Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Fiscalização

Nota Técnica nº 175/2023/CGF/ANPD

## 1. INTERESSADO

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

1.2. Confederação Brasileira de Futebol (CBF).

## 2. ASSUNTO

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).

## 3. REFERÊNCIAS

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 nº 4374407);

3.4. Acordo {***/2023/GM} (SEI nº 4374421);

3.5. Anexo Protocolo de Execução 1/20233 (SEI nº 4374450);

3.6. Relatório de Impacto à Proteção de Dados Pessoais (SEI nº 4375287);

3.7. 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;

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

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

3.10. 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;

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

3.12. 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;

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

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

3.15. 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 (DIOPI) do Ministério da Justiça e Segurança Pública (MJSP), por intermédio de seu encarregado, em que a DIOPI 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 objetivo promover ações de combate ao racismo e à violência nos estádios brasileiros, com a aplicação de tecnologias para, por exemplo, verificar se o comprador de ingressos para jogos 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, SEI nº 4375287).

4.3. Em 21 de junho de 2023, por intermédio do Ofício nº 111/2023/CGDI/AESP/GM/MJ (SEI nº 4374407), 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 4374524), que solicita apreciação e opinião técnica nos termos do §2º do art. 4º da Lei nº 13.709/2018 de três documentos que o acompanham: a minuta Acordo {***/2023/GM} (SEI nº 4374421), o Anexo Protocolo de Execução 1/20233 (SEI nº 4374450) e o Relatório de Impacto à Proteção de Dados Pessoais (SEI nº 4375287).

4.4. Em 29 de junho de 2023, por meio do Despacho GABPR (SEI nº 4374530), os autos foram encaminhados a esta Coordenação-Geral de Fiscalização (CGF) para conhecimento e adoção das providências consideradas cabíveis.

4.5. Considerando o alcance do Projeto, que impacta parcela significativa de cidadãos brasileiros; a relação desse Projeto com os princípios de proteção de dados descritos na Lei Geral de Proteção de Dados Pessoais (LGPD), em acordo com o art. 4º, §§ 1º e 3º, da LGPD; e a indicação do Poder Público como um setor prioritário no Relatório de Ciclo de Monitoramento 2022 (SEI nº 4505844), justificou-se a instauração de procedimento de fiscalização para acompanhar o desenvolvimento do Projeto (Despacho CGF, SEI nº 4645225).

4.6. É o relatório.

## 5. ANÁLISE

### A COMPETÊNCIA DA ANPD E DA INCIDÊNCIA DA LGPD

5.1. Insta salientar que, embora haja exceção prevista na legislação para o tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, III, da Lei nº 13.709/2018 - LGPD), tal tratamento deve observar o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD, de acordo com o disposto no §1º do artigo 4º da mesma lei.

5.2. Além disso, a LGPD expressamente atribui à ANPD a competência para emitir opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do artigo 4º da Lei, e o dever de solicitar aos responsáveis o relatório de impacto à proteção de dados pessoais, de acordo com o disposto no §3º desse mesmo artigo 4º.

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
>
> (…)
>
> III - realizado para fins exclusivos de:
>
> a) segurança pública;
>
> b) defesa nacional;
>
> c) segurança do Estado; ou

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**

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

**§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais**.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) [Grifamos]

5.3. Ainda, ressaltamos a competência da Autoridade Nacional de Proteção de Dados como órgão fiscalizador e responsável último pela interpretação da LGPD, conforme Art. 55-J, inciso XX da mesma lei.

Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019)

(...)

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (Incluído pela Lei nº 13.853, de 2019).

5.4. Incontestes, por conseguinte, tanto a incidência da LGPD sobre a referida atividade, quando envolver tratamento de dados pessoais, quanto a competência da ANPD para emitir opinião técnica e recomendações.

**DO ESCOPO DA ANÁLISE**

5.5. **1.5.** A presente Nota Técnica tem por objetivo avaliar, à luz do disposto nos §§ 1º e 3º do art. 4º da LGPD, o tratamento de dados pessoais no âmbito do Projeto Estádio Seguro, propor a adoção de providências para fazer cessar violações às disposições da LGPD e apresentar as implicações e possíveis consequências da não adoção dessas providências, por intermédio da análise dos documentos encaminhados a esta CGF nos autos do processo SEI nº 00261.001722/2023-13: minuta Acordo {***/2023/GM} (SEI nº 4374421), o Anexo Protocolo de Execução 1/20233 (SEI nº 4374450) e o Relatório de Impacto à Proteção de Dados Pessoais (SEI nº 4375287).

5.6. **1.6.** Para tanto, serão examinados o atendimento ao interesse público; a observância do devido processo legal; a observância aos princípios previstos no art. 6º da LGPD; as hipóteses de compartilhamento de dados; o atendimento às vedações de tratamento de dados por pessoa de direito privado previstas nos §§ 2º e 4º do art. 4º da LGPD; a disponibilidade de mecanismos e procedimentos estabelecidos e padronizados para assegurar o exercício dos direitos dos titulares previstos no art. 18 da LGPD; e a indicação dos encarregados de proteção de dados responsáveis.

**CONSIDERAÇÕES PRELIMINARES**

5.7. Entende-se que alguns elementos da LGPD, tais como o devido processo legal, os princípios gerais de proteção de dados e os direitos do titular devem ser também considerados e, desde já, ponderados em atividades de tratamento de dados cuja finalidade seja a investigação e repressão de infrações penais.

5.8. A partir da análise dos documentos encaminhados, foi possível identificar as finalidades principais da operação de compartilhamento de dados no âmbito do Projeto Estádio Seguro: (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 o cambismo.

5.9. No entanto, cumpre observar que não foi possível diferenciar quando o compartilhamento é feito para a primeira finalidade, de recapturar indivíduos com mandado de prisão ou medidas penais restritivas ou para a terceira, de evitar a venda de ingressos utilizando dados de pessoas falecidas, combatendo o cambismo. Tal circunstância força a conclusão de que ocorrem de forma simultânea e sem uma análise prévia de qual das duas finalidades está sendo alcançada.

5.10. Assim, considerando as disposições dos §§1º e 3º do art. 4º, da LGPD, e, ainda, que as duas finalidades, primeira e terceira, são atingidas na mesma operação de tratamento de dados pessoais, qual seja, o tratamento de dados compartilhados pela Entidade de Prática Desportiva (EPD) com o MJSP e demais órgãos de segurança pública, a presente análise trará um mesmo conjunto de recomendações para as três finalidades, com foco nos princípios da LGPD.

5.11. Cumpre destacar que o caso concreto trata do compartilhamento de dados coletados por entidade privada com o Poder Público. A aplicação do Decreto nº 10.046/2019, portanto, assume caráter subsidiário, trazendo luz a questões que envolvam o compartilhamento de dados pessoais quando uma das partes é o Poder Público, já que o Decreto dispõe apenas sobre "o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União".

5.12. Inicialmente, o Decreto nº 10.046/2019 é expresso ao determinar a necessidade de observância da LGPD nos compartilhamentos de dados pessoais realizados entre entidades e órgãos públicos federais (art. 3º, I, V e VI; art. 5º).

Decreto nº 10.046/2019

Art. 3º O compartilhamento de dados pelos órgãos e entidades de que trata o art. 1º observará as seguintes diretrizes:

I - a informação do Estado será compartilhada da forma mais ampla possível, observadas as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais;

II - o compartilhamento de dados sujeitos a sigilo implica a assunção, pelo recebedor de dados, dos deveres de sigilo e auditabilidade impostos ao custodiante dos dados;

III - os mecanismos de compartilhamento, interoperabilidade e auditabilidade devem ser desenvolvidos de forma a atender às necessidades de negócio dos órgãos e entidades de que trata o art. 1º, para facilitar a execução de políticas públicas orientadas por dados;

IV - os órgãos e entidades de que trata o art. 1º colaborarão para a redução dos custos de acesso a dados no âmbito da administração pública, inclusive, mediante o reaproveitamento de recursos de infraestrutura por múltiplos órgãos e entidades;

V - **nas hipóteses em que se configure tratamento de dados pessoais, serão observados o direito à preservação da intimidade e da privacidade da pessoa natural**, a proteção dos dados e as normas e os procedimentos previstos na legislação; (Redação dada pelo Decreto nº 11.266, de 2022)

VI - a coleta, o tratamento e o compartilhamento de dados por cada órgão serão realizados nos termos do disposto no art. 23 da Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais; (Redação dada pelo Decreto nº 11.266, de 2022)

VII - **a eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados pessoais**, nos termos do disposto no inciso I do caput do art. 6º da Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais; (Incluído pelo Decreto nº 11.266, de 2022)

VIII - **a compatibilidade do tratamento de dados pessoais com as finalidades informadas**, nos termos do disposto no inciso II do caput do art. 6º da Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais; e (Incluído pelo Decreto nº 11.266, de 2022)

IX - **a limitação do compartilhamento de dados pessoais ao mínimo necessário para o atendimento da finalidade informada**, nos termos do disposto no inciso III do caput do art. 6º da Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais, e o cumprimento integral dos requisitos, das garantias e dos procedimentos estabelecidos na referida Lei, no que for compatível com o setor público. (Incluído pelo Decreto nº 11.266, de 2022)

(...)

Art. 5º (…).

§ 1º Os órgãos e entidades de que trata o art. 1º, **para os compartilhamentos de dados pessoais, darão publicidade às hipóteses em que compartilhem ou tenham acesso a banco de dados pessoais**, nos termos do disposto no inciso I do caput do art. 23 da Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais. (Incluído pelo Decreto nº 11.266, de 2022)

§ 2º **As informações sobre compartilhamento de dados pessoais estarão disponíveis em veículos de fácil acesso nos sítios eletrônicos, deverão ser claras e atualizadas**, e conterão a previsão legal do compartilhamento, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades. (Incluído pelo Decreto nº 11.266, de 2022)

§ 3º **O compartilhamento de dados nos níveis de categorização restritos e específicos serão autorizados pelo gestor de dados e seu processo será formalizado por documentos de interoperabilidade** cuja solicitação seguirá os critérios estabelecidos pelo Comitê Central de Governança de Dados, em observância: (Incluído pelo Decreto nº 11.266, de 2022)

I - aos dispositivos: (Incluído pelo Decreto nº 11.266, de 2022)

a) da Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais; (Incluída pelo Decreto nº 11.266, de 2022)

b) da Lei nº 14.129, de 29 de março de 2021; e (Incluída pelo Decreto nº 11.266, de 2022)

c) da Lei nº 12.527, de 18 de novembro de 2011; (Incluída pelo Decreto nº 11.266, de 2022)

II - **às orientações da Autoridade Nacional de Proteção de Dados**; e (Incluído pelo Decreto nº 11.266, de 2022)

> III - às normas correlatas. (Incluído pelo Decreto nº 11.266, de 2022)
>
> **§ 4º Nas solicitações de interoperabilidade que envolvam dados pessoais, serão explicitados, além do disposto no § 3º:** (Incluído pelo Decreto nº 11.266, de 2022)
>
> **I - o propósito legítimo, específico e explícito**; (Incluído pelo Decreto nº 11.266, de 2022)
>
> **II -a compatibilidade com a finalidade**; e (Incluído pelo Decreto nº 11.266, de 2022)
>
> **III - o compartilhamento do mínimo necessário para atendimento da finalidade**. (Incluído pelo Decreto nº 11.266, de 2022)

5.13. Destarte é oportuno que a ANPD apresente recomendações visando a regularizar esta atividade de compartilhamento, tendo agido bem o MJSP em comunicar esta Autoridade.

5.14. Além disso, esse procedimento deve ser seguido para os demais compartilhamentos já realizados com outras entidades e órgãos públicos, bem como os que venham a ser fruto de compartilhamento no futuro.

5.15. A análise a seguir é dividida em três partes. Primeiro, analisa-se qual procedimento deve ser seguido pelo MJSP para esta atividade de compartilhamento de dados. Em segundo, é analisado o tratamento objeto do compartilhamento à luz dos princípios da LGPD, de modo a verificar em que medida eles são respeitados. Em terceiro, são apresentadas observações pontuais sobre os documentos apresentados.

## DO DEVIDO PROCESSO LEGAL, DOS PRINCÍPIOS E DOS DIREITOS DOS TITULARES

*Dos Agentes de Tratamento e do Encarregado*

5.16. O RIPD (SEI nº 4375287) cuida de identificar, logo no seu início, os agentes de tratamento responsáveis e o Encarregado. Tal provisão, considerando que o escopo do Acordo é o compartilhamento de dados pessoais, é boa prática e merece destaque nesta Nota Técnica. A clara identificação dos agentes de tratamento facilita que os envolvidos se tornem cientes de suas competências e obrigações previstas na LGPD.

5.17. Por oportuno, cabe observar que o MJSP indicou a Coordenação-Geral de Inteligência CGINT/DIOPI/SENASP como operador. Muito embora não seja propriamente um erro, cumpre esclarecer que a indicação do operador, quando ele se constitui em órgão do próprio controlador – MJSP – acaba por se tornar uma denominação ineficaz.

5.18. A designação do operador, considerando a estrutura da LGPD baseada em riscos e que distribui competências e obrigações, se presta a estabelecer os limites e responsabilidades dos agentes de tratamento, a exemplo do que dispõe o art. 42. Quando tanto o controlador quanto o operador se confundem na mesma pessoa jurídica, não há uma efetiva distribuição de responsabilidades, já que todas continuam concentradas no controlador. Nesse sentido, recomenda-se a leitura do tópico *4. Operador* constante no Guia para Definições de Agentes de Tratamento de Dados Pessoais e do Encarregado, que foi publicado pela ANPD[1].

> 58. De acordo com a LGPD, pessoas físicas e jurídicas de direito público e privado podem atuar como operadoras. Na maior parte das vezes, o operador é uma pessoa jurídica, que é contratada pelo controlador para realizar o tratamento de dados, conforme as instruções deste último. Contudo, não há óbices para que uma pessoa natural contratada como prestadora de serviços para uma finalidade específica possa ser considerada operadora de dados.
>
> 59. Em caso de pessoa jurídica, importa destacar que a organização ou empresa é entendida como agente de tratamento, de forma que seus funcionários apenas a representam. Assim como explicado no tópico 2.2 e de forma análoga à definição de controlador, **a definição legal de operador também não deve ser entendida como uma norma de distribuição interna de competências e responsabilidades**.

5.19. Ainda sobre a designação do operador, é oportuno citar que no parágrafo 5.3.1. do RIPD, que versa sobre *Medidas para Assegurar a Conformidade do Operador*, consta referência a termo de compromisso e manutenção de sigilo e a orientações técnicas que seriam firmados pelo operador. Considerando que a primeira parte do RIPD apresenta a CGINT como operador, não ficou claro se a palavra operador foi empregada no mesmo sentido nestas duas ocasiões, sobretudo porque há referência expressa ao art. 5º, VII da LGPD nesse parágrafo 5.3.1.

5.20. Por oportuno, diante da possibilidade de que o RIPD, no parágrafo 5.3.1, esteja compreendendo o operador como pessoa física integrante do MJSP, vale nova referência ao Guia para Definições de Agentes de Tratamento de Dados Pessoais e do Encarregado que esclarece:

> 60. **Nesse cenário, 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 o operador será sempre uma pessoa distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos.

5.21. Considerando a possível relação do exposto no parágrafo 5.3.1. com o princípio da segurança, deve o MJSP ajustar o RIPD para esclarecer esta questão, considerando o exposto nos itens acima.

