo modo, indica que as informações referentes ao tratamento de dados no âmbito do projeto poderão ser acessadas por meio do *link* (https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/projeto-estadio-seguro). Destaca, de igual maneira, que as informações relacionadas ao tratamento de dados serão afixadas nas bilheterias dos estádios, nos acessos aos estacionamentos e no ambiente *online* de venda de bilhetes. Em outras partes do documento, como nos itens 28.1.VI[57] e 29.1.I[58], há informações mais claras quanto às informações que devem constar nos instrumentos de transparência relacionados ao tratamento dos dados.

5.5.4.8. O MSJP assegura, dessa forma, que os titulares serão informados sobre o processamento de seus dados pessoais, incluindo propósitos específicos, a base legal, os direitos e o prazo de retenção, por meio de políticas de privacidade, avisos de segurança e comunicações específicas no momento da compra dos bilhetes. Os titulares dos dados pessoais, por conseguinte, poderão exercer seus direitos por meio do Sistema de Informação ao Cidadão e Ouvidoria, disponível em https://falabr.cgu.gov.br. O órgão público federal afirma que, pelo acesso à Plataforma FalaBr, o titular, com base no art. 18 da LGPD[59], terá as suas solicitações analisadas de acordo com a Lei de Acesso à Informação e as normas que regem a atividade de inteligência, enquanto não for promulgada a norma específica prevista no §1º do Art. 4º da LGPD.

5.5.4.9. A Lei nº 12.527/2011, Lei de Acesso à Informação (LAI), regulamenta o direito de acesso a informações de interesse coletivo e geral e de interesse particular dos cidadãos, produzidas ou custodiadas por órgãos e entidades públicas, nos termos do art. 5º, inciso XXXIII, da Constituição Federal. A LAI, por meio de mecanismo de transparência passiva, permite que qualquer possa realizar pedidos de acesso à informação, que são demandas direcionadas aos órgãos e entidades da administração pública, sejam sujeitos de direito público ou privado, realizadas por qualquer pessoa, física ou jurídica (como empresas e associações civis, por exemplo), que tenham por objeto um dado ou informação.

5.5.4.10. Os dados ou informações de interesse do requerente, por sua vez, podem estar armazenados em sistemas, bancos de dados ou registrados em documentos - que são suportes capazes de conter diversas informações. Assim, quando em um mesmo suporte (documento ou banco de dados) coexistirem informações ou dados sem restrição de acesso e informações protegidas por alguma hipótese de sigilo, é assegurado ao cidadão o direito de conhecer as primeiras, seja a partir da entrega do documento com a ocultação (tarja) das informações sigilosas, seja a partir da elaboração de um novo documento que as descreva (extrato ou certidão)[60].

5.5.4.11. O direito de acesso, nos termos do art. 9º da LGPD, por possuir próxima interconexão com o direito de acesso à informação assegurado pelo art. 5º, inciso XXXIII, da Constituição Federal[61], pode ser exercido por meio dos mecanismos de transparência passiva contidos na Lei nº 12.527/2011 (LAI). É importante ressaltar, no entanto, que o acesso a determinadas operações de tratamento de dados pessoais para finalidades associadas a questões de segurança pública poderá ser limitado, se, na análise do caso concreto, for verificado que a divulgação de determinadas informações seria prejudicial ao interesse público.

5.5.4.12. Nesse sentido, a restrição da prestação de informações ao titular poderá ser apontada quando ela for necessária, por exemplo, para impedir prejuízo a inquéritos, investigações ou procedimentos oficiais e judiciais em andamento ou para proteger direitos e liberdades de terceiros[62]. Para que a eventual restrição de acesso seja legítima, contudo, caberá ao MJSP indicar as razões de fato e de direito que impedem o amplo exercício do direito de acesso do titular, sendo a decisão restritiva de acesso passível de remédio legal, nos termos da LAI.

5.5.4.13. É importante, assim, deixar claro que o direito de acesso previsto no art. 9º da LGPD poderá ser limitado em casos específicos, caso seja esse o entendimento do MJSP, quando verificado que o exercício de tal direito poderá trazer prejuízos desproporcionais para o interesse público primário. A eventual negativa de acesso, contudo, deverá ser devidamente motivada, bem como o titular deverá ser informado sobre as razões que impedem o exercício do direito de acesso.

5.5.4.14. Observa-se, por outro lado, que o exercício dos direitos previstos no art. 18 da LGPD não necessariamente poderão ser efetivados por meio de pedido de acesso à informação. Isso ocorre uma vez que direitos como a correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD e a eliminação dos dados pessoais tratados com o consentimento do titular, por exemplo, não possuem conteúdo de pedido de acesso à informação, assemelhando-se a manifestações de ouvidoria, de maneira que se encontram fora do escopo de aplicação da LAI.

5.5.4.15. Assim, por meio da Plataforma FalaBr, as manifestações dos titulares que não possuem conteúdo de pedido de acesso à informação devem ser tratadas como manifestações de ouvidoria, na tipologia de “solicitação de providências” junto à administração. Tais demandas, ainda que tratadas na Plataforma FalaBr, encontram-se regulamentadas pela Lei nº 13.460/2017, Lei de Defesa do Usuário de Serviços Públicos, e Decreto nº 9.492/2018, referente à participação, proteção e defesa do usuário de serviços públicos na Administração Pública Federal.

5.5.4.16. Assim, ainda que tenham sido definidas as obrigações de transparência do controlador e das entidades esportivas, determinando-se o conteúdo, os locais e o modo como as informações de tratamento serão disponibilizadas aos titulares, deve-se ficar claro aos titulares que o direito de acesso poderá sofrer algum tipo de limitação, em virtude de eventuais necessidades de sigilo inerentes às atividades de segurança pública. Tal esclarecimento pode constar na página que traz as informações referentes ao tratamento de dados no âmbito do projeto, https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/projeto-estadio-seguro

5.5.4.17. Cabe ao MJSP, ademais, ao informar os titulares sobre o exercício dos direitos previstos na LGPD, indicar de forma clara e detalhada os direitos que poderão ser assegurados por meio de pedidos de acesso à informação, nos termos da LAI, e os direitos a serem exercidos por meio de solicitações de ouvidoria, na tipologia de “solicitação de providências”, conforme o disposto na Lei nº 13.460/2017 e no Decreto nº 9.492/2018.

5.5.5. *Sobre os princípios da segurança, da prevenção e da responsabilização e prestação de contas: medidas técnicas e administrativas de proteção de dados pessoais e mitigação de riscos.*

5.5.5.1. O princípio da segurança determina que os agentes de tratamento assegurem a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Trata-se de medida que visa não apenas proteger os dados pessoais de acessos indevidos, mas também resguardar a sua qualidade[63]. O princípio da prevenção, a seu turno, responsabiliza os agentes de tratamento pela adoção de medidas preventivas no que se refere à ocorrência de danos em virtude do tratamento de dados pessoais. De acordo com esse princípio, cabe aos controladores, por exemplo, adotar medidas que visem mitigar eventuais prejuízos e danos que possam resultar da ocorrência de eventos adversos no tratamento de dados.

5.5.5.2. Desse modo, enquanto o princípio da segurança visa garantir que o controlador tome medidas técnicas e administrativas necessárias para manter a confidencialidade dos dados pessoais tratados, mantendo-se a sua integralidade e disponibilidade, o princípio da prevenção objetiva a realização de avaliação preventiva pelo controlador, de maneira a identificar riscos e ameaças advindas da operação de tratamento, para que seja possível antever medidas, procedimentos e garantias que possam atenuar os riscos existentes.

