



UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE ENGENHARIA DO CONHECIMENTO
CURSO DE PÓS-GRADUAÇÃO EM INTELIGÊNCIA E INOVAÇÃO APLICADAS NO
ENFRENTAMENTO AO CRIME ORGANIZADO

Rhanderson Lourenço Santos
Victor de Oliveira Ribeiro

**A legalidade do compartilhamento de dados de pessoas de interesse da
segurança pública entre órgãos públicos e produtoras de eventos culturais:
uma análise à luz da LGPD e da LAI**

Florianópolis
2026

Rhanderson Lourenço Santos
Victor de Oliveira Ribeiro

**A legalidade do compartilhamento de dados de pessoas de interesse da
segurança pública entre órgãos públicos e produtoras de eventos culturais:
uma análise à luz da LGPD e da LAI**

Trabalho de Conclusão de Curso submetido ao curso de Pós-Graduação em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado do Centro Tecnológico da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de especialista em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado.

Orientador(a): Prof. Gregório Jean Varvakis Rados, Dr.

Florianópolis

2026

Santos, Rhanderson Lourenço

A legalidade do compartilhamento de dados de pessoas de interesse da segurança pública entre órgãos públicos e produtoras de eventos culturais : uma análise à luz da LGPD e da LAI / Rhanderson Lourenço Santos, Victor de Oliveira Ribeiro ; orientador, Gregorio Jean Varvakis Rados, 2026.

88 p.

Monografia (especialização) - Universidade Federal de Santa Catarina, Centro Tecnológico, Curso de Pós-Graduação em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado, Florianópolis, 2026.

Inclui referências.

1. Segurança Pública. 2. LGPD. 3. Proteção de dados pessoais. 4. Eventos culturais. 5. Reconhecimento facial. I. Ribeiro, Victor de Oliveira. II. Rados, Gregorio Jean Varvakis. III. Universidade Federal de Santa Catarina. Pós-Graduação em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado. IV. Título.

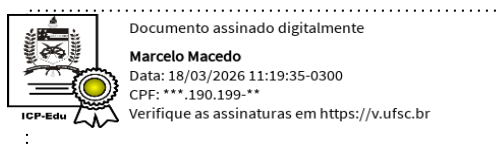
Rhanderson Lourenço Santos

Victor de Oliveira Ribeiro

**A legalidade do compartilhamento de dados de pessoas de interesse da
segurança pública entre órgãos públicos e produtoras de eventos culturais:
uma análise à luz da LGPD e da LAI**

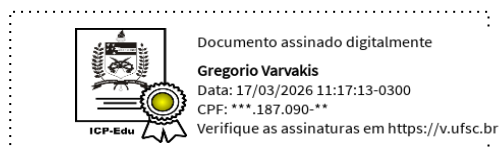
Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do título de Especialista em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado e aprovado em sua forma final pelo Curso de Pós-Graduação em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado

Florianópolis, 03 de março de 2026.



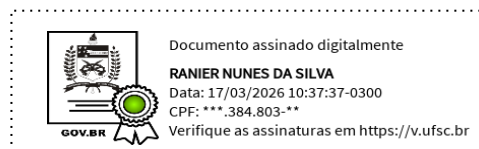
Coordenação do Curso

Banca examinadora



Prof. Gregório Jean Varvakis Rados, Dr.

Orientador(a)



Prof. Ranier Nunes da Silva, Me.

Membro externo

Universidade Federal de Santa Catarina

Florianópolis, 2026.

Às nossas famílias,
base inabalável, fonte constante de apoio,
compreensão e incentivo.

AGRADECIMENTOS

À Universidade Federal de Santa Catarina (UFSC), pela excelência acadêmica, pelo compromisso institucional com a produção científica e pela oportunidade de aprofundamento teórico e crítico proporcionada ao longo do Curso de Especialização, ambiente que estimulou o debate qualificado e o amadurecimento intelectual indispensáveis à construção deste trabalho.

Ao Professor Orientador, pela condução segura, pelas contribuições técnicas precisas, pela disponibilidade constante e pela orientação firme e criteriosa, fundamentais para o desenvolvimento metodológico, o rigor científico e a consolidação das reflexões aqui apresentadas.

Agradecemos, ainda, pelo incentivo à pesquisa responsável e pela confiança depositada na condução deste estudo, elementos que foram determinantes para a conclusão desta etapa acadêmica

“Entre a publicidade e o sigilo, entre a segurança e a liberdade, o Direito não escolhe extremos: ele impõe limites.”

RESUMO

A presente pesquisa analisa a legalidade do compartilhamento de dados de pessoas de interesse da segurança pública entre órgãos estatais e produtoras privadas de eventos culturais, à luz da Lei Geral de Proteção de Dados e da Lei de Acesso à Informação. O problema central reside na incerteza normativa sobre o tratamento de dados biométricos em contextos de segurança preventiva, agravada pela ausência de regulamentação específica. O objetivo geral buscou verificar a legalidade dessas práticas mediante análise sistemática dos dispositivos da LGPD confrontados com os da LAI, identificando convergências normativas. A pesquisa adotou metodologia jurídico-dogmática com abordagem qualitativa, envolvendo revisão bibliográfica sistemática e análise documental dos protocolos em eventos como Rock in Rio, Lollapalooza e Carnaval de Salvador. O estudo demonstrou que existe base legal para o compartilhamento desde que a operação observe os princípios de finalidade específica, necessidade, proporcionalidade e transparência, bem como formalize a responsabilidade solidária entre as partes. A pesquisa identificou, contudo, que o uso de reconhecimento facial sem protocolos adequados gera riscos de discriminação algorítmica, falsos positivos e vazamentos de dados sensíveis. O trabalho conclui que a harmonização entre segurança pública e proteção de dados é juridicamente viável mediante Avaliação de Impacto à Proteção de Dados, termos formais de compartilhamento, auditorias periódicas e canais de contestação acessíveis aos titulares. Como produto aplicado, a pesquisa desenvolveu instrumentos práticos incluindo listas de verificação de conformidade, modelos de termos contratuais e roteiros de checagem de legalidade que mitigam insegurança jurídica e agregam valor estratégico aos eventos culturais.