*Do Interesse Público*

5.22. Nesse instante, cabe verificar se há interesse público no tratamento pelo MJSP de dados pessoais compartilhados pela Entidade de Prática Desportiva (EPD).

5.23. O tratamento de dados pessoais no âmbito da inteligência está condicionado ao art. 4º, §§1º a 4º da LGPD e deve ser capaz de demonstrar o interesse público e a vinculação do tratamento com as atribuições legais do órgão ou entidade que atuará como controlador.

5.24. Segundo afirmado no parágrafo 2.1. do Relatório de Impacto à Proteção de Dados, foi desenvolvido, dentro da Plataforma Córtex, um subsistema destinado às atividades de segurança pública em competições desportivas de grandes eventos.

> (...) O objetivo desse subsistema é utilizar a infraestrutura existente da Plataforma para estabelecer conexões com os Pontos de Vendas (PDV) das entidades esportivas e de entretenimento, com o intuito de gerar conhecimento que auxilie na prevenção de crimes envolvendo torcedores e frequentadores de eventos.
>
> 2.2 O Projeto Estádio Seguro, como parte desse subsistema modular, tem como principal objetivo aumentar a efetividade na recaptura de indivíduos com mandado de prisão ou medidas penais restritivas. Além disso, visa evitar a venda de ingressos utilizando informações de pessoas falecidas fornecidas pelo comprador, com o propósito de combater o cambismo. Essas ações estão em apoio aos serviços de inteligência das Unidades da Federação, por meio da Plataforma Córtex, possibilitando a produção de conhecimento qualificado, oportuno e eficiente para embasar ações policiais efetivas.

5.25. De acordo com o informado, foi possível identificar as finalidades principais da operação de compartilhamento de dados no âmbito do Projeto Estádio Seguro: (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 o cambismo.

5.26. As três finalidades remetem à condução de atividades de investigação e repressão de infrações penais.

5.27. Em diversos trechos do RIPD, como nos parágrafos 2.3., 2.8., 2.9., 2.11., e do Plano de Trabalho, nos parágrafos 2.1. e 2.2., por exemplo, fica caracterizado o embasamento formal do interesse público do MJSP para realizar o tratamento proposto nas finalidades (i) a (iii), seja na escolha da plataforma tecnológica, seja pela aderência das finalidades declaradas para o tratamento com a finalidade da atividade de inteligência.

5.28. No RIPD, parágrafo 2.9., por exemplo, é afirmado que a DIOPI atua alinhada com a Política Nacional de Inteligência de Segurança Pública PNISP (Decreto nº 10.777/21) e com a Estratégia Nacional de Inteligência de Segurança Pública - ENISP (Decreto nº 10.778/21) "*na exata abrangência que se faz necessário para identificar ameaças, riscos e oportunidades, tanto ao País como a população*".

5.29. Oportunamente, o RIPD registra e informa que está reconhecido na ENISP a importância da atividade de inteligência ao elencar desafios e objetivos estratégicos com destaque ao combate à criminalidade organizada e violenta e ao uso e modernização de ferramentas tecnológicas de ponta. Tal previsão vai ao encontro do proposto no Projeto Estádio Seguro, no que se refere ao tratamento dos dados pessoais necessários à consecução de seu objeto.

5.30. Todavia, quanto à terceira finalidade – combate ao cambismo –, esta análise parte da presunção de que o MJSP, ao usar a palavra cambismo, se refere às condutas tipificadas como crimes nos art. 166 e 167 da Lei nº 14.597/2023, o que fundamentaria o interesse público e justificaria a coleta e o tratamento de dados pessoais. Nesse sentido, 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.

*Do Devido Processo Legal, do Princípio da Segurança e da Prevenção*

5.31. O §1º do art. 4º da LGPD expressamente determina a observância do devido processo legal, dos princípios da LGPD e dos direitos dos titulares no tratamento

de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do estado e atividades de investigação e repressão de infrações penais.

5.32. Quanto ao devido processo legal, importa sua análise sob dois aspectos, considerando o caso concreto. O primeiro diz respeito ao rito mínimo necessário à formalização do compartilhamento dos dados pessoais. O segundo trata dos cuidados que o MJSP, ao trazer esses dados pessoais para sua tutela, deve tomar para impedir o seu uso indevido e o desvio de finalidade, o que poderia resultar no abuso em prejuízo ao direito fundamental à proteção de dados.

5.33. No que diz respeito ao primeiro aspecto, a garantia do devido processo legal é condição *sine qua non* para autorizar atividades de compartilhamento de dados pessoal, ainda mais quando este ocorrer em escala massiva. Nesse sentido, cabe citar o acórdão do Supremo Tribunal Federal – STF, na ocasião do julgamento da Ação direta de Inconstitucionalidade (ADI) nº 6387, em que se analisou o compartilhamento de dados por empresas prestadoras de serviço telefônico fixo e móvel com o Instituto Brasileiro de Geografia e Estatística (IBGE).

5.34. No julgado, o STF destacou a importância do devido processo legal ao concluir que este não foi atendido pela MP nº 954/2020, uma vez que ela não definiu apropriadamente como e para que seriam utilizados os dados coletados, e não ofereceu condições de avaliação quanto à adequação e necessidade do compartilhamento, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para o alcance dessas finalidades.

5.35. Por oportuno, acerca das formalidades necessárias, emprestam-se as diretrizes do Decreto nº 10.046/2019. Observe-se que, mesmo para compartilhamento entre entidades e órgãos públicos federais, o Decreto expressamente chama atenção para a necessidade de formalização do compartilhamento (art. 5º, §3º).

5.36. No que diz respeito a compartilhamento de dados entre órgãos públicos ou a partir de órgãos públicos, a ANPD tem reiteradamente se manifestado no sentido de que, quando se trata de dados pessoais, o compartilhamento deve ser precedido de análises técnica e jurídica, além de emissão de decisão administrativa motivada pela autoridade competente, da qual constem a motivação e as condições a serem observadas no caso, em conformidade com o disposto na LGPD, especificamente no art. 26, §2º, e no Decreto nº 10.046/2019[2].

5.37. Nesse mesmo sentido, consta no Guia para Tratamento de Dados Pessoais pelo Poder Público:

> **( a ) Formalização e registro**
>
> O uso compartilhado de dados pessoais pelo Poder Público deve ser formalizado, seja em atenção às normas gerais que regem os procedimentos administrativos, seja em atenção à obrigatoriedade de registro das operações de tratamento, conforme disposto no art. 37 da LGPD. Para tanto, recomenda-se a instauração de processo administrativo, do qual constem os documentos e as informações pertinentes, incluindo análise técnica e jurídica, conforme o caso, que exponham a motivação para a realização do compartilhamento e a sua aderência à legislação em vigor.
>
> Além disso, recomenda-se que o compartilhamento seja estabelecido em ato formal, a exemplo de contratos, convênios ou instrumentos congêneres firmados entre as partes. Outra possibilidade é a expedição de decisão administrativa pela autoridade competente, que autorize o acesso aos dados e estabeleça os requisitos definidos como condição para o compartilhamento.[3]

5.38. No caso concreto, verifica-se que essas formalidades estão sendo observadas. Há uma minuta de acordo de cooperação técnica, com plano de trabalho detalhado; e foi apresentada uma minuta do protocolo de execução detalhando ainda mais as atividades, competências, obrigações e responsabilidades decorrentes do tratamento dos dados pessoais.

5.39. Nessa mesma esteira, especialmente no que concerne à minuta de ACT (SEI nº 4374421), vale citar a previsão constante na Subcláusula Primeira da Cláusula Quarta:

> Cláusula Quarta – Da Operacionalização
>
> (...)
>
> SUBCLÁUSULA PRIMEIRA. As iniciativas previstas no Plano de Trabalho deste Acordo de Cooperação que impliquem em armazenamento, tratamento ou transferência de dados entre os signatários terão suas linhas básicas, atividades e ações constituídas, especificadas e implementadas por meio de Protocolos de Execução específicos firmados entre o MJSP e a CBF, **nos quais estarão prescritas todas as disposições que garantam a responsabilidade pelo tratamento e custódia dos dados pessoais, a ampla proteção dos dados pessoais e o pleno cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD)**, **especialmente mediante a prévia consulta da Autoridade Nacional de Proteção de Dados - ANPD sobre os termos do respectivo Protocolo**. [Grifamos]

5.40. Adicionalmente, observa-se que a proposta de compartilhamento de dados pessoais foi precedida de análises técnica e jurídica, consubstanciadas no RIPD (SEI nº 4375287) e no Parecer nº 381/2023/CONJUR-MJSP/CGU/AGU.

5.41. Para o segundo aspecto, que trata dos cuidados que o MJSP deve tomar para impedir o uso indevido desses dados, o cumprimento do devido processo legal é imprescindível, já que traz garantia adicional de que o tratamento de dados pessoais realizado pela ferramenta não sofrerá desvio da sua finalidade primária.

5.42. Para tanto, o devido processo legal requer controle e auditabilidade, a fim de que seja possível verificar se os atos administrativos não restringem de forma arbitrária os direitos e garantias fundamentais dos cidadãos brasileiros, que abrange também o direito pétreo à proteção de seus dados pessoais, conforme inciso LXXIX do artigo 5º da Constituição Federal.

5.43. Dessa forma, o devido processo legal age também como instrumento para a mitigação de riscos. A seguir, apresentam-se algumas reflexões sobre o caso numa análise conjunta com o princípio da segurança e o princípio da prevenção.

5.44. Conforme prescrito no art. 6º, VII e VIII, da LGPD, os princípios da segurança e da prevenção dizem respeito à utilização de medidas técnicas e administrativas capazes de proteger os dados pessoais de acesso não autorizado e de situações que possam acarretar a perda, destruição, alteração, comunicação ou difusão destes. Esses princípios se referem, ainda, à adoção de medidas que possam prevenir danos decorrentes do tratamento dos dados pessoais.

5.45. A partir do exposto no RIPD, especialmente nos parágrafos 2.4., 3.1.9. a 3.1.23., 5.2.1. e 5.4.2., é possível observar que foram tomadas medidas técnicas e administrativas que guardam relação com o princípio da segurança. Há gestão de perfis de usuário, no intuito de controlar o acesso ao sistema com os dados pessoais, com competências e acesso gerenciados e discriminantes, que permitem distintas possibilidades de segmentação de acesso ao conteúdo.

5.46. Nesse sentido, a partir do exposto na parte de análise de riscos, observa-se que os riscos cibernéticos foram considerados (R01 a R05) e foram apresentadas medidas técnicas aparentemente suficientes para reduzir os riscos a um patamar aceitável (parágrafo 7.4. do RIPD, p. 22 a 28).

5.47. Algumas dessas medidas preveem registros (logs) de uso, de movimentação e de acesso que permitem auditorias. Tais funcionalidades devem ser consideradas em conjunto com a previsão de mecanismo de supervisão, pela figura do Corregedor/Auditor, que tem a responsabilidade de analisar as atividades realizadas pelos usuários, com o objetivo de garantir a conformidade com as políticas estabelecidas, e identificar eventuais desvios e tomando as medidas corretivas necessárias. A existência dos registros e do mecanismo de supervisão cria um ambiente institucional que tende a inibir o uso indevido desses dados e o desvio de finalidade ou que, ao menos, torne possível sua detecção e responsabilização *ex post*.

5.48. É imprescindível que o órgão mantenha um registro de acesso/logs, tendo em vista o princípio do devido processo legal e da responsabilização e prestação de contas. É importante que seja estabelecido um mecanismo que permita verificar em que momentos e contextos os dados foram acessados e quais os gestores responsáveis por esse acesso.

5.49. Nessa senda, a partir das informações prestadas pelo órgão, no que se refere aos princípios da segurança e da prevenção, não se vislumbrou a necessidade de expedir recomendações ao MJSP.

*Do Princípio da Finalidade*

5.50. Com relação à finalidade do tratamento dos dados pessoais, a entidade informa que: "o tratamento de dados pessoais no âmbito da Diretoria de Operações Integradas e de Inteligência tem por objetivo (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 o cambismo, de modo a identificar ameaças, riscos e oportunidades, tanto ao país como à sua população".

> RIPD
>
> 2.1. No ano de 2023, foi desenvolvido, dentro da Plataforma Córtex, um subsistema modular destinado às atividades de segurança pública em Competições Desportivas e Grandes Eventos. O objetivo desse subsistema é utilizar a infraestrutura existente da Plataforma para estabelecer conexões com os Pontos de Vendas (PDV) das entidades esportivas e de entretenimento, com o intuito de gerar conhecimento que auxilie **na prevenção de crimes envolvendo torcedores e frequentadores de eventos**.
>
> 2.2. O Projeto Estádio Seguro, como parte desse subsistema modular, tem como principal objetivo aumentar a efetividade na recaptura de indivíduos com mandado de prisão ou medidas penais restritivas. Além disso, visa evitar a venda de ingressos utilizando informações de pessoas falecidas fornecidas pelo comprador, com o propósito de combater o cambismo. Essas ações estão em apoio aos serviços de inteligência das Unidades da Federação, por meio da Plataforma Córtex, possibilitando a produção de conhecimento qualificado, oportuno e eficiente para embasar ações policiais efetivas.

5.51. Informações igualmente pertinentes sobre a finalidade constam no Plano de Trabalho:

> Identificação do Objeto
>
> 1.1. O presente instrumento tem por objeto a cooperação técnica entre o Ministério da Justiça e Segurança Pública, a Confederação Brasileira de Futebol - CBF e suas entidades afiliadas que vierem a aderir ao Acordo de Cooperação, **para o desenvolvimento de ações de interesse comum, visando à consecução finalística das políticas de segurança pública para tornar os ambientes da prática do futebol profissional brasileiro mais seguro – Projeto Estádio Seguro**.
>
> (...)
>
> Diagnóstico
>
> 2.6. Neste sentido, salienta-se que a formalização de Acordo de Cooperação para ações conjuntas de interesse público, como **o recebimento das bases de dados e fluxo de informações provenientes das entidades de prática desportiva detentoras do mando de jogo e da parte gestora dos estádios**, deverá proporcionar o conhecimento necessário à tomada de decisões administrativas e operacionais, **e a implementação de bancos de dados centralizados de Segurança Pública, a serem empregados exclusivamente para a atividade finalística dos operadores e agentes de segurança pública devidamente aderentes e cadastrados para operar a plataforma**, nos termos legislação aplicável.
>
> (...)
>
> Objetivos Gerais e Específicos
>
> 5.2. Objetivos Gerais:
>
> I - Promover ações em conjunto, bem como promover a troca de dados e informações entre o MJSP, a CBF e agremiações aderentes para tornar os estádios de futebol ambientes mais seguros e inclusivos.
>
> (...)
>
> 5.3. Objetivos específicos:
>
> I - Promover a integração de dados e informações de interesse para a segurança pública para o monitoramento de alvos móveis identificáveis em torno de Estádios de futebol profissional.
>
> II - Promover a integração de dados e informações de interesse para a segurança pública provenientes das vendas de bilhetes de eventos relacionados a jogos de futebol profissional.
>
> III - Promover a integração de dados e informações de interesse para a segurança pública provenientes da movimentação nas catracas nos estádios em jogos de futebol profissional.
>
> IV - Promover o tratamento dos dados e informações e integração para o fluxo das informações da venda dos bilhetes e da verificação dos bilhetes na catraca em estádio em jogos de futebol profissional.
>
> V - Promover a disponibilidade dos alertas, em tempo real, às equipes da segurança pública em atuação em jogos de futebol profissional.
>
> (...)