5.5.5.3. O princípio da responsabilização e da prestação de contas, por sua vez, tem como objetivo garantir que os agentes de tratamento buscaram demonstrar que tomaram todas as medidas técnicas, organizativas e administrativas necessárias para a realização da operação de tratamento de dados. O agente de tratamento de dados, desse modo, deve ser capaz de indicar que realizou todas as ações necessárias para garantir a segurança dos dados dos titulares.

5.5.5.4. O MJSP, destarte, procurou indicar as medidas técnicas e administrativas necessárias para garantir a segurança e a confidencialidade dos dados pessoais no âmbito do projeto. Os aspectos de segurança da informação, na execução do projeto Estádio Seguro, são tratados no item 20 da versão 2.0 do RIPD, que se refere ao “Ambiente de tratamento de dados e de acesso restrito à informação e auditoria”). Em especial foram explicadas questões referentes à realização de auditorias, tanto junto às empresas contratadas pelas entidades esportivas, quanto em reação ao próprio ambiente da Plataforma Córtex, ao nível de segurança da autenticação desse sistema e ao acesso por terceiros. Observe-se abaixo:

> 20.1. Todos os sistemas integrados pelo projeto passarão por auditorias periódicas, realizadas quando apropriado e conveniente, com o propósito de assegurar a transparência e a lisura do referido processo. **Tais auditorias serão essenciais para verificar se as empresas contratadas pelas Organizações Desportivas integradas ao projeto, não receberão quaisquer bases de dados de forma irregular do MJSP. Além disso, será verificado se, ao término de cada evento, as empresas efetivamente eliminarão todos os códigos de vinculação previamente fornecidos pelo MJSP, necessários ao travamento da catraca, o que garante localizar o indivíduo de interesse da segurança pública**.
>
> 20.2. **Todo o cruzamento de dados, bem como os seus resultados e acessos ocorrerão no ambiente da Plataforma Córtex, que possui um sistema auditável, como log de acesso e movimentação.**
>
> 20.3. No âmbito da autenticação no sistema, destaca-se que a Plataforma Córtex utiliza a plataforma GOV.BR para o acesso ao login. É importante ressaltar que o acesso dos profissionais de segurança pública requer o nível ouro. É válido ressaltar que o GOV.BR é utilizado exclusivamente para a autenticação, verificando a identidade do profissional autorizado que utilizará o sistema, desde que sua Instituição de origem possua Acordo de Cooperação Técnica válido com o MJSP. Por outro lado, o processo de autorização, que envolve permissões de acesso, perfis e regras, é realizado internamente pela Área de Gestão e Governança da Plataforma Córtex da CGINT, de forma independente do GOV.BR.
>
> 20.4. Por outro lado, a auditoria na Plataforma Córtex é realizada de forma abrangente e sistemática pela Contrainteligência da Coordenação Geral de Inteligência (CGINT/DIOPI/SENASP/MJSP), visando garantir a integridade, segurança e conformidade das operações realizadas no sistema. A auditoria é conduzida por meio de registros de eventos e atividades relevantes, armazenados e monitorados de maneira contínua.
>
> 20.5. A plataforma possui mecanismos que registram informações detalhadas sobre ações realizadas pelos usuários, tais como autenticações, acessos, modificações de configurações, transações e

outras atividades relevantes. Esses registros de auditoria são armazenados de forma segura e podem ser utilizados posteriormente para análise, detecção de eventuais irregularidades, investigação e tomada de medidas corretivas.

20.6. Além disso, a Plataforma Córtex adota princípios de segregação de funções, significando que diferentes responsabilidades e privilégios são atribuídos aos usuários de acordo com suas funções e níveis de acesso. Isso contribui para a manutenção da integridade e confidencialidade das informações, bem como para a prevenção de práticas indevidas.

20.7. A equipe de auditoria, devidamente capacitada e especializada em segurança da informação, realizará análises regulares dos registros de auditoria, verificando a conformidade das operações com as políticas, normas e regulamentos estabelecidos. Essas análises também permitirão identificar possíveis vulnerabilidades, riscos e anomalias, garantindo a pronta resposta e mitigação de eventuais incidentes de segurança.

20.8. Cabe ressaltar que a auditoria na Plataforma Córtex é um processo contínuo e abrangente, integrado às práticas de governança de TI e segurança da informação. Isso assegura a transparência, rastreabilidade e confiabilidade das operações realizadas no sistema, fortalecendo a confiança dos usuários e promovendo a proteção dos dados e informações sensíveis.

20.9. O subsistema modular "Estádio Seguro" estará disponível na Plataforma Córtex, com acesso restrito a um grupo selecionado de policiais militares e civis responsáveis pela inteligência e policiamento nos estádios. Esses profissionais serão formalmente indicados pelos gestores de suas instituições com a finalidade de participar ativamente do projeto.

20.10. Essa restrição visa garantir que apenas profissionais autorizados, competentes e responsáveis, tenham acesso às funcionalidades e aos dados relevantes ao projeto. Ao restringir o acesso a um grupo específico de policiais designados, o sistema "Estádio Seguro" possibilitará um controle efetivo do compartilhamento e utilização de informações sensíveis relacionadas à segurança dos estádios. Isso contribuirá para prevenir vazamentos de dados, para manutenção da segurança dos titulares dos dados e garantir que apenas os profissionais designados e autorizados possam acessar e utilizar o sistema de acordo com os objetivos e diretrizes estabelecidos.

5.5.5.5. O MJSP, desse modo, procurou explicitar os mecanismos de segurança inerentes ao funcionamento da Plataforma Córtex, ambiente em que ocorrerão os acessos aos dados coletados e todo o cruzamento de dados. Foi indicado, assim, que serão adotados controles de acesso, criptografia, monitoramento de atividades, treinamento de pessoal e a realização de auditorias e avaliações periódicas de segurança.

5.5.5.6. O controlador, além disso, asseverou que a execução do projeto será realizada em consonância com diretrizes[64] que visam assegurar a exatidão, a clareza, a relevância a atualização dos dados coletados:

I - **Verificação e Autenticação**: o projeto reforçará às Entidades Desportivas a necessidade de implementação de protocolos rigorosos para a verificação da autenticidade dos dados fornecidos pelos torcedores no momento da aquisição dos ingressos, assegurando a veracidade das informações cadastradas. De igual forma o MJSP aplicará recurso tecnológico para verificar eventuais inconsistências entre foto e CPF apresentados pelos torcedores no momento da compra (autenticação de dados).

II - Integração de Sistemas: o projeto prevê a integração efetiva entre os sistemas das Entidades Desportivas e o MJSP, possibilitando a atualização em tempo real e a consistência dos dados ao longo do tempo.

III - Utilização de Tecnologias de Ponta: o projeto reforçará às Entidades Desportivas a necessidade de implementação de tecnologias avançadas, como a biometria facial, para corroborar a identidade do portador do ingresso no momento do acesso ao estádio, contribuindo para a clareza e precisão na verificação.

IV - Políticas de Atualização de Cadastro: o projeto reforçará às Entidades Desportivas a necessidade de implementação de políticas que incentivem e facilitem a atualização periódica dos dados cadastrais pelos torcedores, garantindo a relevância e a fidedignidade das informações ao longo do tempo.

V - Auditorias e Monitoramento Contínuo: o projeto prevê a realização de auditorias periódicas e monitoramento constante dos dados armazenados, identificando e corrigindo eventuais inconsistências de forma ágil e eficaz.