Palavras-chave: Proteção de dados pessoais. LGPD. Eventos culturais. Reconhecimento facial. Segurança pública.

ABSTRACT

This research analyzes the legality of sharing data on individuals of interest to public security between state agencies and private cultural event producers, in light of the General Data Protection Law and the Access to Information Law. The central problem lies in regulatory uncertainty regarding the processing of biometric data in preventive security contexts, aggravated by the absence of specific regulation. The general objective sought to verify the legality of these practices through systematic analysis of LGPD provisions confronted with LAI provisions, identifying normative convergences. The research adopted a legal-dogmatic methodology with a qualitative approach, involving systematic bibliographic review and documentary analysis of protocols at events such as Rock in Rio, Lollapalooza and Salvador Carnival. The study demonstrated that there is a legal basis for sharing provided that the operation observes the principles of specific purpose, necessity, proportionality and transparency, as well as formalizes joint liability between the parties. The research identified, however, that the use of facial recognition without adequate protocols generates risks of algorithmic discrimination, false positives and sensitive data leaks. The work concludes that harmonization between public security and data protection is legally viable through Data Protection Impact Assessment, formal sharing agreements, periodic audits and accessible contestation channels for data subjects. As an applied product, the research developed practical instruments including compliance checklists, contractual agreement templates and legality verification roadmaps that mitigate legal uncertainty and add strategic value to cultural events.

Keywords: Personal data protection. LGPD. Cultural events. Facial recognition. Public security.

LISTA DE QUADROS

Quadro 1 - Dispositivos legais aplicáveis ao compartilhamento de dados em eventos.....	21
Quadro 2 - Convergências internacionais em proteção de dados biométricos.....	33
Quadro 3 - Práticas de compartilhamento em eventos culturais brasileiro.....	55

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AI Act	Artificial Intelligence Act (Lei de Inteligência Artificial da União Europeia)
ANPD	Autoridade Nacional de Proteção de Dados
CDC	Código de Defesa do Consumidor
CETIC.BR	Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
CF/88	Constituição Federal de 1988
CGI.br	Comitê Gestor da Internet no Brasil
CGU	Controladoria-Geral da União
CICOM	Centro Integrado de Comunicações (Bahia)
COI	Centro de Operações e Inteligência
CPF	Cadastro de Pessoas Físicas
DPIA	Data Protection Impact Assessment (Avaliação de Impacto à Proteção de Dados)
EC	Emenda Constitucional
EDPB	European Data Protection Board
FTC	Federal Trade Commission (Estados Unidos)
GDPR	General Data Protection Regulation (Regulamento Geral sobre a Proteção de Dados)
IA	Inteligência Artificial
ICO	Information Commissioner's Office (Reino Unido)
ISO	International Organization for Standardization
LAI	Lei de Acesso à Informação (Lei nº 12.527/2011)
LGPD	Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
PIPEDA	Personal Information Protection and Electronic Documents Act (Canadá)
PMBA	Polícia Militar da Bahia
SAEB	Secretaria da Administração do Estado da Bahia
SSP/BA	Secretaria da Segurança Pública da Bahia
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TCC	Trabalho de Conclusão de Curso
TIC	Tecnologias da Informação e da Comunicação
UK GDPR	United Kingdom General Data Protection Regulation

SUMÁRIO

1	INTRODUÇÃO.....	13
2	REVISÃO DE LITERATURA.....	18
2.1	<i>EVOLUÇÃO NORMATIVA DA PROTEÇÃO DE DADOS NO BRASIL.....</i>	<i>18</i>
2.2	<i>LGPD E AS EXCEÇÕES DE SEGURANÇA PÚBLICA.....</i>	<i>22</i>
2.3	<i>LEI DE ACESSO À INFORMAÇÃO E CONVERGÊNCIA COM A LGPD.....</i>	<i>27</i>
2.4	<i>ORIENTAÇÕES DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS.....</i>	<i>30</i>
2.5	<i>MODELOS INTERNACIONAIS DE REGULAMENTAÇÃO.....</i>	<i>34</i>
2.6	<i>SÍNTESE DA FUNDAMENTAÇÃO NORMATIVA.....</i>	<i>37</i>
2.7	<i>LIMITES CONSTITUCIONAIS DA ATUAÇÃO PREVENTIVA ESTATAL.....</i>	<i>39</i>
3	METODOLOGIA.....	42
3.1	<i>CARACTERIZAÇÃO DA PESQUISA.....</i>	<i>42</i>
3.2	<i>COLETA DE DADOS.....</i>	<i>43</i>
3.3	<i>PROCEDIMENTOS DE ANÁLISE</i>	<i>44</i>
3.4	<i>CONSTRUÇÃO DAS FERRAMENTAS PRÁTICAS.....</i>	<i>45</i>
3.5	<i>LIMITAÇÕES METODOLÓGICAS.....</i>	<i>49</i>
3.6	<i>PROCEDIMENTOS ÉTICOS</i>	<i>50</i>
4	ANÁLISE E DISCUSSÃO DOS RESULTADOS.....	52
4.1	<i>PROTOCOLOS DE COMPARTILHAMENTO DE DADOS EM EVENTOS CULTURAIS BRASILEIROS.....</i>	<i>52</i>
4.2	<i>RISCOS E DESAFIOS JURÍDICOS IDENTIFICADOS.....</i>	<i>56</i>
4.3	<i>VALOR ESTRATÉGICO DA CONFORMIDADE COM A LGPD.....</i>	<i>62</i>
4.4	<i>DIRETRIZES PRÁTICAS DE CONFORMIDADE</i>	<i>65</i>
5	CONCLUSÃO.....	71
	REFERÊNCIAS.....	77
	APÊNDICE A – ROTEIRO ORIENTADO PARA CHECAGEM DA LEGALIDADE DO COMPARTILHAMENTO DE DADOS EM EVENTOS CULTURAIS	82
	APÊNDICE B – MODELO COMENTADO DE TERMO DE COMPARTILHAMENTO DE DADOS PARA EVENTOS CULTURAIS.....	84
	APÊNDICE C – CHECKLIST DETALHADO DE CONFORMIDADE PARA PRODUTORAS E ÓRGÃOS PÚBLICOS	87