5.52. Tal pretensão do MJSP é compatível com as competências previstas nos artigos 25 e 28 do Anexo I, do Decreto nº 11.348/2023. Dentre tais competências, destacam-se (i) o processo decisório quanto às políticas de segurança pública; (ii) o planejamento, a coordenação e a integração de atividades de inteligência de segurança pública em âmbito nacional; e (iii) a promoção, com os órgãos componentes do Sistema Brasileiro de Inteligência, da integração e o compartilhamento de dados e conhecimentos necessários à tomada de decisões administrativas e operacionais pela Secretaria Nacional de Segurança Pública (Senasp).

5.53. Aduz, ainda, que o tratamento de dados a ser realizado encontra fundamento na necessidade de cumprimento de obrigação legal do controlador, no tratamento de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis e regulamentos, no exercício regular de direitos e proteção da vida ou a incolumidade física do titular e, em especial, de terceiros.

5.54. O princípio da finalidade, de acordo com o art. 6º, I, da LGPD, pode ser traduzido na realização do tratamento de dados para propósitos legítimos, específicos, de forma explícita e informada ao titular, sem a possibilidade de tratamento posterior para outros fins. A rigor, é possível entender que a exigência de vinculação à execução de finalidade específica constitui verdadeiro freio democrático para impedir o uso abusivo pelo Poder Público dos dados que coleta dos cidadãos, normalmente de modo impositivo. O requisito de que toda finalidade deve ser informada ao titular será analisada no [item 5.70].

5.55. Considerando o exposto nos parágrafos 3.1.1. a 3.1.8., 3.4.2. e 3.4.3., **se vislumbrou, a partir das informações prestadas pelo órgão, que o tratamento de dados pessoais possui propósitos legítimos para utilização dos dados obtidos por meio do ACT celebrado**, ainda mais legitimado pelo compromisso de realizar ampla informação ao titular do uso de tais dados, conforme consta no parágrafo 5.4.1. do RIPD e que será avaliado com mais atenção adiante.

*Dos Princípios da Adequação e Necessidade*

5.56. No que tange aos princípios da adequação e da necessidade do tratamento para atendimento do interesse público, o órgão assim esclarece nos parágrafos 5.1.1. e 5.4.3. do RIPD:

> 5.1.1. O tratamento de dados pessoais no âmbito do projeto Estádio Seguro (...) encontra fundamento na necessidade de cumprimento de obrigação legal do controlador, no tratamento de dados necessários à execução, pela administração pública, de políticas públicas previstas em Leis e regulamentos, no exercício regular de direitos e proteção da vida ou a incolumidade física do titular e, em especial, de terceiros.
>
> (…)
>
> 5.4.3. Minimização de Dados: o projeto Estádio Seguro se limita a coleta e o processamento de dados pessoais ao mínimo necessário para atingir a finalidade específica do tratamento. São adotadas medidas para garantir que apenas os dados estritamente relevantes e indispensáveis sejam tratados, reduzindo assim os riscos e preservando a privacidade dos titulares dos dados.

5.57. Conforme disposto nos incisos II e III do art. 6º, da LGPD, o princípio da adequação trata da "*compatibilidade do tratamento com as finalidades informadas ao titular*" e o princípio da necessidade, por sua vez, diz respeito à "*limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados*".

5.58. A fim de analisar a compatibilidade do tratamento proposto com os princípios acima, é preciso fazer uma comparação entre a finalidade declarada pelo agente de tratamento, os dados pessoais que serão obtidos e as inferências que serão realizadas a partir deles durante o tratamento.

5.59. Por uma questão lógica, é preciso que a finalidade já tenha sido analisada e entendida como legítima e compatível com a LGPD. Tal questão foi enfrentada no tópico anterior, em que se constatou finalidade legítima para utilização dos dados obtidos por meio do ACT celebrado.

5.60. Acerca dos dados pessoais, nos parágrafos 3.2.1. a 3.2.3. do RIPD, o MJSP informa que serão tratados *dados do titular* (nome, data de nascimento, CPF, passaporte) e *dados do evento e da compra* (código da partida e número do evento, data e hora da compra do bilhete, tipo da compra, número do pedido e do bilhete, setor e portão de entrada, número de identificação da catraca, assento adquirido pelo comprador, número do bilhete registrado na catraca, data e hora do registro do bilhete na catraca, número da catraca e localização da catraca utilizada pelo titular).

5.61. O tratamento de tais dados é compatível com as finalidades (i) e (iii) constantes no [item 5.50] desta Nota Técnica e com os procedimentos descritos nos parágrafos 3.1.1. a 3.1.8. do RIPD. Consequentemente, **se vislumbrou, a partir das informações prestadas pelo órgão, que o tratamento de dados pessoais para essas duas finalidades atende ao princípio da necessidade.**

5.62. A mesma afirmação não cabe para a finalidade de (ii) recuperação de veículos roubados ou furtados. Não há qualquer menção aos dados que serão tratados para atingi-la, eles são apenas vagamente mencionados no tópico "10. Plano de Ação" do Plano de Trabalho que acompanha a minuta de ACT (SEI nº 4374421):

| | EIXO | AÇÃO | RESPONSÁVEL | PRAZO | SITUAÇÃO |
|---|---|---|---|---|---|
| I | Promoção da integração de dados e informações de interesse para a segurança pública para o monitoramento de alvos móveis identificáveis. | Encaminhar, via API para a STI do MJSP, os dados e as informações relativas ao registro das passagens e movimentações de veículos registrados pelas câmeras do estacionamento do estádio em tempo real e com imagem. | Entidades de Práticas Desportivas | 30 dias após a celebração do Protocolo de Execução vinculado ao AC | - |

5.63. A ausência de informação acerca de quais dados pessoais serão tratados para essa finalidade impede qualquer apreciação acerca da sua observância aos princípios da necessidade e da adequação.

5.64. **Portanto, não ficou esclarecido como o órgão atenderá aos princípios da necessidade e adequação no que tange à finalidade de (ii) recuperação de veículos roubados ou furtados. Dessa forma, o MJSP deve acrescentar ao RIPD os dados que serão tratados e como serão tratados, nos mesmos moldes do realizado para as outras duas finalidades acima.**

5.65. Igualmente, consta no eixo V do tópico "10. Plano de Ação", do Plano de Trabalho do ACT, que a EPD, no momento da venda, deve capturar o registro facial

do comprador ou beneficiário e encaminhá-lo, via API, ao MJSP.

| EIXO | | AÇÃO | RESPONSÁVEL | PRAZO | SITUAÇÃO |
|---|---|---|---|---|---|
| V | Promoção da integração de dados e informações de interesse para a segurança pública provenientes das vendas de bilhetes. | Capturar, no momento da venda (on-line e física) ou repasse do bilhete, ainda que nos casos de cortesia, o registro facial do comprador ou beneficiário, ou associados e membros, ou sócio-torcedores, membros de torcidas organizadas, com obrigatoriedade para indivíduos com idade ≥ 18 anos e ≤ 80 anos, encaminhando, via API para a STI do MJSP ou de outra forma a ser ajustada entre as partes, quando aplicável. | Entidades de Práticas Desportivas | 365 dias após a celebração do Protocolo de Execução vinculado ao AC | - |

5.66. A foto da face do cidadão, neste caso, deve ser entendida como dado biométrico, uma vez que passará por um sistema de reconhecimento automatizado que possibilita a identificação do titular de dados. Conforme a LGPD, art. 5º, II, dados biométricos são considerados dados sensíveis e merecem um maior nível de proteção.

5.67. Todavia, não há qualquer menção à foto, a dados pessoais biométricos ou sensíveis nos dados discriminados nos parágrafos 3.2.1. a 3.2.3. do RIPD. O RIPD é documento essencial para a regularidade do tratamento que se pretende realizar – seja do ponto de vista formal, porque é obrigação da ANPD (art. 4º, §3º da LGPD) requisitá-lo, seja do ponto de vista material, porque somente a partir da análise das informações contidas nele se torna possível à ANPD cumprir seu papel legal. Dessa sorte, o descasamento entre o previsto no RIPD e o que consta no ACT invalida o segundo naquilo que excede o previsto no primeiro.

5.68. **Portanto, 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 Relatório em questão. Qualquer tratamento do dado biométrico de registro facial antes disso configura tratamento irregular.**

5.69. Adicionalmente, resta destacar o fato de que se pretende coletar a data de nascimento do titular. Aparentemente, tal coleta se justifica para discriminar aqueles titulares cujos dados devem ser repassados pela EPD ao MJSP. **Se tal presunção é verdadeira, 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 idade serão repassados ao MJSP. Do contrário, fica prejudicada a utilidade da coleta da data de nascimento para as finalidades declaradas e tal dado não deve ser coletado pelo MJSP neste tratamento**.

*Dos Princípios da Transparência e Livre Acesso*

5.70. Os princípios do livre acesso e da transparência estão positivados no art. 6º, VI e IV, da LGPD, respectivamente, e garantem ao titular a consulta facilitada e gratuita aos dados tratados e à forma e duração do tratamento, além da prestação de informações claras e precisas sobre a realização do tratamento e sobre seus respectivos agentes de tratamento.

5.71. Além disso, a autodeterminação informativa é fundamento previsto da LGPD e tem como objetivo assegurar certo controle do cidadão sobre informações que se referem a ele. Uma vez que os princípios da transparência e do livre acesso não são observados, tolhe-se também o direito à autodeterminação informativa do titular dos dados pessoais.

5.72. No que se refere ao cumprimento dos princípios da transparência e do livre acesso, o MJSP esclarece, no parágrafo 5.4.1. do RIPD que "*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 e os eventuais compartilhamentos de dados. Essas informações serão disponibilizadas por meio de política de privacidade, avisos de privacidade e comunicações específicas no momento da compra dos bilhetes*." Tal previsão, do ponto de vista formal, parece adequada.

5.73. Por oportuno, cabe celebrar toda previsão de realizar a devida informação aos titulares de dados. Em qualquer situação, quando há tratamento ou compartilhamento de dados pessoais, é importante que haja comunicação pública sobre esta intenção para que o titular de dados e a sociedade estejam a par da iniciativa.

5.74. Do ponto de vista material, cabe algum esclarecimento. Inicialmente, importa ressaltar que, de acordo com o art. 9º da LGPD, o fornecimento de informações ao titular de dados é algo necessário, não se aplicando a condicional "caso necessário" do parágrafo 5.4.1. do RIPD – ainda que tal transparência esteja modulada pelos aspectos que serão tratados nos tópicos a seguir.

5.75. No intuito de dar ciência ao titular do tratamento de dados pessoais sob análise, consta na Cláusula Sexta do Protocolo de Execução (SEI nº 4374450) como obrigação da EPD:

> II - Informar aos compradores de ingressos e/ou torcedores convidados, no momento da compra dos ingressos ou recebimentos dos convites, de que os dados pessoais serão compartilhados com MJSP para fins de segurança pública;

5.76. Previsão semelhante pode ser encontrada no Plano de Trabalho (SEI nº 4374421):

> 6. METODOLOGIA DE INTERVENÇÃO
>
> 6.1. A entidade aderente enviará ao Ministério da Justiça e Segurança Pública os dados das bases constantes no item 5.3, em periodicidade e forma definidas entre os partícipes em Protocolo de Execução, **sendo o repasse dos dados condicionado ao prévio conhecimento do adquirente do ingresso ou sócio-torcedor do repasse dos dados pessoais ao MJSP para tratamento no âmbito de execução de política de segurança pública.** [Grifamos]
>
> (...)
>
> 10. Plano de Ação
>
> Item XII - Informar ao comprador ou beneficiário, ou associados e membros, ou sócio-torcedores, membros de torcidas organizadas, no momento da venda (on-line e física) ou no repasse do bilhete, ainda que nos casos de cortesia, que os dados e informações pessoais serão tratados pelos órgãos de segurança pública para fins de segurança pública.

5.77. O princípio da finalidade dispõe que o tratamento deve ser realizado "para propósitos legítimos, específicos, explícitos **e informados ao titular**, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". Observe-se que, para fins de atendimento aos princípios da transparência e da finalidade, qualquer um dos três textos acima está amplo e não adequado. O caráter genérico da mensagem é incompatível com a previsão do parágrafo 5.4.1. do RIPD do MJSP.

5.78. Importa que a mensagem ao titular de dados não só ocorra nos moldes do previsto no parágrafo 5.4.1. do RIPD, mas também reflita de modo fiel a finalidade declarada para o tratamento, a exemplo do exposto nos parágrafos 2.2., 3.1.1., 3.4.2., 3.4.3. do RIPD.

5.79. No caso de uso pelo Poder Público de dados compartilhados, as informações pertinentes devem ser amplamente divulgadas, igualmente em seus sítios eletrônicos, conforme previsto no art. 23, I, da LGPD, norma que guarda consonância com as disposições da Lei de Acesso à Informação (Lei nº 12.527/2011). Tal constatação é confirmada pela disposição do art. 3º, I, e do art. 5º do Decreto nº 10.046/2019, que veio a ser reforçada pelas alterações trazidas pelo Decreto nº 11.266, de 25 de novembro de 2022, com a inclusão dos §§ 1º a 3º ao art. 5º do Decreto nº 10.046/2019:

> Art. 5º Fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de dados entre os órgãos e as entidades de que trata o art. 1º, observadas as diretrizes do art. 3º e o disposto na Lei nº 13.709, de 2018.
>
> § 1º Os órgãos e entidades de que trata o art. 1º, **para os compartilhamentos de dados pessoais, darão publicidade às hipóteses em que compartilhem ou tenham acesso a banco de dados pessoais**, nos termos do disposto no inciso I do caput do art. 23 da Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais. (Incluído pelo Decreto nº 11.266, de 2022)

5.80. Assim, os atos normativos que regem e autorizam o compartilhamento de dados pessoais devem prever a publicidade a toda a sociedade sobre as finalidades pretendidas, assim como as categorias de dados compartilhadas e informações sobre os agentes de tratamento, incluindo a divulgação do compartilhamento no sítio eletrônico dos órgãos e entidades envolvidos.

5.81. Isto significa que não são apenas as finalidades do compartilhamento que devem ser informadas aos cidadãos, mas também quais dados são compartilhados e quais os agentes de tratamento envolvidos. Tal informação não é protegida por nenhuma hipótese de sigilo legal que justifique a restrição de acessá-la – pelo contrário: o art. 23, I, define explicitamente a sua publicidade, a qual deve ser preferencialmente concretizada por transparência ativa.

5.82. Dessa forma, entende-se necessário que seja dada transparência ao compartilhamento de dados pessoais realizado pela EPD e MJSP com as demais polícias, no sítio eletrônico dos órgãos e entidades envolvidos, informando as finalidades pretendidas, as categorias de dados compartilhadas e informações sobre os agentes de tratamento envolvidos.

5.83. Em tempo, com relação aos princípios elencados no art. 6º da LGPD, norteadores dos direitos dos titulares de dados pessoais, é possível entender que, em alguns tratamentos, especialmente naqueles previstos no art. 4º III, sua aplicação deve se dar em consonância com a finalidade do tratamento de dados pessoais no caso

concreto. Essa análise permite compatibilizar, de um lado, o valor social que o princípio protege, e de outro, a própria finalidade da atividade de tratamento - segurança pública -, que também tem um valor social em si.