VI - Treinamento de Envolvidos: o projeto prevê a capacitação contínua dos profissionais envolvidos no tratamento de dados e uso dos dados tratados, assegurando que compreendam a importância da precisão e atualização das informações, bem como estejam alinhados com as práticas estabelecidas no âmbito da inteligência em segurança pública.

VII - Canais de Atualização para Titulares: o projeto reforçará às Entidades Desportivas quanto a necessidade de disponibilização de canais eficazes para que os titulares dos dados possam atualizar suas informações de forma direta, contribuindo para a manutenção da exatidão e relevância dos dados.

VIII - Conformidade com a LGPD: o projeto manterá a estrita observância das práticas e procedimentos em conformidade com a Lei Geral de Proteção de Dados (LGPD), assegurando que o tratamento e o uso de dados respeitem os princípios da finalidade, necessidade e proporcionalidade.

5.5.5.7. Para realizar a averiguação quanto aos riscos inerentes às operações de tratamento de dados pessoais no contexto do projeto Estádio Seguro, o MJSP adotou a metodologia de análise de risco disponibilizada pelo Ministério da Economia. Dessa maneira, seguiu parâmetros escalares e a mesma matriz de probabilidade x impacto utilizados para calcular e classificar os níveis dos riscos.

5.5.5.8. Com base na aplicação da referida metodologia, foram identificados oito riscos, conforme abaixo:

Id	Risco referente ao tratamento de dados pessoais	P (probabilidade)	I (impacto)	Nível de Risco
R01	Acesso não autorizado	5	10	50
R02	Modificação não autorizada	5	15	75
R03	Perda	10	10	100
R04	Roubo	5	15	75
R05	Remoção não autorizada	5	10	50
R06	Coleta excessiva	5	10	50
R07	Falha em considerar os direitos do titular dos dados pessoais	5	10	50
R08	Retenção prolongada de dados pessoais:	10	10	100

5.5.5.9. O MJSP, ademais, descreveu cada tipo de risco observado, conforme descrito a seguir:

Tipo de risco	Descrição

R01 - Acesso não autorizado	Caracteriza-se como a obtenção de acesso a um ambiente físico de forma ilegítima, sem a devida permissão ou autorização. Trata-se de uma violação à segurança e privacidade, que pode resultar em consequências prejudiciais e danosas para o ambiente em questão, bem como para os indivíduos e informações nele contidos. O acesso indevido implica no desrespeito às restrições e permissões estabelecidas, podendo comprometer a integridade, confidencialidade e disponibilidade dos recursos e dados presentes no ambiente físico. A prevenção e o controle efetivo dessas práticas são fundamentais para preservar a segurança e proteger os direitos das partes envolvidas, sendo necessário adotar medidas adequadas de proteção, tais como sistemas de controle de acesso, monitoramento, autenticação e autorização, conforme as normas e regulamentos aplicáveis.
R02 - Modificação não autorizada	Ocorre quando um usuário, sem as devidas permissões ou autorizações, realiza alterações em um dado pessoal ou registro. Essa ação configura uma violação às normas de privacidade e proteção de dados, podendo resultar em consequências adversas para os direitos e liberdades individuais. É essencial que o processamento de dados seja realizado de forma adequada e em conformidade com as disposições legais e regulamentares aplicáveis, a fim de evitar modificações não autorizadas. Para tanto, é necessário estabelecer controles de acesso eficazes, como sistemas de autenticação e autorização, que garantam que apenas usuários autorizados tenham permissão para modificar os dados pessoais. A implementação de medidas de segurança e a adoção de políticas internas claras são fundamentais para prevenir e mitigar o risco de modificações não autorizadas, assegurando a integridade e a confidencialidade dos dados.
R03 - Perda	Pode ocorrer tanto por ações intencionais de usuários, que resultam na exclusão indevida ou devida e não comunicada desses dados, quanto por ações não intencionais, como falhas em sistemas, sobrescrita de dados, falhas em hardware, entre outras circunstâncias. Tais perdas podem acarretar sérias consequências para a organização, como comprometimento da integridade das informações, interrupção de serviços e danos à reputação. É imprescindível adotar medidas preventivas e corretivas para mitigar esses riscos, garantindo a segurança e a proteção dos dados. Isso inclui a implementação de políticas de backup e recuperação de dados, o estabelecimento de controles de acesso adequados, a utilização de soluções de segurança cibernética eficientes e a realização de auditorias periódicas. Além disso, é fundamental que os incidentes de perda de dados sejam prontamente comunicados e devidamente documentados, a fim de permitir uma resposta adequada e a implementação de medidas de remediação. A conformidade com as normas e regulamentações vigentes, como a Lei Geral de Proteção de Dados (LGPD), também desempenha um papel fundamental na prevenção da perda de dados e na mitigação dos danos decorrentes de incidentes.
R04 - Roubo	Pode ocorrer nas dependências internas do controlador/operador, sendo resultado de falhas nos controles de segurança dos sistemas. Essas falhas podem incluir a ausência ou utilização inadequada de criptografia, a existência de falhas no sistema que permitam a escalação de privilégios ou tratamentos indevidos, e outras vulnerabilidades similares. O roubo de dados representa uma séria violação da privacidade e da segurança das informações, podendo resultar em danos significativos para as partes afetadas, bem como para a reputação e a credibilidade da organização responsável pelo tratamento dos dados. Para mitigar esses riscos, é fundamental adotar medidas de segurança adequadas, como o estabelecimento de controles robustos de acesso, a

	implementação de sistemas de criptografia confiáveis, a realização de testes de vulnerabilidade e a aplicação de patches de segurança regularmente. Além disso, é essencial que a organização esteja em conformidade com as leis e regulamentos pertinentes, como a Lei Geral de Proteção de Dados (LGPD), a fim de garantir a proteção adequada dos dados e evitar violações de segurança. Em caso de ocorrência de roubo de dados, é imprescindível que a organização notifique imediatamente as autoridades competentes e tome todas as medidas necessárias para remediar o incidente, proteger os direitos dos titulares dos dados e mitigar os impactos negativos decorrentes do ocorrido.
R05 - Remoção não autorizada	A remoção não autorizada ocorre quando um usuário realiza a retirada ou cópia de dados pessoais para outro local sem a devida permissão. Essa ação constitui uma violação da privacidade e da segurança dos dados, podendo resultar em consequências graves para os titulares das informações e para a organização responsável pelo tratamento dos dados. É imprescindível que sejam estabelecidos controles adequados para prevenir e detectar tais remoções não autorizadas, garantindo assim a conformidade com as normas e regulamentações aplicáveis, como a Lei Geral de Proteção de Dados (LGPD). Além disso, é fundamental que a organização implemente medidas de segurança, como a atribuição de permissões de acesso adequadas, o monitoramento contínuo das atividades dos usuários e a aplicação de medidas técnicas e organizacionais para prevenir a remoção não autorizada de dados pessoais. Caso ocorra uma remoção não autorizada, é necessário agir prontamente, notificando as autoridades competentes, investigando o incidente e adotando as medidas corretivas necessárias para mitigar os danos e proteger os direitos dos titulares dos dados afetados.
R06 - Coleta excessiva	Ocorre quando são coletadas quantidades de informações além do estritamente necessário para a finalidade específica do tratamento ou atividade que fará uso desses dados. Essa conduta viola os princípios de proteção de dados, em especial o princípio da minimização, que estabelece a necessidade de limitar a coleta ao mínimo indispensável para o cumprimento da finalidade pretendida. É imprescindível que as organizações adotem medidas adequadas para evitar a coleção excessiva de dados pessoais, respeitando os princípios de proteção da privacidade e da minimização de informações. Isso inclui a definição prévia e clara das finalidades do tratamento, bem como a identificação dos dados estritamente necessários para atingir essas finalidades. Além disso, é fundamental que sejam implementados controles e procedimentos internos que garantam a conformidade com as normas e regulamentos aplicáveis, como a Lei Geral de Proteção de Dados (LGPD), a fim de evitar a coleta excessiva de dados pessoais. Caso seja identificada uma situação de coleção excessiva de dados, é necessário corrigir imediatamente essa prática, eliminando ou anonimizando as informações excedentes, de modo a garantir a adequação e a conformidade com as disposições legais e normativas aplicáveis. Isso contribui para proteger a privacidade dos indivíduos e promover uma cultura de respeito aos direitos fundamentais relacionados à proteção de dados pessoais.
R07 - Falha em considerar os direitos do titular dos dados pessoais	Acarreta violações que comprometem a proteção de sua privacidade e a garantia de seus direitos fundamentais. Entre as consequências dessa falha estão a perda do direito de acesso aos dados pessoais, a perda do direito de correção de informações incompletas, inexatas ou desatualizadas, bem como a perda do direito de eliminação dos dados pessoais, entre outros. O titular dos dados possui direitos fundamentais assegurados pela legislação de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil. Esses direitos