1 INTRODUÇÃO

O advento da sociedade da informação transformou radicalmente a forma como o Estado e os agentes privados interagem com os cidadãos, consolidando um cenário de vigilância distribuída onde o fluxo de dados pessoais se tornou o ativo central das relações sociais e econômicas (CASTELLS, 2003). Nesse novo arranjo, a coleta massiva de informações deixa de ser uma exceção para se tornar a regra operacional, permeando desde simples transações comerciais até complexas operações de monitoramento estatal. A capacidade tecnológica de processamento de dados, amplificada pelo uso de inteligência artificial e sistemas de reconhecimento biométrico, cria um ambiente onde a privacidade é constantemente tensionada pela promessa de maior eficiência e segurança, exigindo do Direito uma postura ativa para evitar que a dignidade da pessoa humana seja suprimida pela lógica algorítmica (RODOTÀ, 2008).

Nesse contexto, os grandes eventos culturais brasileiros, como festivais de música, shows de grande porte e celebrações populares, tornaram-se laboratórios privilegiados para a aplicação dessas tecnologias de monitoramento e controle de acesso. Eventos como Rock in Rio, Lollapalooza, Festival de Verão de Salvador e o Carnaval movimentam milhões de pessoas e exigem níveis elevados de coordenação entre poder público e setor privado para garantir a segurança dos participantes. Essa cooperação, contudo, frequentemente envolve o compartilhamento de dados sensíveis, incluindo listas de pessoas procuradas pela Justiça, informações de identificação civil e, em casos mais controversos, dados biométricos capturados por sistemas de reconhecimento facial (DUARTE; CEIA, 2022).

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, inaugurou uma nova cultura jurídica no país, exigindo que o tratamento de informações pessoais, inclusive aquelas voltadas para a segurança, observe princípios rígidos de finalidade, adequação, necessidade e transparência. Rompe-se, assim, com a lógica anterior de coleta indiscriminada, impondo aos organizadores de eventos e ao poder público o dever de justificar cada dado capturado dos participantes. A LGPD estabeleceu, no art. 6º, dez princípios fundamentais que devem nortear todo tratamento de dados pessoais, entre os quais

destacam-se a finalidade (tratamento para propósitos legítimos, específicos e informados), a necessidade (limitação ao mínimo necessário) e a transparência (garantia de informações claras e acessíveis aos titulares) (BIONI, 2021).

Simultaneamente, a Lei de Acesso à Informação (LAI), Lei nº 12.527/2011, consagra o princípio da publicidade como regra e o sigilo como exceção na Administração Pública, estabelecendo no art. 3º que o acesso à informação é direito fundamental e que cabe ao Estado assegurar o direito à informação mediante procedimentos objetivos e ágeis. A LAI cria, portanto, um dever de transparência ativa que pode entrar em aparente conflito com a proteção de dados pessoais garantida pela LGPD, especialmente quando se trata de informações de interesse público relacionadas à segurança (RIBEIRO, 2020).

O problema central desta pesquisa reside, portanto, na zona de incerteza jurídica que permeia o compartilhamento de dados de pessoas de interesse da segurança pública entre órgãos estatais e entidades privadas organizadoras de eventos culturais. Esse dilema jurídico-operacional se manifesta em várias dimensões práticas: a definição das bases legais aplicáveis para o tratamento desses dados, os procedimentos de consentimento ou dispensa dele em casos de interesse público preponderante, as medidas de segurança exigidas para o tratamento de dados sensíveis, bem como os limites temporais e de finalidade para o uso dessas informações. Conforme observado por Mendes (2019), a proteção de dados não é um direito absoluto, mas deve ser ponderado com outros direitos fundamentais, especialmente em contextos em que a segurança pública e a vida dos cidadãos estão em jogo.

Agrava-se esse cenário pela ausência de uma regulação específica para a proteção de dados na esfera penal e de segurança pública no Brasil. A LGPD, em seu artigo 4º, inciso III, exclui parcialmente a aplicação da lei para fins exclusivos de segurança pública, segurança do Estado ou atividades de investigação e repressão de infrações penais, criando um vácuo normativo que desafia os gestores públicos e privados.

Essa exclusão não significa, contudo, que inexistem limites para o tratamento de dados nessa esfera, mas sim que tais limites devem ser buscados em outros diplomas legais e na interpretação sistemática do ordenamento jurídico. Sem uma “LGPD Penal” clara e específica, as produtoras de eventos e as forças policiais operam muitas vezes baseadas em interpretações analógicas, na LAI, e em

pareceres técnicos como o Parecer CGU nº 295/2020, buscando equilibrar a transparência administrativa com o sigilo necessário às operações de inteligência e prevenção criminal (ALMEIDA; ESTELLITA, 2021).