5.84. Nesse sentido, como exemplo, é compreensível que garantir aos titulares dos dados coletados o acesso irrestrito a certas informações, como os procedimentos operacionais descritos nos parágrafos 3.1.1. a 3.1.8., poderá inviabilizar o objetivo do tratamento dos dados pessoais, motivo pelo qual nem tudo deve ser objeto de transparência ou livre acesso. Cabe citar que a própria Lei de Acesso à Informação (Lei nº 12.527/2011) no art. 23, VIII, prevê a restrição de acesso a essas informações.

5.85. Assim, nos termos expostos no item acima, tendo em foco a compatibilidade entre os princípios e a própria finalidade da atividade de tratamento, tais princípios precisam ser atendidos. 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.

5.86. Constitui dever e testemunho de boa-fé da EPD e do MJSP garantir que conste:

5.86.1. 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;

5.86.2. 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[4].

5.87. Para além dos aspectos acima tratados, o MJSP informa, no parágrafo 5.1.3. do RIPD, que o MJSP dispõe de canal próprio, Sistema de Informação ao Cidadão e Ouvidoria, implementado pela plataforma https://falabr.cgu.gov.br, o que também contribui para o atendimento ao princípio do livre acesso e para que que os titulares dos dados pessoais possam exercer os direitos previstos no art. 18 LGPD:

> 5.1.3. Ademais, o Ministério da Justiça e Segurança Pública dispõe de canal próprio, o Sistema de Informação ao Cidadão e Ouvidoria, implementado pela plataforma https://falabr.cgu.gov.br, para que os titulares dos dados pessoais possam demandar as solicitações previstas no Art. 18 LGPD, cujos pedidos serão analisados de acordo com a LAI e as normas que regem a atividade de inteligência enquanto não houver a norma específica prevista no §1 do Art. 4º da LGPD.

5.88. Em adição à previsão no parágrafo 5.1.3. do RIPD, o atendimento ao princípio do livre acesso depende de o titular ter ciência de que seus dados estão sendo tratados. O seu atendimento fica, assim, vinculado ao quanto o princípio da transparência é efetivamente atendido.

*Do Princípio da Qualidade*

5.89. Este princípio estipula que cabe ao agente de tratamento garantir aos titulares a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

5.90. Importa esclarecer que o parágrafo 5.2.1., único neste tópico do RIPD, não trata do princípio da qualidade. Apresenta, todavia, informações que contribuem para a análise da adequação à luz dos princípios da prevenção e segurança, bem como ao devido processo legal, e foi analisado junto com as demais informações pertinentes a eles.

5.91. Do ponto de vista das finalidades 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, tendo em vista o entendimento de que os dados pessoais serão coletados no ato da compra do bilhete e tratados para fins de controle de acesso ao evento esportivo, fica bastante reduzida a possibilidade de tratamento de dados desatualizados ou inexatos.

5.92. Considerando as informações prestadas pelo MJSP, não se vislumbra a necessidade de tecer maiores considerações ou recomendações no que se refere a essas finalidades quanto a esse princípio.

5.93. No que se refere à finalidade de (ii) auxiliar na recuperação de veículos roubados ou furtados, entretanto, a falta de algumas informações no RIPD impede que se possa avaliar o tratamento quanto ao princípio da qualidade. O MJSP deve, por conseguinte, acrescentar ao RIPD esclarecimentos sobre como pretende garantir a exatidão, clareza, relevância e atualização dos dados.

*Da Frequência do Tratamento e do Tempo de Retenção dos Dados Pessoais*

5.94. Quanto à frequência em que os dados são tratados, o MJSP assim informa no RIPD:

> 3.2.4. Frequência em que os dados são tratados: os dados serão recebidos e tratados a cada partida de futebol, quando a entidade desportiva com mando de campo aderir ao acordo de cooperação. Os dados tratados serão encaminhados à autoridade policial militar e à autoridade de polícia judiciária indicados na Portaria que estabelecerão uma comissão específica para a operacionalização de solução tecnológica de interesse da segurança pública em competições desportivas no respectivo Estado.

5.95. Sobre este aspecto, especificamente sobre o compartilhamento dos dados que serão encaminhados à autoridade policial militar e à autoridade de polícia judiciária, o RIPD não deixa claro se serão os dados de todos os cidadãos que frequentarão o evento esportivo ou apenas os dados de sujeitos de interesse (que acusem problema de falha na validação biométrica, suspeitos de usar documento falso ou outro tipo de ocorrência).

5.96. Cabe lembrar que, ainda que o propósito seja a preservação da ordem pública e da incolumidade das pessoas e do patrimônio com o objetivo de garantir o bem-estar e a segurança da sociedade diante de situações que possam ameaçá-la ou causar dano, não se pode conceber o acúmulo e a produção de conhecimento despropositado sob a justificativa de proteger a sociedade de seus próprios cidadãos, quando não há motivo razoável senão em relação a uma parcela reduzida de cidadãos cujo contexto fático destoa do cidadão médio.

5.97. Desta forma, 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).

5.98. No que toca ao tempo de retenção dos dados pelo órgão público, é importante frisar que o tratamento de dados pessoais é um processo com duração definida, após o qual os dados pessoais devem ser eliminados, ressalvadas as hipóteses em que é autorizada a sua conservação, previstas no art. 16 da LGPD. A delimitação do tempo de duração do uso dos dados é relevante e é importante que conste, inclusive, no RIPD.

5.99. Apesar de não constar como um princípio, o tempo de retenção tem vinculação direta com os princípios da qualidade, da necessidade e adequação e, neste caso específico, com o princípio da finalidade declarado nos parágrafos 2.1. e 2.2. do RIPD. A previsão de exclusão dos dados, mais do que boa prática, é condição para um tratamento regular.

5.100. Sobre o tempo de retenção, a partir das informações prestadas pelo MJSP, percebe-se claramente o momento em que os dados são utilizados para a finalidade declarada a partir do exposto no parágrafo 3.2.4. do RIPD.

5.101. Todavia, nos parágrafos 3.2.5., 5.4.4. do RIPD, o MJSP informa que os dados serão mantidos de acordo com sua tabela de temporalidade para documentos do MJSP[5], aprovada por portaria do Arquivo Nacional[6].

5.102. Segundo o MJSP, a tabela de temporalidade prevê um prazo de guarda de 50 anos e guarda permanente para documentos de inteligência.

| Código | Descritor do Código | Prazo de Guarda | | Destinação Final | Observações |
|---|---|---|---|---|---|
| | | Fase Corrente | Fase Intermediária | | |
| 330 | Gestão da Inteligência em Segurança Pública | | | | |
| 331 | Implantação e Monitoramento | Até aprovação das contas pelo TCU ou até a apresentação do Relatório de Gestão | 30 anos | Guarda permanente | Eliminar, após 5 anos, os documentos referentes às contratações não efetivadas. |
| 332 | Produção de Conhecimento de Inteligência e Contrainteligência | 5 anos | 50 anos | Guarda permanente | |
| 333 | Atendimento às instituições de Segurança Pública | 5 anos | 20 anos | Eliminação | |

5.103. Ainda no documento aprovado pelo Arquivo Nacional, assim o MJSP estabelece o escopo de aplicação da tabela de temporalidade:

1. Definição e Conceitos

O código de classificação de documentos de arquivo é um instrumento de gestão utilizado para**classificar todo e qualquer documento produzido ou recebido pelo Ministério da Justiça e Segurança Pública no exercício de suas funções e atividades, inclusive em meio digital**. A classificação por assuntos é utilizada com o objetivo de agrupar os documentos sob um mesmo tema, como forma de agilizar sua recuperação e facilitar as tarefas arquivísticas relacionadas com a avaliação, seleção, eliminação, transferência, recolhimento e acesso a esses documentos, uma vez que o trabalho arquivístico é realizado com base no conteúdo do documento, o qual reflete a atividade que o gerou e determina o uso da informação nele contida.

5.104. Sobre os documentos que se encaixam nesta categoria, constam as seguintes descrições:

**330 Gestão da Inteligência em Segurança Pública**

Nas subdivisões deste descritor classificam-se documentos referentes às atividades de implantação e monitoramento dos sistemas, agências, redes e centros integrados de inteligência em segurança pública, bem como a produção de conhecimento de inteligência e contrainteligência.

**331 Implantação e Monitoramento**

Incluem-se documentos referentes à implantação e monitoramento dos sistemas, agências, redes e centros de inteligência em segurança pública.

**332 Produção de Conhecimento de Inteligência e Contrainteligência**

Incluem-se documentos referentes a atividades de produção de conhecimento de inteligência e contrainteligência, além da análise associativa e avaliação de riscos na área de Segurança Pública.

**333 Atendimento às Instituições de Segurança Pública**

Incluem-se documentos referentes às atividades de produção e suporte tecnológico da Rede Nacional de Inteligência de Segurança Pública, tais como o cadastramento de usuários e instituições, suporte técnico para atendimento a todos os usuários, criação de certificados digitais.

5.105. Como se pode observar do quanto exposto, a tabela de temporalidade diz respeito a documentos produzidos ou recebidos pelo MJSP no exercício de suas funções e atividades.

5.106. Ocorre que a noção de documento não se confunde e nem deve ser igualada ao conjunto de dados pessoais tratados no âmbito deste ACT. Igualmente, não é e nem dever ser automática, implícita ou presumida, a aplicação da tabela de temporalidade a qualquer conjunto de dados pessoais.

5.107. A confirmar este entendimento, cabe citar a própria definição atribuída a documento de inteligência, constante no parágrafo 3.2.6. do RIPD, a partir do que o MJSP afirma constar na Doutrina Nacional de Inteligência e que estabelece o que é conhecimento de inteligência:

3.2.6. Nesse contexto geral é importante ressaltar que o armazenamento dos dados tem como finalidade subsidiar a produção de conhecimento de inteligência no âmbito da Coordenação Geral de Inteligência (CGINT/DIOPI/SENASP), em conformidade com os princípios estabelecidos na Doutrina Nacional de Inteligência de Segurança Pública (DNISP)[4]. A Doutrina Nacional de Inteligência de Segurança Pública estabelece que os conhecimentos produzidos pelas Agências de Inteligência (AIs) pertencentes ao Subsistema de Inteligência de Segurança Pública (SISP) devem ser formalizados em Documentos de Inteligência, incluindo os RELINTs, e disponibilizados ao tomador de decisão a ser assessorado, bem como a outras AIs. Nesse contexto, é fundamental observar os princípios do sigilo, da oportunidade e da necessidade de conhecer.

5.108. A tabela de temporalidade é documento chave do processo de gestão de documentos que, nos termos do art. 1º da Lei nº 8.159/1991, estabelece como dever do Poder Público "*a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação*".

5.109. O tempo de retenção dos dados pessoais, a seu turno, se define segundo o disposto no caput do art. 16 da LGPD, que determina que os dados sejam eliminados após o término do tratamento.

5.110. Observe-se que todo o contexto do ACT e do tratamento dos dados pessoais ocorre sob o argumento de tornar os estádios de futebol ambientes mais seguros e inclusivos:

Plano de Trabalho

5.2. Objetivos Gerais:

I - Promover ações em conjunto, bem como promover a troca de dados e informações entre o MJSP, a CBF e agremiações aderentes para tornar os estádios de futebol ambientes mais seguros e inclusivos.

5.111. Segundo o exposto no RIPD, o tratamento para as finalidades (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, só faz sentido persistir até o encerramento do evento esportivo.

5.112. A mesma afirmação vale para a finalidade de (ii) auxiliar na recuperação de veículos roubados ou furtados.

5.113. Observe-se, também, que no eixo I do tópico 10. Plano de Ação do Plano de Trabalho, está previsto o 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.

5.114. É razoável inferir, consequentemente, que a utilidade dos dados está intrinsicamente sujeita à atualidade, ao momento.

5.115. Não parece haver, portanto, qualquer razão para manutenção dessas informações para além do tempo necessário para garantir a segurança do evento esportivo ou para submetê-las ao tratamento de temporalidade que deve ser conferido apenas a documentos.

5.116. O acúmulo indiscriminado de dados pessoais pode colocar em risco a privacidade do titular de dados e violar direitos fundamentais e os ditames da LGPD, especialmente, em razão do risco de se criar um estado de vigilância indiscriminada.

5.117. Desta forma, quanto ao tempo de retenção, 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.

5.118. Ainda que se admitisse que persiste algum valor, utilidade ou finalidade desses dados, para fins de inteligência, para além do momento do evento esportivo, isso implicaria a instituição de uma quarta finalidade[7] para o tratamento de dados. Nesse caso, ainda assim, valeria o mesmo raciocínio exposto do [item 5.95] até o [item 5.97] desta Nota Técnica, ou seja: só podem ser mantidos dados pessoais 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.

5.119. Não há menor sentido em submeter os dados coletados de cidadãos em pleno exercício de seus direitos civis, que não deram causa para serem objeto de interesse das atividades de segurança pública, ao tratamento convencional que levaria à retenção por 50 anos ou mais, sob o risco de instaurar-se o vigilantismo exacerbado por parte do Estado.

5.120. Alternativamente, e somente se demonstrar claramente as razões para manter esses dados em tempo superior, 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.

**Dos Direitos dos Titulares**

5.121. Com relação ao atendimento ao direito dos titulares, é obrigação do órgão atender tais ditames, ainda que de forma diferenciada em virtude da atividade desempenhada.

5.122. A Lei de Geral de Proteção de Dados (LGPD) foi publicada em 2018, com vigência, na íntegra, em 2020. Os princípios elencados na lei, bem como os direitos dos titulares ali presentes devem ser observados por todos os agentes de tratamento de dados pessoais, independentemente da atividade que desempenham ou do sistema de informação que utilizam.

5.123. Destarte, o MJSP previu, no âmbito do RIPD, como pretende dar cumprimento à LGPD no que se refere aos direitos do titular. Sobre isso, vale lembrar o que foi considerado na análise da adequação do ACT aos princípios da Transparência e do Livre acesso.

5.124. O MJSP informa, no parágrafo 5.1.3. do RIPD, que dispõe de canal próprio, Sistema de Informação ao Cidadão e Ouvidoria, implementado pela plataforma https://falabr.cgu.gov.br, para que os titulares dos dados pessoais possam exercer os direitos previstos no art. 18 LGPD:

5.1.3. Ademais, o Ministério da Justiça e Segurança Pública dispõe de canal próprio, o Sistema de Informação ao Cidadão e Ouvidoria, implementado pela plataforma https://falabr.cgu.gov.br, para que os titulares dos dados pessoais possam demandar as solicitações previstas no Art. 18 LGPD, cujos pedidos serão analisados de acordo com a LAI e as normas que regem a atividade de inteligência enquanto não houver a norma específica prevista no §1 do Art. 4º da LGPD.

5.125. A Lei nº 12.527/2011 - Lei de Acesso à Informação -, possui ritos, sistemas eletrônicos e supervisão próprios e consolidados que, por força do disposto no art.

23, §3º da LGPD, são aplicáveis para exercício dos direitos do titular perante o Poder Público.

5.126. No que se refere aos direitos dos titulares, a partir das informações prestadas, não se vislumbrou a necessidade de expedir recomendações ao MJSP.

5.127. Saliente-se, por oportuno, que a efetividade do canal e do próprio exercício do direito pelo titular depende de o titular ter ciência de que seus dados estão sendo tratados. O atendimento fica, assim, vinculado ao quanto o princípio da transparência é efetivamente atendido, consoante recomendações constantes do [item 5.70] ao [item 5.88] desta Nota Técnica.