	incluem o direito de acessar seus dados pessoais e obter informações claras e transparentes sobre o tratamento realizado, o direito de retificar dados incorretos ou desatualizados, o direito de excluir os dados pessoais quando não forem mais necessários para a finalidade do tratamento, entre outros. Ao negligenciar esses direitos, as organizações descumprem suas obrigações legais e comprometem a confiança do titular dos dados. É fundamental que as empresas adotem políticas e práticas que garantam o respeito aos direitos do titular, estabelecendo mecanismos adequados para que os titulares possam exercer seus direitos de forma efetiva. Além disso, é importante destacar que a não observância dos direitos do titular dos dados pode acarretar responsabilização jurídica e em sanções previstas na legislação. A LGPD, por exemplo, prevê penalidades que variam desde advertências e multas até a suspensão parcial ou total do funcionamento do banco de dados utilizado para o tratamento dos dados pessoais. Portanto, é imprescindível que as organizações estejam cientes e considerem os direitos do titular dos dados pessoais em todas as etapas do tratamento, adotando medidas adequadas para garantir o exercício desses direitos e promover uma cultura de respeito à privacidade e proteção de dados.
R08 - Retenção prolongada de dados pessoais	Mesmo após o término da prestação de um serviço ou do prazo estabelecido para fins legais, configura uma prática em desacordo com as normas e regulamentos aplicáveis. Nesses casos, é imprescindível que ocorra a exclusão e/ou descarte seguro dos dados pessoais. Conforme estabelecido em legislações e regulamentações, como a Lei Geral de Proteção de Dados (LGPD), é fundamental que a retenção dos dados pessoais seja realizada apenas pelo tempo estritamente necessário para cumprir a finalidade para a qual foram coletados. Uma vez que essa finalidade é alcançada, os dados pessoais devem ser prontamente excluídos ou descartados de forma segura. A retenção prolongada dos dados pessoais além do necessário não apenas contraria as diretrizes legais e regulatórias, mas também representa um risco para a privacidade e segurança dos titulares dos dados. Manter informações pessoais desnecessárias por um período prolongado aumenta a exposição a potenciais violações de segurança e pode levar ao uso indevido desses dados. Assim, é fundamental que as organizações adotem políticas e procedimentos claros para a retenção e descarte seguro dos dados pessoais, garantindo o cumprimento dos requisitos legais e preservando a privacidade dos titulares dos dados. Isso envolve a implementação de práticas adequadas de gerenciamento de dados, incluindo a definição de prazos de retenção claros, a utilização de métodos de exclusão segura e a adoção de medidas de segurança para proteger os dados durante todo o ciclo de vida. A adoção de medidas adequadas de retenção e descarte de dados pessoais demonstra o compromisso da organização com a privacidade e a conformidade com as obrigações legais e normativas. Além disso, contribui para a minimização de riscos, a transparência no tratamento de dados pessoais e a proteção dos direitos dos titulares dos dados.

5.5.5.10. Foram apontadas, ainda, as medidas de mitigação dos riscos encontrados, bem como os efeitos esperados pelas ações tomadas para a atenuação de ameaças aos direitos dos titulares:

Risco	Medida(s)	Efeito sobre o Risco
R01: Acesso não autorizado	1. *Compliance* com a privacidade; 2. Controles criptográficos;	Reduzir

	3. Controle de acesso lógico; 4. Controle de acesso e privacidade; 5. Controles de segurança em redes, proteção física e do ambiente; 6. Desenvolvimento seguro; 7. Segurança web; 8. Registro de eventos, rastreabilidade e salvaguarda de logs; e 9. Respostas a incidentes.	
R02: Modificação não autorizada	Todas Já descritas no R01	Reduzir
R03: Perda	Todas Já descritas no R01	Reduzir
R04: Roubo	Todas Já descritas no R01	Reduzir
R05:Remoção não autorizada	Todas Já descritas no R01	Reduzir
R06: Coleção excessiva	Delineamento dos dados provenientes das Entidades Desportivas e das bases de checagem. · Tendo em vista o risco ser baixo, a própria elaboração do RIPD, onde foi definido os dados tratados e apresentados para a apreciação técnica da ANDP se torna, por si só, medidas suficientes.	Evitar
R07: Falha em considerar os direitos do titular dos dados pessoais	Participação individual e acesso. · Tendo em vista o risco ser baixo, a própria elaboração do RIPD, onde foi definido os dados tratados e apresentados para a apreciação técnica da ANDP se torna, por si só, medidas suficientes.	Evitar
R08: Retenção prolongada de dados pessoais sem necessidade.	1. Definição do prazo de retenção dos dados · A definição do prazo de retenção dos dados pessoais provenientes das Entidades Desportivas, retidos no MJSP, é estabelecida em até 20 (vinte) anos, considerando as finalidades justificadas no RIPD.	Evitar
	2. Descarte adequado de dados pessoais · Implementação de controles e sistemas de gestão que possibilitam a identificação e o descarte automatizado e apropriado dos dados pessoais após o término do período necessário para a finalidade específica. Um mecanismo tecnológico observa a data de inserção dos dados e, caso o período seja superior a 20 anos, ocorrerá a exclusão automática desses dados. · Avaliações periódicas para assegurar a conformidade contínua com os prazos de retenção estabelecidos. Quando necessário, os prazos serão revisados e atualizados de acordo com as mudanças	

	nas circunstâncias ou na legislação aplicável, garantindo a conformidade com as normas vigentes.	

5.5.5.11. O MJSP, assim, procurou suprir as deficiências apontadas nas medidas de mitigação e tratamentos dos riscos R06, R07, R09, R10 e R11, conforme elaboradas na primeira versão do RIPD. Observa-se, consoante já apontado nesta Nota Técnica, que nem todas as medidas propostas para a mitigação dos riscos apontados, em especial a coleção excessiva e a retenção prolongada de dados pessoais sem necessidade, foram suficientes para sanar os riscos indicados pela versão 2.0. do RIPD. Como já ressaltado, entende-se que há riscos de coleta excessiva de dados pessoais no projeto Estádio Seguro, bem como de retenção prolongada de dados pessoais sem necessidade.