A justificativa para este estudo apoia-se não apenas na relevância econômica do setor de entretenimento, que movimenta bilhões de reais anualmente e emprega milhares de pessoas, mas sobretudo na urgência de mitigar riscos de violação de direitos humanos e fundamentais. A implementação de sistemas de reconhecimento facial em cidades como Salvador, especialmente durante grandes festividades como o Carnaval, demonstrou que a tecnologia, se mal aplicada ou desprovida de salvaguardas adequadas, pode amplificar riscos de discriminação algorítmica, viés racial e produzir falsos positivos que resultam em constrangimento indevido e até prisões ilegais (DUARTE; CEIA, 2022). A ausência de transparência sobre o destino dos dados biométricos coletados, a falta de canais efetivos de contestação para os titulares e a inexistência de auditorias independentes nos algoritmos utilizados exigem uma governança robusta, capaz de transformar a conformidade legal em um ativo de segurança jurídica e reputação para o evento.

Além disso, a pesquisa recente do CETIC.BR (2023) sobre privacidade e proteção de dados pessoais revelou que 74% dos brasileiros desconfiam de eventos e serviços que não explicitam suas políticas de privacidade, indicando que a transparência no tratamento de dados não é apenas uma exigência legal, mas também um diferencial competitivo e um fator de construção de confiança com o público. Eventos que demonstram compromisso com a proteção de dados tendem a atrair mais patrocinadores, investidores institucionais e consumidores conscientes de seus direitos, agregando valor econômico à marca (CETIC.BR, 2023).

Considerando esse panorama, os objetivos traçados para esta investigação são os seguintes. Como objetivo geral, busca-se analisar a legalidade do compartilhamento de dados de pessoas de interesse da segurança pública entre órgãos públicos e produtoras de eventos culturais, à luz dos princípios e dispositivos da LGPD e da LAI, propondo instrumentos de governança que harmonizem segurança e privacidade.

Como objetivos específicos, propõe-se: (a) identificar as bases legais da LGPD e da LAI aplicáveis ao compartilhamento de dados para fins de segurança preventiva em eventos culturais; (b) examinar os limites, requisitos e salvaguardas exigidos para o tratamento de dados sensíveis por empresas privadas em

cooperação com órgãos públicos; (c) mapear os riscos jurídicos associados ao uso de reconhecimento facial e outras tecnologias biométricas em eventos de massa; e (d) desenvolver diretrizes práticas de conformidade, traduzindo a dogmática jurídica em instrumentos de gestão aplicáveis ao cotidiano das produtoras e órgãos de segurança.

Para atingir os objetivos propostos, a pesquisa adota metodologia jurídico-dogmática com abordagem qualitativa, estruturada sob a lógica do Ensino por Projetos que privilegia o engajamento com problemas reais e a construção de soluções práticas aplicáveis. O percurso metodológico envolveu revisão bibliográfica sistemática, análise documental de protocolos de segurança de eventos brasileiros (Rock in Rio, Lollapalooza, Carnaval de Salvador) e exame de orientações técnicas da ANPD, culminando no desenvolvimento de instrumentos de governança que traduzem requisitos legais em procedimentos operacionais verificáveis. A metodologia encontra-se detalhada em seção específica, que justifica as escolhas metodológicas e descreve os procedimentos de coleta e análise de dados.

O trabalho estrutura-se em sessões que refletem progressão lógica dedutiva do problema aos instrumentos de solução. A Revisão da Literatura analisa a evolução normativa da proteção de dados no Brasil, as exceções de segurança pública da LGPD, a convergência entre LGPD e LAI, as orientações da ANPD e modelos internacionais de regulamentação.

A Metodologia detalha a abordagem jurídico-dogmática adotada e os procedimentos de coleta e análise de dados. A Análise e Discussão dos Resultados examina protocolos efetivamente adotados em eventos brasileiros, identifica riscos jurídicos, demonstra o valor estratégico da conformidade e propõe diretrizes práticas aplicáveis ao setor. As Considerações Finais sintetizam os achados, retomam os objetivos alcançados e reafirmam a viabilidade de harmonizar segurança e privacidade mediante protocolos juridicamente fundamentados e transparentes.

Como produto aplicado desta pesquisa, desenvolveram-se três instrumentos práticos de governança apresentados nos Apêndices: (A) Roteiro orientado para checagem da legalidade do compartilhamento de dados em eventos culturais, que permite verificação rápida de conformidade mediante perguntas estruturadas; (B) Modelo comentado de termo de compartilhamento de dados para eventos culturais, que traduz exigências do artigo vinte e seis da LGPD em cláusulas contratuais específicas; e (C) Checklist detalhado de conformidade para produtoras e órgãos

públicos, que sistematiza cinquenta requisitos jurídicos, técnicos e operacionais em formato de verificação pontuada. Esses artefatos contribuem para redução da insegurança jurídica no setor e para construção de cultura de compliance que respeite simultaneamente a segurança dos participantes e os direitos fundamentais dos cidadãos.

2 REVISÃO DA LITERATURA

2.1 EVOLUÇÃO NORMATIVA DA PROTEÇÃO DE DADOS NO BRASIL

A trajetória normativa da proteção de dados pessoais no Brasil caracteriza-se por uma evolução gradual, marcada pela transição de um modelo de tutela genérica da privacidade para um regime especializado de governança de dados. Essa transformação reflete a crescente percepção, tanto no âmbito legislativo quanto jurisprudencial, de que a proteção de dados constitui direito fundamental autônomo, cuja efetivação exige instrumentos normativos específicos e mecanismos institucionais dedicados.

O marco inicial dessa trajetória encontra-se na Constituição Federal de 1988, que consagrou, no art. 5º, incisos X e XII, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como o sigilo das comunicações. Esses dispositivos, contudo, foram concebidos em contexto histórico anterior à massificação da internet e ao processamento automatizado de dados, razão pela qual sua aplicação aos desafios contemporâneos da sociedade da informação exigiu significativa criatividade hermenêutica por parte dos tribunais e da doutrina. Conforme observa Doneda (2006), a privacidade, originalmente concebida como direito de ser deixado só (*right to be let alone*), precisou ser reinterpretada para abarcar a dimensão informacional, traduzindo-se no direito de controlar o fluxo de informações pessoais e de conhecer a finalidade de seu tratamento.