**Da Análise dos Riscos**

5.128. A seguir, apresentam-se alguns comentários acerca da atividade de identificação, avaliação e tratamento dos riscos no RIPD.

5.129. Em princípio, observa-se que o MJSP cuidou de adotar metodologia de análise de risco disponibilizada pelo Ministério da Economia e tomou por base a lista de riscos de privacidade e segurança da informação relacionados à proteção de dados pessoais previamente mapeados pelo Ministério. Consequentemente, foram mapeados 11 riscos, tanto referentes à segurança da informação (R01 a R05) quanto referentes à privacidade (R06 a R11).

5.130. Da avalição de risco pelo MJSP, não foi identificado nenhum risco classificado como alto, havendo somente riscos com níveis moderado e baixo. Segundo o MJSP, isso ocorre porque a atividade de inteligência já é naturalmente cercada de procedimentos e técnicas que lhe conferem vantagem no que diz respeito aos princípios da compartimentação e da necessidade de conhecer, reforçando a privacidade dos dados.

5.131. Independentemente do nível de risco identificado, o RIPD apresentou medidas de mitigação e tratamento para os riscos referentes à segurança da informação (M1 a M9) e medidas de mitigação e tratamento para os riscos referentes à privacidade (MP1 a MP4).

5.132. Quantos aos riscos referentes à segurança da informação e suas respectivas medidas de mitigação e tratamento, elas parecem ser suficientes, tendo em vista o já exposto no [item 5.41] ao [item 5.48] desta Nota Técnica e os controles apresentados na tabela seguinte ao parágrafo 7.4. do RIPD. Não há, portanto, recomendações a serem feitas.

5.133. Quantos aos riscos referentes à privacidade, os comentários e as providências necessárias estão no quadro a seguir:

| Risco | Medida | Comentário | Providência necessária |
|---|---|---|---|
| R06 Coleta Excessiva | MP1. Abertura, Transparência e Notificação<br>MJSP informa que atende ao Parecer nº 381/2023/CONJURMJSP/CGU/AGU (SEI 24491931)<br><br>MP2. Precisão e Qualidade. As informações serão analisadas por especialistas em inteligência altamente capacitados. | Abertura, transparência e notificação têm, em si, pouca relação com o risco identificado.<br><br>Do mesmo modo, informar que o MJSP atendeu a um parecer jurídico (especialmente quando tal parecer possivelmente versa sobre temas mais amplos do que a LGPD) parece ter pouca relação com o risco de coleta excessiva.<br>Igualmente, a análise de informações por especialistas em inteligência guarda tênue relação com o risco mapeado. O mecanismo tem sua importância, todavia, para evitar erros oriundos do processo automatizado e filtrar falsos positivos. Nesse sentido, poderia estar em outro lugar.<br>O risco final sequer foi alterado em função dessas medidas. | 1) Inclusão expressa no "Protocolo de Execução" dos dados exatos que serão fornecidos ao MJSP (ver explicação no [item 5.160] ao [item 5.163] abaixo).<br><br>2) Inclusão expressa no RIPD: i) das medidas indicadas no Parecer nº 381/2023/CONJURMJSP/CGU/AGU relacionadas a "coleta excessiva de dados"; e ii) a forma como essas medidas foram implantadas no escopo do acordo de cooperação ora analisado.<br>Tendo em vista que o risco é baixo, a própria elaboração do RIPD, definindo os dados tratados, e sua apresentação para apreciação técnica da ANPD são medidas suficientes – desde que sejam realizados no RIPD os ajustes indicados nesta Nota Técnica. |
| R07 Informação insuficiente sobre a finalidade do tratamento | MP1. Abertura, Transparência e Notificação<br>MJSP informa que atende ao Parecer nº 381/2023/CONJURMJSP/CGU/AGU (SEI 24491931)<br><br>MP2. Precisão e Qualidade. As informações serão analisadas por especialistas em inteligência altamente capacitados. | Esforço de abertura, transparência e notificação guardam evidente relação com o risco identificado.<br><br>Esta medida parece ter pouca relação com o risco de informação suficiente, ligado ao princípio da transparência e da finalidade.<br>O risco final sequer foi alterado em função dessas medidas. | 1) Atender às recomendações da ANPD referentes ao princípio da transparência, indicadas acima.<br><br>2) Inclusão expressa no RIPD: i) das medidas indicadas no Parecer nº 381/2023/CONJURMJSP/CGU/AGU relacionadas a "informação insuficiente sobre a finalidade do tratamento"; e ii) a forma como essas medidas foram implantadas no escopo do acordo de cooperação ora analisado. |
| R08 Tratamento sem consentimento | M1. Compliance com privacidade. Acesso aos dados é restrito.<br><br>M8. Registro de Eventos. Registro detalhado de todas as atividades por meio de logs, o que permite a realização de auditorias quando necessário | As medidas indicadas não respondem a esse risco, já que apontam para o controle de acesso aos dados e não a uma questão de hipótese de tratamento correta ou adequada coleta do consentimento.<br><br>O risco final sequer foi alterado em função dessas medidas. | Nenhuma.<br>No entanto, alternativamente, e como medida facultativa, sugere-se excluir a análise desse risco do RIPD. Para fins do art. 4º, III, o consentimento não é uma necessidade. Vale o disposto no art. 6º, notadamente os princípios da transparência e da finalidade que apontam mais para a ciência de que os dados estão sendo tratados, ao invés do consentimento. A referência ao consentimento em uma análise de risco para um tratamento que não o utiliza como base legal pode gerar mais dúvidas do que esclarecimentos. |
| R09 Falha em considerar direitos dos titulares | MP3.<br>Participação Individual e acesso – acesso concedido segundo a legislação vigente | A LAI possui ritos, sistemas eletrônicos e supervisão próprios e consolidados que, por força do disposto no art. 23, §3º da LGPD, são aplicáveis para exercício dos direitos do titular perante o Poder Público. | Atender às recomendações da ANPD referentes ao princípio da transparência, indicadas acima. |
| R10 Compartilhar ou distribuir dados pessoais com terceiros sem consentimento | MP4. Uso, retenção e limitação de divulgação.<br>Diretrizes preveem um prazo de guarda de 50 anos ou de guarda permanente para documentos de inteligência. | A medida não tem relação com o risco, considerando que sua descrição aponta para o tempo de retenção e não aos mecanismos de controle sobre compartilhamento. | Atender às recomendações referentes ao compartilhamento, indicadas nas seções seguintes.<br><br>Como medida facultativa, sugere-se excluir a análise desse risco do RIPD. Para fins do art. 4º, III, o consentimento não é uma necessidade. Vale o disposto no art. 6º, notadamente os princípios da transparência e da finalidade que apontam mais para a ciência de que os dados estão sendo tratados, ao invés do consentimento. A referência ao consentimento em uma análise de risco para um tratamento que não o utiliza como base legal pode gerar mais dúvidas do que esclarecimentos. |

| | | | |
|---|---|---|---|
| R11 Retenção prolongada de dados pessoais sem necessidade | MP1. Abertura, Transparência e Notificação<br>MJSP informa que atende ao Parecer nº 381/2023/CONJURMJSP/CGU/AGU (SEI 24491931) | A medida não responde a esse risco, considerando que sua descrição não aponta para o tempo de retenção. | 1) Atender às recomendações referentes ao tempo de retenção.<br><br>2) Inclusão expressa no RIPD: i) das medidas indicadas no Parecer nº 381/2023/CONJURMJSP/CGU/AGU relacionadas a "retenção prolongada de dados pessoais sem necessidade"; e ii) a forma como essas medidas foram implantadas no escopo do acordo de cooperação ora analisado. |

5.134. O MJSP deve adotar as providências indicadas como necessários no quadro acima, com vistas a suprir as deficiências apontadas nas medidas de mitigação e tratamento dos riscos.

**QUESTÕES ADICIONAIS**

**Do Plano Trabalho**

5.135. Acerca do plano de trabalho, em complemento aos comentários já expostos nos demais itens desta Nota Técnica, cabe uma ressalva ao disposto em seu parágrafo 8.1.:

> 8.1. No prazo de 10 (dez) dias a contar da celebração do presente acordo, cada partícipe e entidades de prática desportiva aderente designarão formalmente, no caso do MJSP mediante portaria e **preferencialmente** servidores públicos, os respectivos gestores envolvidos e responsáveis para (i) gerenciar a parceria; (ii) zelar por seu fiel cumprimento; (iii) coordenar, organizar, articular, acompanhar monitorar e supervisionar as ações que serão tomadas para o cumprimento do ajuste. [Grifamos]

5.136. A indicação pelo MJSP de qualquer gestor ou responsável que não seja servidor público invalida a garantia expressa em diversos pontos do RIPD de que apenas profissionais da inteligência teriam acesso aos dados pessoais e coloca em risco todo o modelo de segurança da informação, a adequação aos princípios da segurança, da prevenção e a observância do devido processo legal, no que se refere a evitar o uso indevido ou desvio de finalidade.

5.137. Nesse sentido, em função de exigências da própria política de segurança de informação do MJSP com relação ao acesso a informações no córtex, recomenda-se expressa menção de que a designação se dê apenas a agentes públicos, restrita a usuários previamente autorizados e autenticados pelos MJSP, e desde que integrantes do Sistema Único de Segurança Pública - SUSP, e de investigação e repressão de infrações penais, conforme política de governança de dados deste Ministério.

5.138. O MJSP deve ajustar a minuta de ACT para garantir que, em seu nome, apenas servidores públicos possam ser designados como gestores e responsáveis.

**Do Plano de Ação**

5.139. Acerca do tópico 10. Plano de Ação, do Plano de Trabalho, detectou-se inconsistência entre o previsto nos parágrafos 3.2.1. a 3.2.3. do RIPD. Não há menção no RIPD à coleta e ao tratamento do número de telefone; todavia, no eixo IV do plano, consta como obrigação da EPD o envio ao MJSP de diversos dados referentes à venda do bilhete, inclusive o telefone.

5.140. A partir das características do tratamento, sua finalidade e os procedimentos descritos nos parágrafos 3.1.1. a 3.1.8. do RIPD, não se vislumbra como estritamente necessária a coleta e repasse do número de telefone ao MJSP. Em verdade, tendo em vista que já são coletadas diversas outras informações, como o registro facial, catraca de entrada no estádio e o assento vinculado ao bilhete, a coleta do número do telefone é desnecessária e excessiva, especialmente considerando a utilidade do dado no contexto da atualidade (ou seja, durante o tempo necessário para garantir a segurança do evento desportivo). O MJSP deve ajustar o eixo IV do Plano de Ação para excluir a coleta e o compartilhamento do número do telefone.

5.141. No eixo V, o plano de ação prevê a captura, no momento da venda (on-line ou física), do registro facial do comprador ou beneficiário. Tal previsão gera um severo risco de desproporcionalidade, sobretudo para casos de compra por terceiros. Adicionalmente, não parece prudente estimular uma entidade privada a coletar e guardar dados biométricos, quando não há informações sobre por quanto tempo essas informações serão armazenadas pelos EPD, sobre as medidas técnicas e administrativas de segurança da informação, e nem sobre a impossibilidade de compartilhá-las. Reforçam-se, portanto, as recomendações constantes do [item 5.194] ao [item 5.197] desta Nota Técnica.

5.142. Adicionalmente, o plano de ação prevê, no eixo XI, que as EPDs devem cooperar para a criação da base nacional de torcedores impedidos de acesso a estádios de futebol. Sobre tal obrigação, é preciso que sejam prestados esclarecimentos pelo MJSP, uma vez que não está claro se a base será inteiramente gerida pela MJSP, se haverá compartilhamento dessas informações com as Entidades de Práticas Desportivas e em que condições.

5.143. Ainda, o MJSP precisa explicar quem é controlador dessa base, qual a sua finalidade, em que ela difere do BNMP ou das bases que os próprios clubes já têm. Por fim, caso este eixo XI esteja relacionado aos incisos III e XVII da Cláusula Sexta do Protocolo de Execução, 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*", no intuito de evitar posterior alargamento irregular e indevido dos dados compartilhados sem fundamento legal ou sem a devida reflexão quanto aos riscos associados ao tratamento quando da elaboração do RIPD.

5.144. Ressalte-se, ainda, que a condição de impedido de ter acesso às áreas desportivas é temporária, entre 3 meses e 5 anos (ver §2º do art. 183 c/c §2º do art. 201, ambos da Lei nº 14.597/2023), e a inclusão dessas informações no sistema do MJSP pode findar por sujeitá-las aos longos prazos de retenção de documentos relativos à produção de conhecimento de inteligência.

**Do Protocolo de Execução**

5.145. Logo no preâmbulo, o documento faz menção às metas de execução do plano de trabalho, em especial às previstas no item 6.2.1 a 6.2.6. Entretanto, não foi possível localizar esses itens no ACT, no Plano de Trabalho, no Termo de Adesão e tampouco no próprio Protocolo de Execução. É importante que seja revisada a redação do preâmbulo para correta referência aos parágrafos do ACT.

5.146. É necessário, ademais, que o protocolo de execução, considerando seu objeto, coleta e compartilhamento de dados pessoais, também faça referência expressa à Lei nº 13.709/2018.

5.147. Na Cláusula Quarta, inciso I, consta como obrigação do MJSP:

> I - Zelar pela adequada utilização das informações postas à disposição, de modo a preservar o caráter sigiloso,**delas devendo se valer exclusivamente para fins de formulação das políticas promovidas pelo Ministério da Justiça e Segurança Pública, por meio da SENASP, especialmente políticas de segurança pública, de produção de conhecimento no âmbito da inteligência de segurança pública, de investigação e de repressão de infrações penais**, de acordo com o disposto no art. 4º, inciso III, alíneas "a" e "d" da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018) [Grifamos]

5.148. A finalidade declarada nesse inciso I vai além do previsto e declarado nos documentos apresentados até o momento, e não se confunde com as finalidades declaradas nos parágrafos 2.1. e 2.2. do RIPD e parágrafo 1.1. do ACT.

5.149. Por mais que a aplicação da LGPD não seja integral a situações de tratamento de dados pessoais, o §1º do art. 4º, é taxativo ao determinar que os princípios da LGPD devem ser respeitados. O alargamento da finalidade, como pretendido pelo MJSP no inciso I, vai de encontro ao que dispõe o princípio da finalidade, que determina que o tratamento deve ser realizado "para propósitos legítimos, **específicos, explícitos e informados ao titular**, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".

5.150. A previsão legal de que seria possível tratamento posterior compatível com essa finalidade não exime o agente de tratamento de declarar nova finalidade que, por sua vez, também deve ser realizado "para propósitos legítimos, específicos, explícitos e informados ao titular.

5.151. Acerca desta possível "quarta" finalidade constante no inciso I, já houve manifestação nesta Nota Técnica no tópico que tratou do tempo de retenção e reiteram-se as recomendações dos [item 5.118] ao [item 5.120].

5.152. Nessa esteira, 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 utilizar documento falso ou outro tipo de ocorrência) ou relacionados a veículos furtados ou roubados.

5.153. Já no inciso II da Cláusula Quarta, há a previsão de que é vedada qualquer forma de acesso direto aos bancos de dados disponibilizados entre os partícipes, salvo para a Senasp, permitidas outras exceções, mediante proposta da Senasp e deliberação do Comitê de Governança de Dados e Sistemas de Informação do MJSP – CGDI.