6. CONCLUSÃO

6.1. Diante do exposto, acerca da análise da versão 2.0. do RIPD e da minuta do protocolo de execução do projeto Estádio Seguro, celebrados no âmbito do Acordo de Cooperação Técnica entre a CBF e o MJSP, considerando as competências que a Lei nº 13.709, de 14 de agosto de 2018, concedeu à Autoridade Nacional de Proteção de Dados (ANPD), em especial aquelas previstas no art. 31, nos incisos I, VI, VIII, XI e XX, todos do art. 55-J, bem como as atribuições que foram concedidas à Coordenação-Geral de Fiscalização desta ANPD, por meio do art. 17, *caput* e incisos III, VIII e XXIII do Regimento Interno da ANPD, conclui-se que:

· ***Sobre os agentes de tratamento.***

6.1.1. Os agentes de tratamento responsáveis pela execução do projeto Estádio Seguro foram devidamente identificados. Além disso, o Ministério da Justiça e Segurança Pública, por meio de obrigação expressa no inciso XVI da cláusula quinta do protocolo de execução, asseverou que apenas servidores públicos serão designados, em nome do órgão público federal, como gestores e responsáveis pela execução do projeto. Entretanto, o MJSP deve alterar o item 1. da versão 2.0 do RIPD, de maneira que o Diretor do Departamento de Projetos e de Políticas de Direitos Coletivos e Difusos da Secretaria Nacional do Consumidor seja indicado como o encarregado pelo tratamento de dados pessoais, conforme consta no sítio do órgão.

· ***Sobre a existência da base legal que autoriza o tratamento e o compartilhamento de dados pessoais.***

6.1.2. O tratamento de dados pessoais no âmbito do projeto Estádio Seguro encontra-se dentro das competências legais do órgão federal, bem como vai ao encontro de finalidades de interesse público, de maneira que se observa os parâmetros de tratamento de dados pessoais por órgãos do Poder Público, nos termos do art. 23 da LGPD.

6.1.3. A Lei nº 14.597, de 14 de junho de 2023, Lei Geral do Esporte, não pode ser considerada como norma autorizadora para a transmissão de dados pessoais de torcedores, coletados pelos clubes de futebol, ao Ministério da Justiça e Segurança Pública para fins da consecução dos objetivos do projeto Estádio Seguro, uma vez que a norma não definiu critérios, procedimentos e limites para o uso compartilhado de dados pessoais com órgãos do Poder Público. Compete ao MJSP, portanto, em virtude da inexistência de regulamentação específica sobre o tratamento de dados pessoais para finalidades exclusivas de segurança pública e atividades de investigação e repressão de infrações penais, conforme determinado pelo art. 4º, § 1º, da LGPD, assegurar que o tratamento de dados pessoais no âmbito do projeto Estádio Seguro seja realizado com o estrito cumprimento dos parâmetros definidos para a aplicação das normas de proteção de dados pessoais às exceções do art. 4º, inciso III, alíneas “a” e “d”, da LGPD.

6.1.4. O tratamento de dados pessoais para (i) prevenir falsificações, fraudes e outras práticas que contribuem para a evasão da receita decorrente do evento esportivo e (ii) garantir a segurança dos expectadores antes, durante e após o evento esportivo, é compatível com as competências legais do órgão público federal. Desse modo, o tratamento dos dados pessoais coletados no âmbito do projeto Estádio Seguro está relacionado a finalidades de interesse público, conforme definido no *caput* pelo art. 23 da LGPD.

6.1.5. O tratamento de dados pessoais pelas entidades privadas, no âmbito do projeto Estádio Seguro, deve ser tutelado pelo Ministério da Justiça e Segurança Pública, nos termos do §2º do art. 4º da

LGPD. Desse modo, cabe ao MJSP, sob o risco de prejudicar a cadeia de tratamento dos dados pessoais, assegurar que as entidades esportivas custodiantes dos dados pessoais dos torcedores indiquem, de forma clara e específica, a base legal que autoriza o seu uso compartilhado com órgão público federal, para o atingimento das finalidades específicas do projeto Estádio Seguro.

· ***Da observação dos princípios gerais de tratamento de dados pessoais.***

6.1.6. O MJSP deve restringir a coleta, o tratamento e o armazenamento de dados pessoais, no âmbito do projeto Estádio Seguro, apenas às finalidades específicas informadas ao titular, não sendo admitido tratamento posterior para o atendimento de finalidades genéricas. Desse modo, o tratamento de dados pessoais dos frequentadores dos eventos esportivos deverá ser limitado aos seguintes propósitos:

i. Identificação e recaptura de indivíduos com mandado de prisão em aberto e aplicação de medidas judiciais;

ii. Localização de pessoas maiores de idade registradas como desaparecidas;

iii. Identificação de torcedores que estão sujeitos a medidas judiciais restritivas, tais como a proibição de frequentar estádios, com o objetivo de aplicar as referidas medidas judiciais;

iv. Identificação da utilização indevida de dados de pessoas falecidas para a retirada de bilhetes e sua posterior revenda a preços elevados *("cambismo"*);

v. Combate à falsidade ideológica, por meio da identificação de inconsistências entre o CPF e a fotografia do torcedor, no intuito de prevenir que indivíduos procurados e impedidos adquiram ingressos utilizando CPF inexistentes e informações fictícias;

vi. Identificação e recuperação de veículos roubados ou furtados que adentrarem os estádios;

vii. Identificação e recaptura de proprietários de veículos procurados pela justiça; e

viii. Identificação de autores de delitos relacionados ao evento esportivo, como atos de violência, racismo, xenofobia, LGBTfobia e violação das regras de segurança praticados no período que antecede, coincide e prossegue após a partida.

6.1.7. O Ministério da Justiça e Segurança Pública indicou detalhadamente os dados pessoais dos frequentadores dos eventos esportivos que serão coletados no âmbito do projeto Estádio Seguro. Além disso, o órgão público federal associou os dados pessoais coletados à cada finalidade específica que justificou o seu recolhimento, bem como indicou as razões pelas quais o seu tratamento seria necessário para a consecução dos propósitos do projeto e as bases de verificação com as quais os dados pessoais recolhidos serão processados. Dessa forma, o MJSP procurou justificar a adequação e a necessidade da coleta de todos os dados pessoais dos frequentadores dos eventos esportivos que serão coletados, inclusive dos dados biométricos dos torcedores, para o atingimento das finalidades do projeto Estádio Seguro.

6.1.8. O compartilhamento dos dados pessoais de todos os frequentadores do evento esportivo, pelas entidades esportivas, é necessário para que o Ministério da Justiça e Segurança Pública possa, durante a fase de consciência situacional, identificar os sujeitos de interesse da justiça e segurança pública, conforme as finalidades do projeto. O MJSP, entretanto, deve deixar claro que serão coletados apenas os dados pessoais dos frequentadores dos eventos esportivos, conforme o limite imposto pelo art. 148 da nº 14.597, de 14 de junho de 2023, Lei Geral do Esporte. Desse modo, a coleta de dados pessoais de associados, membros, sócios-torcedores e membros de torcidas organizadas das entidades esportivas que não tiverem adquirido ingressos para a partida mostra-se excessiva tanto em relação às finalidades específicas do projeto Estádio Seguro quanto à autorização legislativa que permite a coleta dos dados.