O primeiro avanço legislativo significativo nessa direção foi a promulgação da Lei de Acesso à Informação (LAI), Lei nº 12.527, de 18 de novembro de 2011, que regulamentou o direito fundamental de acesso à informação previsto no art. 5º, XXXIII, da Constituição. A LAI estabeleceu, em seu art. 3º, que o acesso à informação é direito fundamental, consagrando a publicidade como regra e o sigilo como exceção na Administração Pública. Esse diploma legal representou mudança paradigmática na cultura administrativa brasileira, impondo ao Estado o dever de transparência ativa e de prestação de contas à sociedade. Contudo, a LAI também estabeleceu, em seus arts. 21, 23 e 31, importantes ressalvas relacionadas à proteção de informações pessoais, reconhecendo que a transparência administrativa não pode se sobrepor ao direito à privacidade dos cidadãos. O art. 31, especificamente, determina que o tratamento de informações pessoais deve ser feito

de forma transparente e com respeito à intimidade, vida privada, honra e imagem, estabelecendo as bases para o posterior desenvolvimento de legislação específica sobre proteção de dados (RIBEIRO, 2020).

Em 2014, foi promulgado o Marco Civil da Internet (Lei nº 12.965/2014), que estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil. Embora não se trate de lei específica sobre proteção de dados, o Marco Civil consagrou, em seu art. 3º, inciso III, a proteção dos dados pessoais como princípio fundamental da rede, e dedicou a Seção I do Capítulo III (arts. 7º a 11) à proteção aos registros, aos dados pessoais e às comunicações privadas. Esse diploma normativo foi importante precursor da LGPD, ao estabelecer que o tratamento de dados pessoais deve respeitar a privacidade, a proteção dos dados e o sigilo das comunicações privadas, salvo por ordem judicial (BIONI, 2021).

O marco regulatório específico para a proteção de dados pessoais no Brasil foi estabelecido com a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, que entrou em vigor em setembro de 2020. A LGPD foi fortemente inspirada no Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), mas apresenta particularidades que refletem a realidade institucional e social brasileira. A lei estabelece, em seu art. 1º, que disciplina o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade. Conforme destaca Mendes (2019), a LGPD inaugura um modelo de proteção de dados, fundado na ideia de que, diante do processamento automatizado e generalizado de dados na sociedade da informação, não existem mais dados irrelevantes, pois qualquer informação pessoal pode ser utilizada para criar perfis, tomar decisões e afetar direitos fundamentais.

A LGPD estabeleceu dez princípios fundamentais que devem nortear todo tratamento de dados pessoais (art. 6º): finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (accountability). Esses princípios representam mudança de paradigma em relação à lógica anterior de coleta indiscriminada, exigindo que cada operação de tratamento seja justificada por finalidade legítima, específica e informada ao titular, e que a coleta seja limitada ao mínimo necessário para atingir essa finalidade. Além disso, a LGPD criou categoria especial de dados sensíveis (art. 5º, II), que incluem dados biométricos, e

estabeleceu regime mais restritivo para seu tratamento (art. 11), reconhecendo o maior potencial lesivo dessas informações (BIONI, 2021).

Entretanto, a LGPD apresenta lacuna significativa no que se refere ao tratamento de dados para fins de segurança pública. O art. 4º, inciso III, exclui parcialmente a aplicação da lei para tratamento de dados realizado para fins exclusivos de segurança pública, segurança do Estado ou atividades de investigação e repressão de infrações penais. Essa exclusão criou vácuo normativo que afeta diretamente a questão objeto desta pesquisa, pois não há, até o presente momento, legislação específica que discipline o tratamento de dados pessoais na esfera penal e de segurança pública (uma “LGPD Penal”), deixando gestores públicos e empresas privadas que atuam nessa área sem parâmetros claros de conformidade. Conforme observam Almeida e Estellita (2021), essa lacuna legislativa não significa que inexistam limites para o tratamento de dados nessa esfera, mas sim que tais limites devem ser buscados na interpretação sistemática da Constituição Federal, da LAI, da própria LGPD (em seus dispositivos não excepcionados) e dos tratados internacionais de direitos humanos dos quais o Brasil é signatário.

O reconhecimento definitivo da proteção de dados como direito fundamental autônomo veio com a promulgação da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que incluiu a proteção de dados pessoais no rol de direitos e garantias fundamentais do art. 5º da Constituição Federal. O novo inciso LXXIX estabelece que “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”, enquanto o inciso LXXX atribui à União a competência privativa para legislar sobre proteção e tratamento de dados pessoais. Essa elevação ao status constitucional consolida a autonomia da proteção de dados em relação ao direito à privacidade tradicional e reforça a necessidade de ponderação cuidadosa quando esse direito entra em tensão com outros direitos fundamentais, como a segurança pública (MENDES; DONEDA, 2018).

Essa trajetória normativa evidencia que o ordenamento jurídico brasileiro passou de um modelo de tutela genérica e reativa da privacidade para um regime especializado e proativo de governança de dados, caracterizado pela exigência de justificação prévia de cada operação de tratamento, pela imposição de medidas técnicas e organizacionais de segurança, e pela responsabilização dos agentes de tratamento. Contudo, a persistência da lacuna regulatória na esfera penal e de

segurança pública, somada à tensão estrutural entre o dever de transparência consagrado pela LAI e as exceções de sigilo previstas na LGPD, cria desafios operacionais significativos, especialmente em contextos de cooperação público-privada como os eventos culturais de massa, onde a necessidade de compartilhamento de dados para fins preventivos deve ser harmonizada com os direitos fundamentais dos titulares.