5.154. Acerca dessa previsão, é necessário incluir nesse inciso referência às obrigações contidas nos §§ 1º a 4º do art. 4º da LGPD. O §1º do art. 4º, é taxativo ao determinar que os princípios da LGPD devem ser respeitados. Os §§2º e 4º trazem contornos para o tratamento desses dados por entidades de direito privado. O §3º determina que a ANPD emita opiniões técnicas e recomendações e solicite ao agente de tratamento público o Relatório de Impacto à Proteção de Dados.

5.155. Nesse sentido, o MJSP deve fazer constar expressa menção ao dever de elaborar RIPD e submeter a proposta de compartilhamento de dados previamente à ANPD.

5.156. Ainda na Cláusula Quarta, no inciso VI, há a previsão que de compete ao MJSP:

> VI - Assumir ou transferir a **terceiro** a responsabilidade pela execução do objeto da parceria, no caso de paralisação, de modo a evitar sua descontinuidade; [Grifamos]

5.157. Acerca da possibilidade de transferir a terceiro a responsabilidade pela execução do projeto, valem as mesmas considerações expostas anteriormente sobre o parágrafo 8.1. do Plano de Trabalho, no [item 5.136] ao [item 5.138] desta Nota Técnica.

5.158. Nesse sentido, recomenda-se expressa menção a que a transferência a terceiro se dê apenas a agentes públicos, restrita a usuários previamente autorizados e autenticados pelos MJSP e desde que integrantes do Sistema Único de Segurança Pública - SUSP, e de investigação e repressão de infrações penais, conforme política de governança de dados deste Ministério.

5.159. 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.

5.160. Na Cláusula Sexta, inciso I, consta como obrigação da EPD o fornecimento ao MJSP dos dados de compradores de ingressos e convidados para jogos de futebol profissional.

5.161. Entende-se que tais dados são aqueles definidos nos parágrafos 3.2.1. a 3.2.3. do RIPD, que foram citados nos incisos IV, V, VI, VII e VIII seguintes da Cláusula Sexta. Em caso afirmativo, é importante que isso conste expressamente no protocolo, no intuito de evitar alargamento irregular e indevido dos dados compartilhados sem fundamento legal ou sem a devida reflexão quanto aos riscos associados ao tratamento quando da elaboração do RIPD.

5.162. O compartilhamento é definido e limitado pela sua finalidade. O princípio da finalidade dispõe que o tratamento deve ser realizado “para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”. A redação do inciso I do protocolo de execução está ampla e não atende ao princípio da finalidade.

5.163. 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.

5.164. No inciso XVII da Cláusula Sexta, que trata da criação e atualização periódica do banco de dados nacional relativo a pessoas com acesso impedido a estádios, o protocolo de execução faz referência ao Estatuto do Torcedor. O Estatuto do Torcedor (Lei nº 10.671/2003) foi revogado pela Lei nº 14.597/2023– Lei Geral do Esporte, caindo a previsão do seu art. 5º, §1º, VI, que trata da lista de torcedores impedidos.

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

**Da Referência no RIDP ao Consentimento**

5.166. A análise sobre a hipótese legal que ampara uma atividade de tratamento é questão central em qualquer caso em que dados pessoais sejam tratados.

5.167. Muito embora não se tenha expressamente declarado no RIPD, consta em seu parágrafo 5.1.1. que o tratamento dos dados pessoais encontra fundamento na necessidade de cumprimento de obrigação do controlador de execução de política pública.

5.168. Dadas as fartas referências a dispositivos normativos que fundamentam a atuação do MJSP, conforme já exposto no [item 5.26] ao [item 5.30] desta Nota Técnica, e o fato de que duas finalidades remetem à condução de atividades de investigação e repressão de infrações penais, tanto a hipótese legal de execução de política pública quanto a de obrigação legal seriam cabíveis para o caso em tela.

5.169. Entretanto, a questão que chama atenção é a referência no RIPD ao consentimento do titular de dados, especialmente na identificação e tratamento dos riscos identificados.

5.170. Cumpre esclarecer que não se deve confundir consentimento para tratamento de dados pessoais com conhecimento/ciência de que dados pessoais são tratados. O primeiro é uma hipótese legal para tratamento de dados pessoais e molda sobremaneira os cuidados e deveres que o controlador assume ao eleger esta hipótese de tratamento, a exemplo do que dispõem o art. 8º, o art. 18, VI, e o art. 19, §3º. O uso do consentimento como hipótese legal decorre de uma escolha do controlador, não é obrigatório.

5.171. O segundo é condição inafastável em qualquer situação e hipótese de tratamento: é imperativo que o cidadão tenha ciência de que seus dados pessoais estão sendo tratados, por quem, para quais finalidades e por quanto tempo. Do contrário, invalidam-se por ineficazes todos os mecanismos previstos na LGPD para promover o equilíbrio entre controladores e titulares e para conferir ao titular o exercício de sua autodeterminação informativa, princípios consubstanciados nos direitos previstos nos artigos 9º, 18, 19 e demais da LGPD. Negar ciência ao titular impede que ele possa agir em defesa de sua privacidade ou da inviolabilidade de sua intimidade, honra e imagem.

5.172. Não parece, contudo, que o MJSP quis fundamentar o tratamento dos dados no consentimento, tanto que assim dispõe no parágrafo 3.3.3. do RIPD:

> 3.3.3. Com efeito, o tratamento de dados pessoais ocorrerá com ou até mesmo sem o consentimento prévio do titular, já que considera-se que a simples confirmação da existência de tratamento de dados pessoais poderá comprometer as atividades excepcionadas no inciso III, do art. 4º da LGPD, pelo que antes de se estabelecer procedimentos para informar ou dar acesso aos dados tratados ao titular aguarda-se a edição de legislação específica.

5.173. Com efeito, sugeriu-se que as referências relacionadas ao risco de tratamento de dados sem consentimento sejam excluídas do RIPD. As observações acima, consequentemente, devem ser entendidas no âmbito da atuação orientativa e preventiva da fiscalização.

5.174. Por oportuno, vale observar que o uso do consentimento pelo Estado nas relações com o cidadão é deveras incomum, quiçá problemático. É difícil conceber que um consentimento se dê de forma *livre*, principalmente em função da assimetria de forças entre ambos, do fato de que as relações entre o cidadão e o Estado normalmente não são voluntárias e, mesmo quando o são, a recusa do cidadão em não compartilhar dados pode alijá-lo do acesso a políticas públicas de modo geral.

**DO COMPARTILHAMENTO DOS DADOS PESSOAIS COM INTEGRANTES DO SUSP**

5.175. No que tange ao acesso aos dados obtidos mediante o acordo de cooperação técnica, há a informação, no parágrafo 3.2.4. do RIPD, de que o Ministério da Justiça e Segurança Pública pretende encaminhar à autoridade policial militar e à autoridade policial judiciária os dados tratados a cada partida de futebol.

5.176. Por outro lado, no parágrafo 5.9. da minuta do ACT, consta como obrigação comum manter sigilo das informações sensíveis obtidas em razão da execução do acordo, vedando-se o compartilhamento com outros órgãos e instituições não partícipes do ACT. Aparentemente, há uma contradição entre o previsto no RIPD e no ACT que deve ser esclarecida pelo MJSP.

5.177. Independentemente, da mesma forma que o MJSP precisa obedecer aos ditames da LGPD, especialmente os dispostos no art. 4º, §1º, os demais órgãos que terão acesso aos dados também deverão fazê-lo. Dessa maneira, precisarão comprovar a necessidade do tratamento dos dados pessoais, precedido pela demonstração de que há, de fato, um devido processo legal e respeito aos princípios e direitos dos titulares, conforme previsão da legislação.

5.178. Em razão disso, recomenda-se que o fornecimento de acesso a outros órgãos e entidades públicas aos dados especificamente coletados com fundamento neste ACT seja precedido de análises técnica e jurídica, além de emissão de decisão administrativa motivada pela autoridade competente, da qual constem a justificativa e as condições a serem observadas no caso, em conformidade com o disposto na LGPD.

5.179. Além disso, recomenda-se que tais órgãos elaborem seus próprios RIPDs no tratamento desses dados, uma vez que a finalidade e a hipótese legal do tratamento podem ser divergentes das utilizadas pelo MJSP.

**DA INFORMAÇÃO COMPARTILHADA PELO MJSP COM A EPD**

5.180. A partir do relato constante do RIPD, observa-se que a EPD receberá do MJSP um código informando sobre a necessidade de bloquear a catraca associada a um determinado bilhete que, por sua vez, está associado a determinado titular. Não serão fornecidas à EPD maiores informações sobre as razões para o bloqueio.

Concomitantemente, serão fornecidos às autoridades policiais no local dados suficientes para abordagem e identificação do indivíduo cujo bilhete foi marcado para bloqueio na catraca.

5.181. Cabe destacar que a atribuição do código de bloqueio se dará com fundamento na Base Nacional de Mandados de Prisão, cuja consulta é de acesso público, e na lista de torcedores impedidos de comparecer ao local do evento esportivo, que até o advento da Lei nº 14.597/2023, deveria estar publicada na internet, no sítio da entidade responsável pela organização do evento (art. 5, §1º da Lei nº 10.671/2003).

5.182. Adicionalmente, o Protocolo de Execução (SEI nº 4374450) prevê explicitamente a obrigação dessas informações serem excluídas ao fim do evento desportivo:

> 6.1. Ficam terminantemente vedadas às agremiações afiliadas à Confederação Brasileira de Futebol (CBF) que vierem a aderir ao presente Acordo de Cooperação, a possibilidade de armazenar os dados tratados provenientes do Ministério da Justiça e Segurança Pública, estabelecendo-se como imperativa a adoção de medidas efetivas para a completa exclusão desses dados na oportuna e conveniente, concomitantemente ao encerramento da partida. Ademais, destaca-se que o sistema da empresa contratada pela entidade desportiva responsável pela comercialização de bilhetes estará sujeita a auditorias periódicas, a fim de salvaguardar o interesse público, a serem realizadas no momento que se mostrar pertinente e conveniente, com vistas a assegurar a transparência e lisura do referido processo.

5.183. O tratamento de dados ou uso compartilhado de dados pessoais de órgãos públicos por empresas privadas é permitido desde que seja demonstrada a hipótese legal e desde que sejam atendidos os limites dispostos na LGPD para cada caso concreto, como a observância dos princípios e fundamentos da proteção de dados pessoais (art. 6º c/c art. 2º) e dos direitos dos titulares previstos nos arts. 8º, 9º, 18 e 19.

5.184. Exceções à afirmativa do item anterior são as atividades previstas no art. 4º, III: segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

5.185. Considerando que apenas uma informação é repassada pelo MJSP à EPD e que as demais informações tratadas e coletadas pela EPD ocorrem sob a tutela do MJSP e nem constituem a totalidade dos dados pessoais de banco de dados, entende-se como atendidos os limites impostos pelos §§ 2º e 4º do art. 4º da LGPD.

5.186. Neste tópico, não foi avaliada a circunstância em que a empresa privada atue como operadora de dados de órgãos públicos, mas apenas na função de controladora e tão somente do dado compartilhado pelo MJSP.

**DO TRATAMENTO DE DADOS PESSOAIS PELA ENTIDADE DE PRÁTICA DESPORTIVA (EPD)**

5.187. Diante das informações apresentadas, em que não constam quaisquer documentos sobre o tratamento de dados pessoais pela EPD fora do escopo do ACT, e da circunstância de que o segundo signatário do ACT, a CBF, não tratará dados pessoais, não há como analisar, neste momento, a regularidade do tratamento de dados pessoais pelas eventuais EPDs quando estiverem atuando como controladoras. Não há como analisar sequer se elas podem compartilhar esses dados pessoais.

5.188. Destaque-se que, exceto pelo disposto no parágrafo 6.1. do protocolo de execução, não há nenhuma salvaguarda apontada para a Entidade de Prática Desportiva sobre o reuso dos dados tratados no âmbito do ACT, e tampouco previsão de que tais dados não serão utilizados para outras finalidades.

5.189. Na linha de que a EPD deve atuar apenas como operadora, o art. 4º, III determina que tais dados são de uso exclusivo por pessoas jurídicas de direito público, exceto quando a pessoa jurídica de direito privado age tutelada por pessoa jurídica de direito público. Neste caso, é importante que fique claro que os dados estão sendo coletados exclusivamente para fins de segurança pública, não havendo circunstância em que possam ser tratados pela entidade de direito privado para finalidade distinta. Adicionalmente, considerando esse contexto, esses dados sequer devem ser retidos pela Entidade de Prática Desportiva (EPD) após o fim do evento esportivo.

5.190. Alternativamente, é possível que a coleta desses dados (inclusive os sensíveis) pelas Entidades de Prática Desportiva se dê com fundamento próprio (finalidade e hipótese legal próprias). É essencial que o MJSP só permita a adesão de EPD que, no mínimo: i) já houver preparado o RIPD (necessariamente abordando os mesmos riscos abordados no RIPD apresentado) e o Registro das Operações de Tratamento; ii) que já tenha encarregado designado; iii) disponha de ferramenta para exercício de direitos do titular; e iv) tenha disponibilizado informações sobre coleta e tratamento nos termos do art. 9º em lugar de franco e fácil acesso.

5.191. Do contrário, as informações teriam sido coletadas em tratamento irregular, passíveis de determinação de exclusão, e viciando qualquer tratamento de dados pessoais posteriormente realizado nesses dados, inclusive os tratamentos objeto do presente ACT.

5.192. É importante perceber que a EPD pode assumir múltipla função no âmbito do ACT, a depender do contexto do tratamento, quando se pretende analisar a observância das disposições da LGPD: é operadora, caso não venha a tratar os dados pessoais para finalidade própria; é co-controladora, caso se entenda que as finalidades discriminadas no ACT são de interesse comum; é controladora, caso pretenda tratar esses dados pessoais para finalidades próprias, distintas das declaradas neste ACT.

5.193. Convém salientar que tal entendimento se alinha com o exposto na Subcláusula Primeira da Cláusula Quarta – Da Operacionalização do ACT:

> SUBCLÁUSULA PRIMEIRA. As iniciativas previstas no Plano de Trabalho deste Acordo de Cooperação que impliquem em armazenamento, tratamento ou transferência de dados entre os signatários terão suas linhas básicas, atividades e ações constituídas, especificadas e implementadas por meio de Protocolos de Execução específicos firmados entre o MJSP e a CBF, nos quais estarão prescritas todas as disposições que garantam a responsabilidade pelo tratamento e custódia dos dados pessoais, a ampla proteção dos dados pessoais e o pleno cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente mediante a prévia consulta da Autoridade Nacional de Proteção de Dados – ANPD sobre os termos do respectivo Protocolo.

5.194. Caso a EPD tenha qualquer função de controladora com relação aos dados que estão sendo tratados no âmbito deste ACT, importa frisar que a regularidade do presente ACT em relação aos dados de determinada EPD depende da regularidade do tratamento da EPD para os dados por ela coletados.

5.195. Explica-se. Antes de poder compartilhar dados pessoais, é preciso que a EPD tenha hipótese legal para coletá-los e tratá-los, de acordo com sua finalidade própria. Em complemento, a EPD precisa estar regular com os demais requisitos para um tratamento conforme à LGPD (princípios, direitos dos titulares, RIPD, registro de operações de tratamento, medidas técnicas e administrativas de segurança da informação, regras de eliminação, nomeação de encarregado etc.).