6.1.9. A captação de dados pessoais, por meio do uso de imagens de câmeras de segurança, será legítima, desde que tenha como finalidade a prevenção da ocorrência de atos ilícitos no contexto da realização do evento esportivo e a identificação de indivíduos envolvidos em atividades ilícitas, como as descritas nas finalidades específicas do projeto. Desse modo, as imagens dos indivíduos poderão ser

capturadas somente quando a ação estiver relacionada à realização do evento esportivo, permitindo-se as filmagens no interior do estádio, nas suas proximidades e no percurso entre um ponto de concentração de torcedores e o estádio. A utilização de tecnologia de reconhecimento facial, associada a sistemas de monitoramento por vídeo, no entanto, deverá estar submetida ao envio de RIPD específico para a Autoridade Nacional de Proteção de Dados Pessoais.

6.1.10. A captação de dados pessoais, por meio do uso de imagens de câmeras de segurança, deverá ter como finalidade a identificação de indivíduos envolvidos em delitos, como atos de violência, racismo, xenofobia, LGBTfobia e violação das regras de segurança praticados no período que antecede, coincide e prossegue após a partida.

6.1.11. A retenção dos dados pessoais coletados para a consecução das finalidades (i) a (vii), após o encerramento do evento esportivo, excede a necessidade para a qual eles foram coletados junto às entidades esportivas, exceto quando os dados pessoais estiverem vinculados a pessoas de interesse da justiça e segurança pública que tenham sido devidamente identificadas após a etapa de consciência situacional. A retenção das imagens dos torcedores captadas por câmeras de vigilância, assim como dos dados biométricos compartilhados pelas entidades esportivas, para a identificação de indivíduos envolvidos em delitos, como atos de violência, racismo, xenofobia, LGBTfobia e violação das regras de segurança praticados no período que antecede, coincide e prossegue após a partida, é justificável, desde que o prazo de conservação dos dados pessoais seja limitado temporalmente, bem como seja proporcional em relação à finalidade para a qual eles foram coletados.

6.1.12. As imagens captadas dos torcedores por câmeras de vigilância, assim como os dados biométricos compartilhados pelas entidades esportivas, coletadas para finalidade específica (viii) devem ser mantidas por, no máximo, 30 (trinta) dias após o encerramento do evento esportivo, ressalvadas as situações em que autoridade policial ou administrativa ou o Ministério Público requeira ao MJSP a guarda por prazo superior, caso se verifique a necessidade de sua utilização no âmbito de investigações de atividades criminosas ocorridas antes, durante e após o evento esportivo.

6.1.13. O prazo de retenção de dados pessoais estipulado em 20 anos, conforme o prazo prescricional do artigo 109, inciso I, do Código Penal, é genérico, pois desconsidera as diversas finalidades para as quais os dados pessoais foram coletados, bem como é desproporcional, uma vez que se mostra excessivo em relação aos propósitos de tratamento relacionados ao projeto Estádio Seguro.

6.1.14. A proposta do projeto Estádio Seguro atenderia os requisitos de livre acesso e transparência, conforme os princípios definidos nos incisos IV e VI do artigo 6º da LGPD, ao garantir que:

i. os titulares serão informados sobre o processamento de seus dados pessoais, incluindo propósitos específicos, a finalidade do tratamento, a base legal, os direitos e o prazo de retenção, por meio de políticas de privacidade, avisos de segurança e comunicações específicas no momento da compra dos bilhetes;

ii. as informações relacionadas ao tratamento de dados pessoais no âmbito do projeto Estádio Seguro estarão disponíveis em transparência ativa, por meio do *link* https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/projeto-estadio-seguro; e

iii. as entidades esportivas estarão obrigadas, nos termos da cláusula quinta, inciso XI, da minuta do protocolo de execução, a afixar avisos sobre o tratamento de dados pessoais nas bilheterias físicas e nos acessos de estacionamento dos locais dos eventos.

6.1.15. Os aspectos de prevenção, segurança e responsabilização relacionados ao tratamento de dados pessoais no âmbito do projeto Estádio Seguro foram devidamente esclarecidos na versão 2.0 do RIPD. Em especial foram detalhadas questões referentes à realização de auditorias, tanto junto às empresas contratadas pelas EPDs, quanto em reação ao próprio ambiente da Plataforma Córtex, ao nível de segurança da autenticação desse sistema e ao acesso por terceiros, inclusive agentes públicos. Da mesma forma, foram listados os parâmetros administrativos que visam assegurar a qualidade e a integridade dos dados a serem tratados no âmbito do projeto.

6.1.16. O MJSP, assim, procurou suprir as deficiências apontadas nas medidas de mitigação e tratamentos de riscos verificadas na primeira versão do RIPD. Acredita-se, no entanto, que nem todas as

medidas propostas para a mitigação dos riscos apontados, em particular a coleta excessiva e a retenção prolongada de dados pessoais sem necessidade, foram suficientes para sanar os riscos indicados pela versão 2.0. do RIPD. Observa-se, desse modo, que há riscos de coleta excessiva de dados pessoais no projeto Estádio Seguro, bem como de retenção prolongada de dados pessoais sem necessidade.

· ***Dos direitos dos titulares***

6.1.17. Embora o MJSP afirme que os titulares dos dados pessoais poderão exercer seus direitos por meio do Sistema de Informação ao Cidadão e Ouvidoria, disponível em https://falabr.cgu.gov.br, nos termos da Lei nº 12.527/2011(Lei de Acesso à Informação – LAI), o órgão público federal deve informar os titulares quanto a possibilidade de restrição ao exercício do direito de acesso, caso a divulgação de informações relacionadas a inquéritos ou processos administrativos em andamento puder ser incompatível com o interesse público primários.

6.1.18. Igualmente, em atenção ao exposto no item 5.5.1.5, importa que seja esclarecido que há, no Poder Executivo Federal, dois mecanismos institucionais para o exercício de direitos previstos na LGPD, em especial aqueles relacionados ao art. 18, os quais são regidos por normas distintas e cujos procedimentos não são equiparáveis. Primeiro, para o exercício dos direitos de acesso, o titular pode utilizar os pedidos de acesso à informação, regidos pela Lei nº 12.527/2011 e pelo Decreto nº 7.724/2012. Segundo, para as demandas semelhantes a solicitações de providências, há as manifestações de ouvidoria, regulamentadas pela Lei nº 13.460/2017 e pelo Decreto nº 9.492/2018. A utilização do mecanismo institucional equivocado para o exercício dos direitos previstos na LGPD poderá prejudicar os titulares.

6.1.19. Ambas as recomendações de esclarecimentos podem ser atendidas pela disponibilização de instruções na página que traz as informações referentes ao tratamento de dados no âmbito do projeto, https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/projeto-estadio-seguro.

· ***Sobre o uso compartilhado de dados pessoais.***

6.1.20. Haverá, no âmbito do projeto Estádio Seguro, o tratamento compartilhado, por órgãos e entidades públicas, de dados e informações contidos em bancos de dados pessoais. O uso compartilhado de dados pessoais, por meio da Plataforma Córtex, porém, será realizado apenas com agentes públicos de entidades federativas devidamente conveniadas, nos termos da legislação aplicável, os quais deverão assinar previamente Termo de Compromisso e Manutenção do Sigilo (TCMS). Caberá ao Ministério da Justiça e Segurança Pública responsabilizar-se, nos termos do inciso VIII, da cláusula quinta do protocolo de execução, por verificar se os órgãos públicos com os quais compartilhará os dados pessoais dos frequentadores dos eventos esportivos, ainda que tenham sido devidamente identificados como sujeitos de interesse, cumprem todos os requisitos legais e administrativos necessários para realizar o tratamento dos dados pessoais recebidos.