Para visualizar a convergência normativa identificada, sistematizaram-se os principais dispositivos aplicáveis no Quadro 1.

Quadro 1 — Dispositivos Legais Aplicáveis ao Compartilhamento de Dados em Eventos

Artigo	Base Legal	Aplicação	Requisitos
LGPD Art.7º	Bases legais gerais	Tratamento de dados não sensíveis	Consentimento livre/informado OU hipótese legal específica
LGPD Art.9º	Bases legais especiais	Tratamento de dados sensíveis (biométricos)	Consentimento específico OU tutela da saúde/segurança
LGPD Art.11	Dados sensíveis	Vedação de acesso público	Exceção: prevenção de fraude e segurança
LGPD Art.23	Dados sensíveis no poder público	Dispensa de consentimento para interesse público	Finalidade pública + proporcionalidade
LGPD Art.26	Compartilhamento	Uso entre público e privado	Termo formal com responsabilidades
LAI Art.3º	Publicidade	Transparência como regra	Acesso amplo
LAI Art.6º	Gestão documentos	Classificação e acesso	Garantir acesso e proteção
LAI Art.31	Proteção dados pessoais	Tratamento transparente	Acesso restrito + finalidade + prazo

Fonte: Elaborado pelos autores

Legenda: com base na Lei 13.709/2018 (LGPD) e Lei 12.527/2011 (LAI).

Conforme demonstrado no Quadro 1, a LGPD e a LAI não estabelecem regimes conflitantes, mas requisitos cumulativos que devem ser simultaneamente observados nas operações de compartilhamento de dados entre setor público e privado. A análise comparativa evidencia que ambos os diplomas legais convergem na proteção de dados pessoais como valor jurídico tutelado, divergindo apenas quanto ao foco normativo: enquanto a LGPD estabelece bases legais, princípios de proteção e direitos dos titulares, a LAI disciplina aspectos de transparência,

publicidade e controle social quando há participação de órgão público. Essa complementaridade normativa implica que o compartilhamento de dados biométricos capturados em eventos culturais com órgãos de segurança pública não pode invocar a publicidade da LAI para dispensar os requisitos protetivos da LGPD, nem utilizar a exceção de segurança pública da LGPD para afastar a transparência exigida pela LAI. A legalidade do compartilhamento depende, portanto, do atendimento simultâneo de ambos os regimes normativos.

A sistematização comparativa apresentada no Quadro 1 permite concluir que a aparente tensão entre publicidade e proteção de dados resolve-se mediante interpretação harmônica e sistemática dos diplomas legais. O compartilhamento legítimo de dados em eventos culturais exige não apenas base legal adequada conforme artigos 7º ou 9º da LGPD e observância de seus princípios estruturantes, mas também transparência ativa, finalidade pública delimitada e formalização mediante termo de compartilhamento nos moldes do artigo 26, harmonizando-se com as exigências de controle social estabelecidas pela LAI. Essa convergência normativa fornece fundamento sólido para análise das práticas efetivamente adotadas pelo setor de eventos culturais no Brasil.

2.2 LGPD E AS EXCEÇÕES DE SEGURANÇA PÚBLICA

A Lei Geral de Proteção de Dados Pessoais estabelece, em seu art. 4º, as hipóteses de não aplicação de suas disposições, criando zonas de exclusão que refletem a ponderação legislativa entre a proteção de dados e outros interesses constitucionalmente protegidos. O inciso III desse dispositivo determina que a LGPD não se aplica ao tratamento de dados realizado para fins exclusivos de segurança pública, segurança do Estado ou atividades de investigação e repressão de infrações penais. Essa exclusão, contudo, deve ser interpretada de forma estrita e sistemática, considerando que mesmo nas hipóteses excepcionadas persistem limitações constitucionais e legais ao tratamento de dados pessoais.

A doutrina tem debatido intensamente os contornos dessa exceção. Conforme observam Almeida e Estellita (2021), a expressão “fins exclusivos” sugere que a exclusão não se aplica quando o tratamento de dados, embora relacionado à segurança pública, não se destina exclusivamente a essa finalidade ou quando envolve também finalidades comerciais ou administrativas. No contexto de eventos

culturais, onde há cooperação entre órgãos públicos de segurança e produtoras privadas que possuem interesses econômicos evidentes, a aplicabilidade da exceção torna-se particularmente controversa. A simples alegação de que o compartilhamento visa à segurança não é suficiente para afastar, automaticamente, todas as garantias da LGPD, especialmente quando o tratamento envolve dados sensíveis como informações biométricas.

Mesmo nas hipóteses em que a exceção do art. 4º, III, seja aplicável, os princípios constitucionais da proporcionalidade, razoabilidade e respeito aos direitos fundamentais continuam vinculando a atuação estatal. Ademais, outros dispositivos da própria LGPD permanecem relevantes mesmo em contextos de segurança pública. O art. 23, por exemplo, estabelece que o tratamento de dados pessoais pelas pessoas jurídicas de direito público deve atender à finalidade pública e à persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais e forneçam informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas. Esse dispositivo demonstra que, ainda que excluída a aplicação geral da LGPD, subsiste o dever de transparência e de fundamentação legal para o tratamento de dados pelo poder público (MALMANN; SULZBACH, 2020).

Para compreender as bases legais aplicáveis ao compartilhamento de dados em eventos culturais, torna-se necessário examinar as hipóteses de tratamento de dados pessoais estabelecidas no art. 7º da LGPD. Embora esse artigo se destine primordialmente ao setor privado, seus incisos II (cumprimento de obrigação legal ou regulatória pelo controlador), III (execução de políticas públicas), V (execução de contrato) e IX (proteção do crédito) fornecem parâmetros interpretativos relevantes. Especialmente relevante é o inciso IX, que autoriza o tratamento quando necessário para proteção da vida ou da incolumidade física do titular ou de terceiro, hipótese que poderia fundamentar o compartilhamento de dados de pessoas procuradas quando há risco concreto à segurança dos participantes do evento.