5.196. Um controlador realizando tratamento de dados pessoais irregular é incapaz de realizar um compartilhamento regular e, por consequência, contamina como irregular qualquer tratamento dele decorrente, ainda que o controlador que os recebe esteja em condições de receber tais dados de modo regular. Aparentemente, a única exceção consiste na situação em que os dados pessoais sejam utilizados pela ANPD para fins de apurar a irregularidade do tratamento, ou no Judiciário, para fins de determinar a responsabilidade do controlador que executou tratamento irregular.

5.197. Vencida a questão da regularidade do tratamento dos dados pessoais pela EPD, é preciso verificar se ela pode compartilhá-los. O compartilhamento é uma forma de tratamento e somente pode ser efetuado se a finalidade estiver amparada numa hipótese legal, além de atendidos requisitos adicionais específicos. É preciso que o cedente possa 'compartilhar' os dados e que o cessionário possa 'recebê-los'. Este segundo quesito se verifica pela existência de uma hipótese legal que ampare a finalidade que demanda o tratamento dos dados pelo cessionário, e que esta finalidade seja compatível com a finalidade original e com requisitos específicos que permitam o uso compartilhado.

5.198. A fim de ilustrar o exposto acima, a seguir, apresenta-se um diagrama descrevendo a cadeia de legitimidade de tratamento de dados pessoais, a partir do titular, segundo as informações apresentadas pelo MJSP.

5.199. As setas de mesmas cores referem-se ao mesmo conjunto de dados e representam o caminho percorrido pelos dados, as hipóteses legais envolvidas, as hipóteses de compartilhamento e o instrumento formal de compartilhamento. Cada cor representa um conjunto distinto de dados, segundo sua origem.

5.200. Cabe ressaltar, como visto acima, que o uso compartilhado é uma forma de tratamento e somente pode ser efetuado se a finalidade estiver amparada numa hipótese legal, além de atendidos requisitos adicionais específicos. É preciso que o cedente da base possa 'compartilhar' os dados e que o cessionário possa 'recebê-los'.

5.201. Cumpre destacar que o titular de dados foi inserido no diagrama não como elemento ilustrativo, mas como raiz de validade e legitimidade da cadeia de tratamento que atesta a legítima procedência dos dados. A existência do titular é requisito fundamental para que qualquer tratamento que se faça tenha amparo legal. Isso ocorre tanto no fluxo azul, que indica que os dados foram obtidos de forma lícita, quanto no fluxo vermelho, que se refere aos dados de impedimento, gerados pela comparação entre os dados encaminhados pela EPD e os dados das bases públicas do BNMP e Lista de torcedores impedidos.

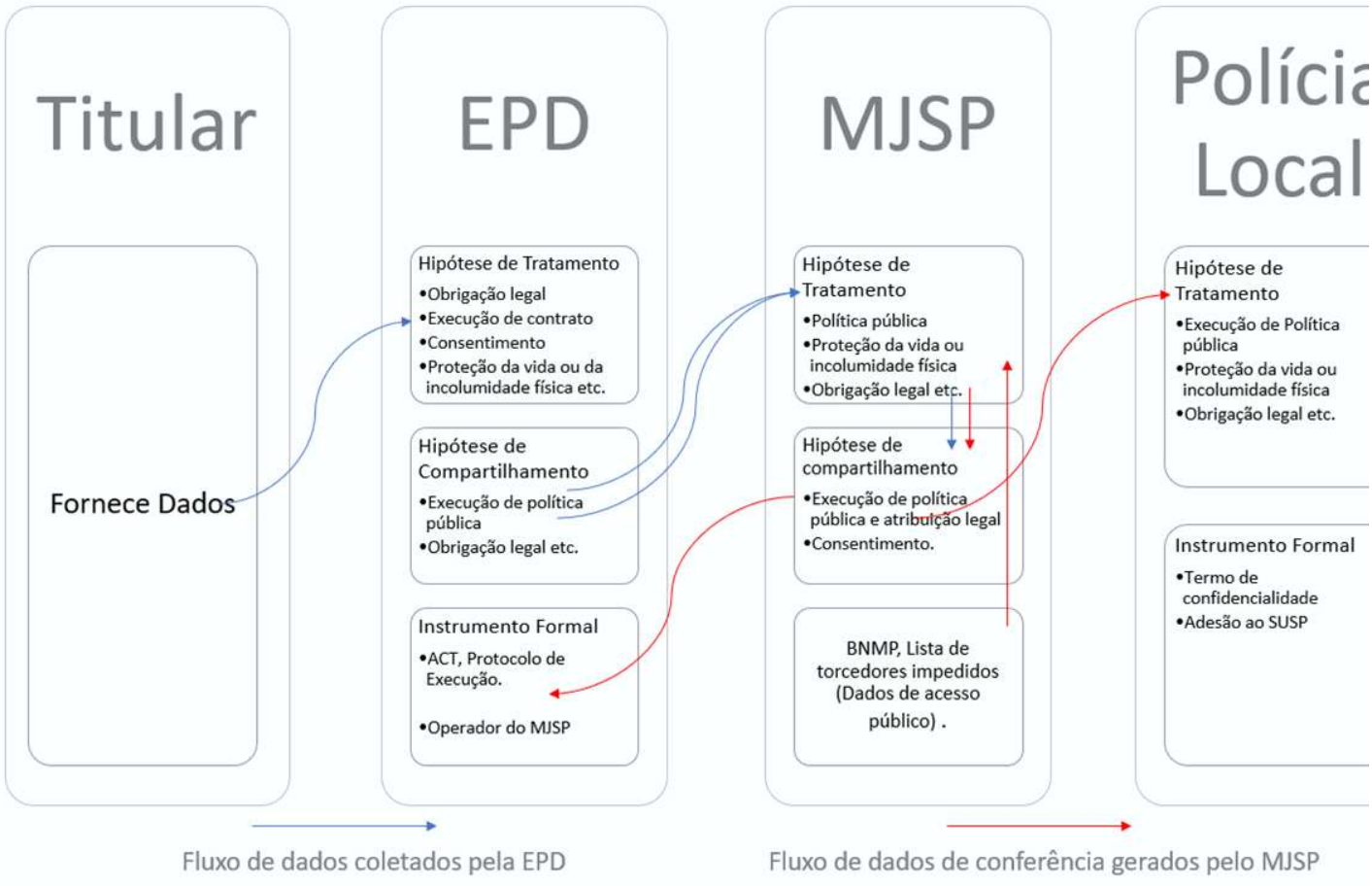


Figura 1: Desenho geral dos fluxos de tratamento de dados. Fonte: Elaboração própria.

5.202. De acordo com o diagrama acima, no fluxo azul, é preciso que o titular forneça seus dados pessoais à EPD. Esses dados, ainda que a EPD possa tê-los e usá-los (tratá-los para as finalidades específicas que justificaram sua coleta), só podem ser compartilhados se houver hipótese legal que justifique o compartilhamento (já que o compartilhamento é um tipo de tratamento). Admitindo-se, por conjectura, que existe hipótese legal, esses dados estão disponíveis para o MJSP.

5.203. Num outro momento, no fluxo vermelho, o MJSP produz um novo dado pessoal, as informações de impedimento, e as compartilha com a EPD. Adicionalmente, ele armazena, atualmente por até cinquenta anos (temporalidade essa que foi objeto de recomendação na presente NT), os dados recebidos da EPD, os dados recebidos da BNMP e lista de torcedores impedidos e os dados de impedimento associados ao evento esportivo.

5.204. Em síntese: os fluxos indicados no desenho acima somente estarão de acordo com a LGPD se: i) a coleta de dados pelas EPDs ocorrer em conformidade com a LGPD (ver [item 5.187] ao [item 5.203]); ii) o compartilhamento de dados do MJSP com as EPDs seguir o Projeto ora analisado, com a incorporação das recomendações aqui sugeridas; e iii) os órgãos integrantes do SUSP que receberem os dados do MJSP realizarem o tratamento para a finalidade específica a que esse compartilhamento se destina, conforme [item 5.175] ao [item 5.179]. Ressalte-se que, desses três requisitos, apenas o ii corresponde ao escopo do presente procedimento de fiscalização.

5.205. Por oportuno, cumpre citar a Lei nº 14.597, de 14 de junho de 2023, (Lei Geral do Esporte) e seus artigos 144 e 148, uma vez que ambos atribuem responsabilidades para a CBF e para as Entidades de Prática Desportiva.

5.206. O art. 144 determina a implantação de sistema de segurança contra falsificações, fraudes e outras práticas que contribuam para a evasão da receita decorrente do evento esportivo. Bem como, atribui tal implementação à organização esportiva que administra a competição e a organização esportiva mandante da partida. Ou seja, é possível inferir que, no caso concreto, essas organizações seria, respectivamente, a CBF e as Entidades de Prática Desportiva.

5.207. Já o art. 148 determina que deverá haver controle e fiscalização de acesso do público, via monitoramento por imagem das catracas e com identificação biométrica dos espectadores, em arenas esportivas cuja capacidade seja maior que 20 mil pessoas. Observe que a lei impõe que o controlador implemente tais medidas técnicas de controle.

5.208. Note-se que tais dispositivos podem oferecer um caminho e uma justificativa legal para que ocorra a cooperação entre o Ministério da Justiça e Segurança Pública, a Confederação Brasileira de Futebol e as Entidades de Prática Desportiva.

**Da Atuação Fiscalizatória da ANPD e Da Expedição de Opiniões Técnicas e Recomendações**

5.209. O Regulamento de Fiscalização busca uma atuação responsiva do agente de tratamento. Dessa forma, a autoridade possui prerrogativa de adotar diferentes formas de atuação para além da típica atividade repressiva, como a atividade de monitoramento, orientação e prevenção. Nesse sentido, o art. 15, do Regulamento de Fiscalização, indica que:

> Art. 15. A ANPD adotará atividades de monitoramento, de orientação e de prevenção no processo de fiscalização e poderá iniciar a atividade repressiva.
>
> § 1º A atividade de monitoramento destina-se ao levantamento de informações e dados relevantes para subsidiar a tomada de decisões pela ANPD com o fim de assegurar o regular funcionamento do ambiente regulado.
>
> § 2º A atividade de orientação caracteriza-se pela atuação baseada na economicidade e na utilização de métodos e ferramentas que almejam a promover a orientação, a conscientização e a educação dos agentes de tratamento e dos titulares de dados pessoais.
>
> § 3º A atividade preventiva consiste em uma atuação baseada, preferencialmente, na construção conjunta e dialogada de soluções e medidas que visam a reconduzir o agente de tratamento à plena conformidade ou a evitar ou remediar situações que possam acarretar risco ou dano aos titulares de dados pessoais e a outros agentes de tratamento.
>
> § 4º A atividade repressiva caracteriza-se pela atuação coercitiva da ANPD, voltada à interrupção de situações de dano ou risco, à recondução à plena conformidade e à punição dos responsáveis mediante a aplicação das sanções previstas no artigo 52 da LGPD, por meio de processo administrativo sancionador.

5.210. Em vista desse sistema de atividades possíveis na atuação fiscalizatória, cabe à Autoridade conduzir procedimento de fiscalização para guiar o agente de tratamento à plena conformidade às obrigações previstas na LGPD, de forma direta e menos onerosa.

5.211. É nesse sentido que esta CGF conduz o presente procedimento de fiscalização para que o MJ e a CBF atuem em acordo com o previsto em lei, especialmente em observância ao devido processo legal, aos princípios gerais de proteção de dados e aos direitos do titular, como especificado no §1º, do art. 4º, da LGPD.

## 6. CONCLUSÃO

6.1. Ante o exposto, até o momento, acerca da celebração 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:

6.2. **Sobre a competência da ANPD:**

6.2.1. O caso versa sobre tratamento de dados pessoais, sensíveis ou não, de forma que incide a competência da ANPD, prevista no art. 55-J, I c/c art. 55-J, XX.

6.2.2. Relativamente ao art. 4º, III, da LGPD, destaca-se que as exceções de aplicação da Lei previstas no artigo em comento não se aplicam de forma absoluta aos casos das atividades previstas no inciso III, tendo em vista as disposições dos parágrafos deste artigo, como informado na análise.

6.2.3. O tratamento de dados pessoais com fundamento no art. 4º, III da LGPD atrai de plano a competência da ANPD, inclusive nas hipóteses de compartilhamento indevido com outros órgãos fora da estrutura da segurança pública ou de inteligência, por exemplo.

6.3. **Sobre a designação de operador constante do parágrafo 5.3.1 do RIPD**

6.3.1. A indicação do operador, quando ele se constitui em órgão do próprio controlador – MJSP – acaba por se tornar uma denominação sem efeito prático tendo em vista que não deve ser usada como uma formalização de distribuição interna de competências e responsabilidades.

6.3.2. No parágrafo 5.3.1. do RIPD, consta referência a termo de compromisso e manutenção de sigilo e a orientações técnicas que seriam firmados pelo operador. Considerando que a primeira parte do RIPD apresenta a CGINT como operador, não ficou claro se a palavra operador foi empregada no mesmo sentido nestas duas ocasiões, sobretudo porque há referência expressa ao art. 5º, VII da LGPD nesse parágrafo 5.3.1.

a) O MJSP deve ajustar o RIPD para esclarecer esta questão, considerando o exposto no [item 5.17] ao [item 5.21] desta Nota Técnica.

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

6.4.1. 6.4.1. Para as finalidades de (i) recapturar indivíduos com mandado de prisão ou medidas penais restritivas, de (ii) auxiliar na recuperação de veículos roubados ou furtados e de (iii) evitar a venda de ingressos utilizando dados de pessoas falecidas, combatendo o cambismo, foi possível verificar sua relação com o previsto no art. 4º, III da LGPD.

b) Nesse sentido, 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.

6.5. **Sobre a observância aos princípios da adequação e necessidade**

6.5.1. A ausência dos dados pessoais que serão tratados para a finalidade (ii) de recuperação de veículos roubados ou furtados impede qualquer apreciação acerca da sua observância aos princípios da necessidade e da adequação.

6.5.2. Portanto, não ficou esclarecido como o órgão atenderá aos princípios da necessidade e da adequação no que tange a essa finalidade.

c) MJSP deve acrescentar ao RIPD os dados que serão tratados e como serão tratados, 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.

6.5.3. Quanto ao tratamento do registro facial, coletado no ato da venda, não há qualquer menção à foto, a dados pessoais biométricos ou sensíveis nos dados discriminados no RIPD.

6.5.4. O RIPD é documento essencial para a regularidade do tratamento que se pretende. Seja do ponto de vista formal, porque é obrigação da ANPD requisitá-lo, seja do ponto de vista material, porque somente a partir da análise das informações contidas nele se torna possível à ANPD cumprir seu papel legal.

6.5.5. Ante o descasamento entre o previsto no RIPD e o que consta no ACT, invalida-se o segundo naquilo que excede o previsto no primeiro.

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.

6.5.6. Qualquer tratamento do dado biométrico de registro facial antes de cumprido o disposto na alínea d) acima configura tratamento irregular.

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.

6.6. **Sobre a observância aos princípios da Transparência e do Livre Acesso**

6.6.1. Para fins de atendimento aos princípios da transparência e da finalidade, a previsão no inciso II da Cláusula Sexta do Protocolo de Execução está ampla e não é adequada. Igualmente, ela é incompatível com a previsão do parágrafo 5.4.1. do RIPD do MJSP.