6.1.21. O Ministério da Justiça e Segurança Pública não prestou maiores informações sobre a existência de acordos de cooperação ou de instrumentos legais que permitam a reproposição das bases de dados utilizadas para a verificação da identidade dos sujeitos de interesse, disponibilizadas por outros órgãos públicos, como o Tribunal Superior Eleitoral (TSE), a Receita Federal do Brasil (RFB), o Departamento Nacional de Trânsito (DENATRAN) e do Serviço Federal de Processamento de Dados (Serpro). A inexistência de instrumentos legais que indiquem a possibilidade de reutilização de dados pessoais coletados em função de obrigação legal, para finalidades incompatíveis com os propósitos que justificaram o seu recolhimento, pode ensejar na inobservância da legítima expectativa dos titulares e do princípio da finalidade, o que estaria em desacordo com o art. 6º, inciso I, da LGPD. O MJSP, portanto, deve se certificar de atualizar, ou de formalizar caso não existam, os instrumentos legais que permitem a reutilização das suas bases de verificação para os propósitos de segurança pública e atividades de investigação e repressão de infrações penais vinculadas ao projeto Estádio Seguro.

7. ENCAMINHAMENTOS

7.1. Por fim, tendo em vista as conclusões supramencionadas, encaminhe-se este documento à Secretaria-Geral, nos termos do art. 10, VIII, do Regimento Interno.

7.2. Sugere-se o encaminhamento desta Nota Técnica ao Ministério da Justiça e Segurança Pública para que:

a) tome conhecimento e providências em atenção às recomendações constantes nos itens 6.1.1 a 6.1.21 da Conclusão; e

b) no prazo de 10 dias úteis, se manifeste quanto aos trechos desta NT que devem ser tarjados, indicando os dispositivos legais que justifiquem a imposição de restrição de acesso, considerando que ela será tornada pública.

À consideração superior.

Brasília-DF, 09 de julho de 2024.

JORGE ANDRÉ FERREIRA FONTELLES DE LIMA
Coordenador de Fiscalização

De acordo. Encaminha-se.

Brasília-DF, 09 de julho de 2024.

FABRÍCIO GUIMARÃES MADRUGA LOPES
Coordenador-Geral de Fiscalização

_____

[1] Item 4.1 da versão 2.0 do relatório de impacto de proteção de dados.

[2] O projeto Estádio Seguro estará presente em todos os estados brasileiros que possuírem estádios de futebol, desde que as entidades desportivas de futebol profissional manifestem interesse na pactuação com o Acordo de Cooperação (item 25.1 da versão 2.0 do RIPD).

[3] Item 24.2 da versão 2.0 do RIPD.

[4] Item 24.3. da versão 2.0 do RIPD.

[5] Item 17.9. da versão 2.0 do RIPD.

[6] Item 17.10. da versão 2.0 do RIPD.

[7] Item 16 da da versão 2.0 do RIPD.

[8] WIMMER, Miriam. *Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia*. Revista Brasileira de Políticas Públicas. Volume 11, nº 01, Abril, 2021. p. 123-144.

[9] Disponível em https://www.gov.br/mj/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais. Acessado em 27/02/2024.

[10] TASSO, Fernando Antônio. Capítulo IV: Do tratamento de dados pessoais pelo Poder Público. *In* MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (coord.). LGPD: Lei Geral de Proteção de Dados (Comentada). 4.ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2022. p. 272.

[11]BARROSO, Luiz Roberto. *Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo*. 5 ed. Rio de Janeiro: Saraiva, 2015.

[12] *Ibid.*

[13] ABREU, Jacqueline de Souza. Tratamento de dados pessoais para a segurança pública: contornos do regime jurídico pós-LGPD. *In* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz; BIONI, Bruno (Coord.). Tratado de Proteção de Dados pessoais. 2. ed. Rio de Janeiro: Forense, 2023. p. 602.

[14] WIMMER, Miriam. *Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia*. Revista Brasileira de Políticas Públicas. Volume 11, nº 01, Abril, 2021. p. 123-144.

[15] *Ibid,* p. 123-144.

[16] TERWANGNE, Cécile. Article 5: Principles Relating to Processing of Personal Data. *In* KUNER, Chistopher (ed.). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford, UK: Oxford University Press, 2020. p.316.

[17] WIMMER, Miriam. *Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia*. Revista Brasileira de Políticas Públicas. Volume 11, nº 01, Abril, 2021. p. 123-144.

[18] TERWANGNE, Cécile. Article 5: Principles Relating to Processing of Personal Data. *In* KUNER, Chistopher *et all* (ed.). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford, UK: Oxford University Press, 2020. p.313.

[19] LINSKEY, Orla. *The foundations of EU data protection law*. Oxford, UK: Oxford University Press, 2015. p. 111.

[20] BASAN, Arthur Pinheiro. Art. 4º: limites hermenêuticos da LGPD. *In* MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (coord.). Comentários à Lei Geral de Proteção de Dados Pessoais: Lei nº 13.709/2018. Indaiatuba, SP: Editora Foco, 2022. p. 33 - 34.

[21] *Ibid,* p. 33 - 34.

[22] COLAÇO, Hian Silva; MENEZES, Joyceane Bezerra de. Quando a Lei Geral de Proteção de Dados não se aplica?. *In* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2 ed. São Paulo: Revista dos Tribunais, 2022. p. 183.

[23] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais: fundamentos da LGPD*. 1 ed. Rio de Janeiro: Forense, 2022. p. 45-46.

[24] Sistema Brasileiro de Inteligência, criado pela Lei nº 9.883, de 7 de dezembro de 1999, e regulamentado pelo Decreto nº 11.693, de 6 de setembro de 2023.

[25] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf

[26] Conforme a definição do art. 4º, inciso III, da Portaria nº 218, de 29 de setembro de 2021, API (Application Programming Interface, é a ponte com que se conectam dois sistemas, construída em linguagem capaz de ser compreendida por qualquer sistema, com o objetivo de prover ou receber dados e informações de um sistema, de sensores, ou de bases de dados, sendo também designada como webservice.

[27] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais: fundamentos da LGPD*. 1 ed. Rio de Janeiro: Forense, 2022. p. 74.

[28] *Ibid,* p. 73.

[29] TERWANGNE, Cécile. Article 5: Principles Relating to Processing of Personal Data. *In* KUNER, Chistopher (ed.). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford, UK: Oxford University Press, 2020. p. 315.

[30] *Ibid,* p. 315.

[31] Item 15.3. da versão 2.0 do RIPD.

[32] TERWANGNE, Cécile. Article 5: Principles Relating to Processing of Personal Data. *In* KUNER, Chistopher (ed.). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford, UK: Oxford University Press, 2020. p. 317.