No que se refere aos dados sensíveis, categoria na qual se incluem os dados biométricos utilizados em sistemas de reconhecimento facial, o art. 11 da LGPD estabelece regime ainda mais restritivo. O tratamento de dados sensíveis somente pode ocorrer nas hipóteses previstas nos incisos I a X desse artigo, entre

as quais destacam-se: o consentimento do titular (inciso I), o cumprimento de obrigação legal ou regulatória (inciso II), a execução de políticas públicas previstas em leis ou regulamentos (inciso II, alínea a), e a proteção da vida ou da incolumidade física do titular ou de terceiro (inciso VII). A aplicação dessas hipóteses ao contexto de eventos culturais é complexa. O consentimento, embora seja a base legal mais segura sob a perspectiva da proteção de dados, pode ser de difícil obtenção em eventos de massa, especialmente quando se trata de pessoas procuradas que, por definição, não consentiriam voluntariamente com o tratamento. Por outro lado, a execução de políticas públicas de segurança (inciso II, alínea a) e a proteção da vida (inciso VII) podem fornecer fundamentação mais sólida, desde que demonstrada a necessidade e proporcionalidade da medida (BIONI, 2021).

Diante da análise dessas hipóteses, o art. 11, inciso II, alínea "a", da LGPD emerge como a base legal mais adequada para o tratamento de dados biométricos em contextos de segurança pública em eventos culturais. Esse dispositivo autoriza o tratamento sem consentimento do titular quando executadas políticas públicas previstas em leis ou regulamentos, condição verificada quando órgãos de segurança pública atuam com fundamento em suas atribuições constitucionais e legais. A adequação desse fundamento decorre de três razões convergentes: em primeiro lugar, a segurança pública constitui política pública constitucionalmente prevista nos arts. 6º e 144 da CF/88, o que satisfaz o requisito de previsão normativa exigido pelo dispositivo; em segundo lugar, a base legal independe do consentimento da pessoa de interesse da segurança, cujo paradeiro a autoridade busca identificar precisamente porque ela não se submete voluntariamente à abordagem; em terceiro lugar, a exigência de que o tratamento seja indispensável à execução da política pública impõe juízo de proporcionalidade que constitui salvaguarda contra o uso desmedido da tecnologia biométrica.

A utilização do art. 11, II, alínea "a", como base legal não é, contudo, ilimitada. Bioni (2021) adverte que a expressão "necessário" contida no dispositivo impõe ônus argumentativo ao controlador, que deve demonstrar, de forma documentada, que o tratamento biométrico não pode ser substituído por medida menos invasiva com eficácia equivalente. Essa exigência ganha especial relevo no contexto de eventos culturais de massa, onde a coleta biométrica indiscriminada de todos os participantes pode não satisfazer o critério de indispensabilidade quando os sistemas apresentam elevadas taxas de erro.

Malmann e Sulzbach (2020) acrescentam que o tratamento de dados sensíveis deve observar o princípio da minimização de forma estrita, priorizando abordagens baseadas em consulta a bancos de dados pré-selecionados em vez de varredura biométrica universal, modelo que reduz significativamente a exposição de titulares que não são objeto de interesse policial. Medeiros (2025), em estudo sobre o reconhecimento facial como política de segurança pública em Santa Catarina, confirma que a ausência de critérios objetivos de proporcionalidade na coleta biométrica constitui o principal fator de risco jurídico para as operações analisadas.

O art. 26 da LGPD assume particular relevância no contexto do compartilhamento de dados entre órgãos públicos e produtoras de eventos. Esse dispositivo estabelece que o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado em legítimo interesse. Mais importante ainda, o parágrafo 1º determina que o uso compartilhado de dados pessoais pelo controlador com outros controladores para o cumprimento de obrigação legal ou regulatória, para a execução de políticas públicas previstas em leis ou regulamentos ou para a realização de estudos por órgão de pesquisa deve ser informado ao titular. O parágrafo 2º complementa que é dispensada a exigência de consentimento para os dados tornados públicos, resguardados os direitos do titular e os princípios da LGPD. Esses dispositivos estabelecem que, mesmo quando o compartilhamento é legalmente autorizado, deve haver transparência em relação aos titulares e respeito aos princípios da finalidade, necessidade e adequação (MALMANN; SULZBACH, 2020).

Os princípios estabelecidos no art. 6º da LGPD assumem função estruturante mesmo em contextos de segurança pública. O princípio da finalidade (inciso I) exige que o tratamento seja realizado para propósitos legítimos, específicos, explícitos e informados ao titular, vedando o tratamento posterior de forma incompatível com essas finalidades. No contexto de eventos, isso significa que os dados compartilhados não podem ser utilizados para finalidades genéricas de “segurança”, mas devem ter destinação específica e delimitada (por exemplo, verificação de pessoas com mandados de prisão em aberto para prisões em flagrante durante o evento). O princípio da adequação (inciso II) determina que o tratamento deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento. O princípio da necessidade (inciso III), também chamado de minimização de dados, estabelece que o tratamento deve se limitar ao

mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento. Esse princípio é especialmente relevante no contexto de reconhecimento facial em eventos, pois impõe o questionamento sobre se a captura biométrica massiva de todos os participantes é realmente necessária ou se medidas menos invasivas poderiam atingir os mesmos objetivos de segurança (BIONI, 2021).