6.6.2. A obrigação de atender aos princípios da transparência e do livre acesso não deve ser ônus apenas da EPD, mas do MJSP e demais integrantes das forças de segurança pública que participarem do Projeto Estádio Seguro.

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.

6.7. **Sobre a observância do princípio da Qualidade**

6.7.1. No que se refere à finalidade de (ii) auxiliar na recuperação de veículos roubados ou furtados, entretanto, a falta de algumas informações no RIPD referentes a essa finalidade impede que se possa avaliar o tratamento quanto ao 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.

6.8. **Sobre a Frequência do Tratamento e Tempo de Retenção**

6.8.1. No compartilhamento dos dados que serão encaminhados à autoridade policial militar e à autoridade de polícia judiciária, o RIPD não deixa claro se serão os dados de todos os cidadãos que frequentarão o evento esportivo ou apenas os dados de sujeitos de interesse, que acusem problema de falha na validação biométrica, suspeitos de usar documento falso ou de outro tipo de ocorrência.

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).

6.8.2. Ainda que o propósito seja a preservação da ordem pública e da incolumidade das pessoas e do patrimônio com o objetivo de garantir o bem-estar e a segurança da sociedade diante de situações que possam ameaçá-la ou causar dano, não se pode conceber o acúmulo e a produção de conhecimento despropositado sob a justificativa de proteger a sociedade de seus próprios cidadãos quando não há motivo razoável senão em relação a uma parcela reduzida de cidadãos cujo contexto fático destoa do cidadão médio.

6.8.3. A noção de documento não se confunde e nem deve ser igualada ao conjunto de dados pessoais tratados no âmbito deste ACT. Igualmente, não é e nem dever ser automática, implícita ou presumida, a aplicação da tabela de temporalidade a qualquer conjunto de dados pessoais.

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.

6.9. **Sobre os direitos dos titulares**

6.9.1. A Lei nº 12.527/2011 - Lei de Acesso à Informação possui ritos, sistemas eletrônicos e supervisão próprios e consolidados que, por força do disposto no art.

23, §3º da LGPD, são aplicáveis para exercício dos direitos do titular perante o Poder Público.

6.9.2. A efetividade do canal previsto na LAI e do próprio exercício do direito pelo titular depende de o titular ter ciência de que seus dados estão sendo tratados. O atendimento fica, assim, vinculado ao quanto o princípio da transparência é efetivamente atendido.

6.9.3. Cumpre esclarecer que não se deve confundir consentimento para tratamento de dados pessoais com conhecimento/ciência de que dados pessoais são tratados. O primeiro é uma hipótese legal para tratamento de dados pessoais e molda sobremaneira os cuidados e deveres que o controlador assume ao eleger essa hipótese de tratamento, a exemplo do que dispõem o art. 8º, o art. 18, VI, e o art. 19, §3º. O uso do consentimento como hipótese legal decorre de uma escolha do controlador, não é obrigatório.

6.9.4. O segundo é condição inafastável em qualquer situação e hipótese de tratamento. É imperativo que o cidadão tenha ciência de que seus dados pessoais estão sendo tratados, por quem, para quais finalidades e por quanto tempo. Do contrário, invalidam-se por ineficazes todos os mecanismos previstos na LGPD para equilibrar controladores e titulares, para conferir ao titular o exercício de sua autodeterminação informativa, consubstanciados nos direitos previstos nos artigos 9º, 18, 19 e demais da LGPD. Negar ciência ao titular impede que ele possa agir em defesa de sua privacidade ou da inviolabilidade de sua intimidade, honra e imagem.

**Questões Adicionais**

6.10. **Sobre o Relatório de Impacto à Proteção de Dados Pessoais**

6.10.1. No RIPD, cabe ao agente de tratamento informar quais dados são tratados, identificar sua fonte, registrar como o tratamento será realizado, quem tem acesso às informações, como elas são utilizadas, para que finalidades e por quanto tempo.

6.10.2. No intuito de demonstrar a adequação ao devido processo legal, cabe ao controlador explicar no âmbito de que processo administrativo ou judicial essas informações são utilizadas e quais medidas são implementadas para evitar abusos e desvios de finalidade.

6.10.3. O controlador deve explicar como são respeitados os princípios do art. 6º, principalmente no que tange à segurança, prevenção, transparência, finalidade, necessidade, adequação e não discriminação.

6.10.4. O controlador deve apresentar em que medida e de que forma os direitos dos titulares são executados diante do tratamento de dados pessoais realizado.

6.10.5. O controlador deve realizar a avalição dos riscos, tanto cibernéticos quanto a direitos fundamentais. Sua avaliação de risco deve contemplar as medidas de segurança da informação, os direitos fundamentais possivelmente afetados pelo tratamento (ex. direito de ir e vir, à proteção de dados, à privacidade).

6.11. **Sobre o compartilhamento de dados pessoais**

6.11.1. O compartilhamento de dados pessoais no âmbito da inteligência está condicionado à observância do devido processo legal, que consiste num rito mínimo necessário à formalização do compartilhamento nos moldes do que foi mencionado nessa Nota Técnica. Esta formalização deve ser fundamentada por um estudo mais aprofundado (RIPD, por exemplo), que leve em consideração toda a análise principiológica supramencionada, e em particular:

6.11.1.1. Demonstre o interesse público e a vinculação do tratamento de dados pessoais com as atribuições legais do órgão ou entidade que receberá os dados pessoais.

6.11.1.2. Preveja regras sobre a eliminação dos dados pessoais (art. 16, da LGPD).

6.11.1.3. Preveja medidas de atendimento aos direitos dos titulares.

6.11.1.4. Atenda ao princípio da transparência e informe sobre o tratamento, as finalidades pretendidas, incluindo se as informações são compartilhadas, tanto no sítio eletrônico do MJSP quanto dos demais órgãos e entidades envolvidos, em atenção ao disposto no art. 6º, VI, e 23, I, da LGPD.

6.11.1.5. Informe como pretende atender aos demais princípios elencados no art. 6º da LGPD.

6.11.2. Ademais, é imprescindível que o Relatório de Impacto à Proteção de Dados – RIPD, uma vez elaborado, seja enviado para que a ANPD o avalie e, se for o caso, determine a adoção de providências para fazer cessar violações às disposições da LGPD e, caso entenda pela sua publicação, em que medida ele deverá ser publicado.

6.11.3. Adicionalmente, é essencial que o Ministério da Justiça e Segurança Pública:

6.11.3.1. Indique aos demais órgãos que receberão acesso aos dados pessoais que, caso pretendam tratá-los para finalidade distinta das aqui analisadas, devem elaborar Relatório de Impacto à Proteção de Dados no âmbito de suas atividades e no que tange ao uso desses dados pessoais, previamente ao efetivo tratamento.

6.11.3.2. Confirme a ciência e responsabilidade dos demais órgãos que acessarão os dados, com anuência expressa destes às condições estipuladas nos instrumentos de formalização do compartilhamento (ACT, Plano de Trabalho, Protocolo de Execução etc.).

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.

6.11.4. Especificamente no que se refere ao compartilhamento pelo MJSP com a EPD, considerando que apenas uma informação é repassada pelo MJSP à EPD e que as demais informações tratadas e coletadas pela EPD ocorrem sob a tutela do MJSP e nem constituem a totalidade dos dados pessoais de banco de dados, entende-se como atendidos os limites impostos pelos §§ 2º e 4º do art. 4º da LGPD.

6.12. **Sobre o tratamento de dados pessoais pela EPD**

6.12.1. Diante das informações apresentadas, não foi possível analisar a regularidade do tratamento de dados pessoais pelas eventuais EPDs quando estiverem atuando como controladoras, não há como analisar sequer se elas podem compartilhar esses dados pessoais.

6.12.2. Caso atue como controladora, antes de poder compartilhar dados pessoais, é preciso que a EPD se ampare em hipótese legal para coletá-los e tratá-los, de acordo com sua finalidade própria. Em complemento, a EPD precisa estar regular com demais requisitos para um tratamento conforme à LGPD.

6.12.3. Um controlador realizando tratamento de dados pessoais irregular é incapaz de realizar um compartilhamento regular e, por consequência, contamina como irregular qualquer tratamento decorrente dele.

6.12.4. Caso a EPD tenha qualquer função de controladora com relação aos dados que estão sendo tratados no âmbito deste ACT, a regularidade do presente ACT depende da regularidade do tratamento da EPD para os dados por ela coletados.

6.13. **Sobre a Análise dos Riscos**

6.13.1. Quantos aos riscos referentes à segurança da informação e suas respectivas medidas de mitigação e tratamento, elas parecem ser suficientes, tendo em vista o já exposto no [item 5.41] ao [item 5.48] desta Nota Técnica e os controles apresentados na tabela seguinte ao parágrafo 7.4. do RIPD. Não há, portanto, recomendações a serem feitas.

6.13.2. Quanto aos riscos referentes à privacidade identificou-se nesta Nota Técnica a necessidade de expedir recomendações para adoção de providências.

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.

6.14. **Sobre o plano de trabalho**

6.14.1. A indicação pelo MJSP como gestor e responsável de qualquer pessoa que não seja servidor público invalida a garantia expressa em diversos pontos do RIPD de que apenas profissionais da inteligência teriam acesso aos dados pessoais, e coloca em risco todo o modelo de segurança da informação, a adequação aos princípios da segurança, da prevenção e a observância do devido processo legal no que se refere a evitar o uso indevido ou desvio de finalidade.

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.

6.14.2. Sobre o eixo IV do Plano de Ação, não se vislumbra como estritamente necessária a coleta e o repasse do número de telefone ao MJSP. Tendo em vista que já são coletadas diversas outras informações, como o registro facial, catraca de entrada no estádio e o assento vinculado ao bilhete, a coleta do número do telefone é desnecessária e excessiva.

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

6.14.3. Sobre o eixo XI do Plano de Ação, que trata de cooperação para a criação da base nacional de torcedores impedidos de acesso a estádios de futebol, não está claro se a base será inteiramente gerida pela MJSP, se haverá compartilhamento dessas informações com as Entidades de Práticas Desportivas e em que condições e os limites dessa cooperação no que se refere ao compartilhamento de dados pessoais.

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*".

6.15. **Sobre o Protocolo de Execução**

6.15.1. Não foi possível localizar os itens 6.2.1 a 6.2.6 no ACT, no Plano de Trabalho, no Termo de Adesão referidos no preâmbulo do Protocolo de Execução.

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

6.15.2. A finalidade declarada no inciso I da Cláusula Quarta vai além do previsto e declarado nos documentos apresentados até o momento, e não se confunde com as finalidades declaradas nos parágrafos 2.1. e 2.2. do RIPD e parágrafo 1.1. do ACT.

6.15.3. O §1º do art. 4º, é taxativo ao determinar que os princípios da LGPD devem ser respeitados. O alargamento da finalidade, como pretendido pelo MJSP no inciso I vai de encontro ao que dispõe o princípio da finalidade que determina que o tratamento deve ser realizado "*para propósitos legítimos, **específicos, explícitos e informados ao titular**, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades*".

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.

6.15.4. No inciso II da Cláusula Quarta, há a previsão de que é vedada qualquer forma de acesso direto aos bancos de dados disponibilizados entre os participes, salvo para a Senasp, permitidas outras exceções, mediante proposta da Senasp e deliberação do Comitê de Governança de Dados e Sistemas de Informação do MJSP – CGDI. Acerca dessa previsão, é necessário incluir nesse inciso referência às obrigações contidas nos §§ 1º a 4º do art. 4º da LGPD.

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.

6.15.5. Acerca da possibilidade de transferir a terceiro a responsabilidade pela execução do projeto, consoante previsto no inciso VI da Cláusula Quarta do Protocolo de Execução, valem as mesmas considerações expostas anteriormente sobre o parágrafo 8.1. do Plano de Trabalho, no [item 5.136] ao [item 5.138] desta Nota Técnica.

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.

6.15.6. Na Cláusula Sexta, inciso I, consta como obrigação da EPD, o fornecimento ao MJSP dos dados de compradores de ingressos e convidados para jogos de futebol profissional. A redação deste inciso I do protocolo de execução está ampla e não atende ao princípio da finalidade.

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.

6.15.7. No inciso XVII da Cláusula Sexta, que trata da criação e atualização periódica do banco de dados nacional relativo aos dados de pessoas cujo acesso a estádios esteja impedido em estádios, o protocolo de execução faz referência ao Estatuto do Torcedor. O Estatuto do Torcedor (Lei nº 10.671/2003) foi revogado pela Lei nº 14.597/2023– Lei Geral do Esporte, caindo a previsão do seu art. 5º, §1º, VI.

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.

6.16. Por fim, o atendimento às recomendações constantes das alíneas '*a*' a 'w' desta Conclusão é condição necessária para regularização do tratamento de dados pessoais nos termos previstos no ACT analisado à luz da LGPD e devem os signatários apresentar evidências nesse sentido, caso pretendam manter o ACT vigente.

## 7. ENCAMINHAMENTOS

7.1. Encaminhe-se à Secretaria-Geral, nos termos do art. 10, VIII, do Regimento Interno.

7.2. Sugere-se o encaminhamento desta Nota Técnica ao MJSP para que:

a) no prazo 20 dias úteis, se manifeste, apresentando evidências de atendimento, em relação às determinações constantes das alíneas '*a*' a 'w' da Conclusão; e

b) no prazo de 5 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.

7.3. Sugere-se o encaminhamento à Comissão Mista de Controle das Atividades de Inteligência do Congresso Nacional em atenção ao disposto no art. 6º da Lei nº 9.883/1999 c/c art. 3º da Resolução nº 2, de 2013-CN[8], para ciência.

_____

[1] ANPD. Guia para Definições de Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf . Acesso em out de 2023.
[2] Nota Técnica nº 5/2021/CGTP/ANPD; Nota Técnica nº 72/2022/CGF/ANPD e Nota Técnica nº 82/2022/CGF/ANPD.
[3] ANPD. Guia de tratamento de dados pessoais pelo poder público. V2. 2023, p. 30. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf . Acesso em out 2023
[4] Não há necessidade de indicar onde estão as câmeras e tampouco para onde estão apontando. Basta que os avisos estejam nas vias e nos estacionamentos cobertos pelas câmeras.
[5] Disponível em: https://www.gov.br/arquivonacional/pt-br/arquivos%20pdf/codigos-de-classificacao/CCD_TTD_MJSP.pdf. Acesso em 13 out 2023.
[6] Disponível em: https://www.in.gov.br/web/dou/-/portaria-an-n-74-de-29-de-agosto-de-2022-427630610 . Acesso em 13 out 2023.
[7] Sobre essa quarta finalidade, não se pode admitir como específica o suficiente em atenção aos princípios da finalidade e da adequação, declarações como "consecução finalística das políticas de segurança pública", "tratamento no âmbito da execução de política de segurança pública", "formulação das políticas de segurança pública, de produção de conhecimento no âmbito da inteligência de segurança pública, de investigação e de repressão de infrações penais."
[8] Disponível em: https://legis.senado.leg.br/sdleg-getter/documento/download/5b66aa0b-cd16-41f6-9c58-f045bc5f45c9. Acesso em 10 out 23.

Documento assinado eletronicamente por **Fabricio Guimarães Madruga Lopes**, **Coordenador(a)-Geral**, em 25/10/2023, às 19:20, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade do documento pode ser conferida informando o código verificador **4656752** e o código CRC **AC5C4B6A** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0