[33] Legenda. SERPRO: Serviço Federal de Processamento de Dados; TSE: Tribunal Superior Eleitoral; RFB: Receita Federal do Brasil; BNMP-CNJ: Banco; Nacional de Mandado de Prisão - Conselho Nacional de Justiça; 2.0 e 3.0: Versão do Banco; SENATRAN: Sistema Nacional de Trânsito; BOPC-SINESP: Base de Boletim de Ocorrência das Polícias Civis - Sistema Nacional de Informações de Segurança Pública; CPF: Cadastro de Pessoa Física; MJSP: Ministério da Justiça e Segurança Pública; SIRC: Sistema Nacional de Informações de Registro Civil. *O número do bilhete configura-se como o elemento primordial de conexão entre o CPF do indivíduo e o procedimento de bloqueio na catraca. Nota. Dado Primário:

informação mínima necessária, proveniente da Entidade Desportiva - Ticketeira ou Estádio, utilizada como elemento principal, como o CPF e Placa Veicular, para cruzamento e geração dos indicativos.

[34] Legenda. SERPRO: Serviço Federal de Processamento de Dados; TSE: Tribunal Superior Eleitoral; RFB: Receita Federal do Brasil; BNMP-CNJ: Banco; Nacional de Mandado de Prisão - Conselho Nacional de Justiça; 2.0 e 3.0: Versão do Banco; SENATRAN: Sistema Nacional de Trânsito; BOPC-SINESP: Base de Boletim de Ocorrência das Polícias Civis - Sistema Nacional de Informações de Segurança Pública; CPF: Cadastro de Pessoa Física; MJSP: Ministério da Justiça e Segurança Pública; SIRC: Sistema Nacional de Informações de Registro Civil. Nota. Dado Primário: informação mínima necessária, proveniente da Entidade Desportiva - Ticketeira ou Estádio, utilizada como elemento principal, como o CPF e Placa Veicular, para cruzamento e geração dos indicativos. Dados Secundários: informações mínimas necessárias, como foto, nome e data de nascimento, que acompanham o CPF e funcionam como fatores de confirmação das informações. Dados Complementares: informações mínimas necessárias provenientes da Entidade Desportiva - Ticketeira, utilizadas como elementos adicionais para auxiliar ações de inteligência em segurança pública.

[35] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais: fundamentos da LGPD*. 1 ed. Rio de Janeiro: Forense, 2022. p. 56.

[36] DE TEFFÉ, Chiara Spadaccini & RAAD FERNANDES, Elora. Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites. *In* TEPEDINO, Gustavo (coord.); SILVA, Rodrigo da Guia (coord.). *Direito Civil na era da inteligência artificial*. 1 ed. São Paulo: Thomson Reuters. Brasil, 2020. p. 284 – 315.

[37] *Ibid,* p. 284 – 315

[38] *Ibid,* p. 284 – 315

[39] Item 17.16, versão 2.0. do RIPD.

[40] Item 16.4., alínea “d” e item 17.18 da versão 2.0 do RIPD.

[41] Itens 17.18 e 17.19 da versão 2.0. do RIPD.

[42] LINSKEY, Orla. *The foundations of EU data protection law*. Oxford, UK: Oxford University Press, 2015. p.108 – 110.

[43] HOFFMAN-RIEM, Wolfgang. *Teoria geral do direito digital: transformação digital: desafios para o direito*. 2 ed. Rio de Janeiro: Forense, 2022. p. 19-23

[44] *Ibid,* p. 19-23.

[45] ABREU, Jacqueline de Souza. Tratamento de dados pessoais para a segurança pública: contornos do regime jurídico pós-LGPD. *In* MENDES, Laura Schertel (coord.); DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); RODRIGUES JR, Otavio Luiz (coord.); BIONI, Bruno (coord.). *Tratado de Proteção de Dados pessoais*. 2 ed. Rio de Janeiro: Forense, 2023. p. 600-601.

[46] *Ibid,* p. 600-601.

[47] *Ibid,* p. 600-601.

[48] Item 12.5 da versão 2.0. do RIPD.

[49] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais: fundamentos da LGPD*. 1 ed. Rio de Janeiro: Forense, 2022. p. 86-87.

[50] QUINELATO, Pietra Daneluzi. Seção IV: Do término do tratamento de dados pessoais. *In* MARTINS, Guilherme Magalhães (coord.); LONGHI, João Victor Rozatti (coord.); FALEIROS JÚNIOR, José Luiz de Moura (coord.). *Comentários à Lei Geral de Proteção de Dados Pessoais: Lei nº 13.709/2018*. Indaiatuba, SP: Editora Foco, 2022. p. 201-202.

[51] *Ibid,* p. 201-202.

[52] (i) Identificação e recaptura de indivíduos com mandado de prisão em aberto e aplicação de medidas judiciais; (ii) Localização de pessoas maiores de idade registradas como desaparecidas; (iii) Identificação de torcedores que estão sujeitos a medidas judiciais restritivas, tais como a proibição de frequentar

estádios, com o objetivo de aplicar as referidas medidas judiciais; (iv) Identificação da utilização indevida de dados de pessoas falecidas para a retirada de bilhetes e sua posterior revenda a preços elevados (cambismo); (v) Combate à falsidade ideológica, por meio da identificação de inconsistências entre o CPF e a fotografia do torcedor, no intuito de prevenir que indivíduos procurados e impedidos adquiram ingressos utilizando CPF inexistentes e informações fictícias; (vi) Identificação e recuperação de veículos roubados ou furtados que adentrarem os estádios; (vii) Identificação e recaptura de proprietários de veículos procurados pela justiça.

[53] Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

[54] TASSO, Fernando Antônio. Capítulo IV: Do tratamento de dados pessoais pelo Poder Público. *In* MALDONADO, Viviane Nóbrega (coord.); OPICE BLUM, Renato (coord.). *LGPD: Lei Geral de Proteção de Dados (Comentada)*. 4 ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2022. p. 272.

[55] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais: fundamentos da LGPD*. 1 ed. Rio de Janeiro: Forense, 2022. p. 147.

[56] BRASIL. Autoridade Nacional de Proteção de Dados. *Guia orientativo Tratamento de dados pessoais pelo Poder Público, versão 2.0*. Brasília, 2023.

[57] VI - Transparência aos titulares dos dados: os titulares dos dados serão informados sobre o processamento de suas informações pessoais, incluindo os propósitos específicos, os direitos dos titulares e as medidas de segurança adotadas. Por exemplo, serão disponibilizadas políticas de privacidade detalhadas no momento da coleta de dados.

[58] I - Transparência e Informação: caso necessário, serão fornecidas ao titular dos dados informações claras, completas e acessíveis sobre o tratamento de seus dados pessoais, incluindo a finalidade do tratamento, a base legal, os direitos do titular, o prazo de retenção de dados. Parte dessas informações já serão disponibilizadas por meio de política de privacidade, avisos de privacidade e comunicações específicas no momento da compra dos bilhetes.

[59] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional. § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei. § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento. § 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá: I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência. § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento. § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que

repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador. § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

[60] https://www.gov.br/acessoainformacao/pt-br/central-de-conteudo/publicacoes/arquivos/aplicacao_lai_2edicao.pdf

[61] XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

[62] BURITI, Arlos Roberto. *Proteção de dados pessoais em face do Estado: direito à privacidade*. Curitiba: Juruá, 2021. p 138 a 141.

[63] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais: fundamentos da LGPD*. 1 ed. Rio de Janeiro: Forense, 2022. p.95.

[64] Item 30.1. da versão 2.0 do RIPD.

Documento assinado eletronicamente por **Jorge André Ferreira Fontelles de Lima**, **Coordenador(a)**, em 09/07/2024, às 19:22, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Fabrício Guimarães Madruga Lopes**, **Coordenador(a)-Geral de Fiscalização**, em 09/07/2024, às 19:36, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0132350** e o código CRC **15CC6C07**.