O princípio da transparência (inciso VI) assegura aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. No contexto de eventos culturais, isso se traduz no dever de informar, de forma clara e visível (por exemplo, no momento da compra do ingresso, no site do evento e na entrada do local), que haverá captura de imagens, uso de reconhecimento facial e compartilhamento de dados com órgãos de segurança, explicitando a finalidade, a base legal, o período de retenção e os direitos dos titulares. O princípio da segurança (inciso VII) exige a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Dados biométricos, por sua natureza sensível e permanente (diferentemente de senhas, que podem ser alteradas), exigem níveis particularmente elevados de proteção, incluindo criptografia, controle rigoroso de acessos e políticas claras de retenção e descarte (DONEDA; TEFFÉ, 2024).

A análise desses dispositivos permite concluir que, embora a LGPD preveja exceção para tratamento de dados em contextos de segurança pública, essa exceção não é absoluta nem dispensa completamente a observância de princípios fundamentais. No contexto de eventos culturais, onde há cooperação público-privada e interesses comerciais evidentes, a aplicabilidade integral ou parcial da LGPD deve ser avaliada caso a caso, considerando especialmente: (a) se a finalidade é exclusivamente de segurança pública ou se há também finalidades comerciais ou administrativas; (b) se o tratamento envolve dados sensíveis, especialmente biométricos; (c) se há base legal específica para o compartilhamento; (d) se são observados os princípios da necessidade, proporcionalidade e transparência; e (e) se há medidas adequadas de segurança e responsabilização. A ausência de regulamentação específica para a “LGPD Penal” torna ainda mais relevante a aplicação analógica e sistemática desses dispositivos, buscando

harmonizar a proteção de dados com a legítima atuação estatal na preservação da segurança pública.

2.3 LEI DE ACESSO À INFORMAÇÃO E CONVERGÊNCIA COM A LGPD

A Lei de Acesso à Informação (LAI), Lei nº 12.527, de 18 de novembro de 2011, constitui o segundo pilar normativo fundamental para compreender o regime jurídico do compartilhamento de dados entre órgãos públicos e entidades privadas. A LAI estabelece, em seu art. 3º, que o acesso à informação é direito fundamental, devendo ser assegurado mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão. O inciso I desse artigo consagra a publicidade como preceito geral e o sigilo como exceção, estabelecendo diretriz que pode, à primeira vista, parecer conflitante com a proteção de dados consagrada pela LGPD.

Entretanto, a própria LAI estabelece importantes ressalvas relacionadas à proteção de informações pessoais. O art. 6º, inciso III, determina que é dever dos órgãos e entidades promover, independentemente de requerimentos, a divulgação em local de fácil acesso de informações de interesse coletivo ou geral por eles produzidas ou custodiadas, mas o art. 21 estabelece que não podem ser objeto de acesso público informações consideradas sigilosas por razões de segurança da sociedade ou do Estado. O art. 23, por sua vez, estabelece que são consideradas imprescindíveis à segurança da sociedade ou do Estado informações cuja divulgação ou acesso irrestrito possam oferecer risco à vida, à segurança ou à saúde da população, às operações e planos estratégicos das Forças Armadas, às atividades de inteligência, bem como às ações de investigação e fiscalização em andamento. Esse dispositivo fornece fundamento para a manutenção de sigilo sobre listas de pessoas procuradas antes de sua utilização em eventos, evitando que a publicização prévia frustre a finalidade da medida (RIBEIRO, 2020).

Particularmente relevante para o objeto desta pesquisa é o art. 31 da LAI, que trata especificamente do tratamento de informações pessoais. O caput determina que o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. O § 1º estabelece que as informações pessoais relativas à intimidade, vida privada, honra e imagem terão seu

acesso restrito, independentemente de classificação de sigilo, pelo prazo máximo de 100 anos a contar da data de sua produção. O § 3º, por sua vez, dispõe que o consentimento do titular não é exigido quando as informações forem necessárias à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem. Esse dispositivo estabelece hipótese de tratamento de dados pessoais sem consentimento que antecipa, em certa medida, as bases legais posteriormente consagradas pela LGPD (MALMANN; SULZBACH, 2020).

A aparente tensão entre o dever de transparência estabelecido pela LAI e a proteção de dados consagrada pela LGPD foi objeto de importante pronunciamento da Controladoria-Geral da União no Parecer nº 00295/2020/CONJUR-CGU/CGU/AGU. Esse parecer, que se tornou referência fundamental para a interpretação conjunta dos dois diplomas legais, estabeleceu que não há, necessariamente, contradição entre LAI e LGPD, mas sim a necessidade de interpretação sistemática que leve em conta os princípios da finalidade, necessidade, transparência e interesse público. O parecer analisa especificamente a questão do compartilhamento e divulgação de dados pessoais pelo poder público, concluindo que a LAI deve ser interpretada à luz da LGPD e vice-versa, buscando harmonização que respeite tanto o direito à informação quanto à proteção de dados.

Um dos aspectos mais relevantes do Parecer CGU nº 295/2020 para o objeto desta pesquisa é a análise sobre o tratamento de dados de pessoas procuradas pela Justiça. O parecer estabelece que a situação de pessoa procurada por mandado de prisão constitui informação de evidente interesse público, não se enquadrando nas hipóteses de informação pessoal sigilosa previstas no art. 31 da LAI. Isso porque, segundo o entendimento da CGU, a condição de procurado pela Justiça não se refere à esfera da intimidade ou vida privada no sentido tradicional, mas sim a situação jurídica que afeta o interesse público e a ordem social. O parecer ressalva, contudo, que isso não autoriza a divulgação indiscriminada ou desproporcional, devendo ser observados os princípios da necessidade, adequação e segurança no tratamento desses dados. Especificamente, a CGU orienta que o compartilhamento de listas de pessoas procuradas entre órgãos públicos ou entre órgãos públicos e entidades privadas que atuem na execução de políticas públicas

deve ser feito mediante instrumentos formais que estabeleçam finalidade específica, medidas de segurança, prazo de retenção e responsabilidade solidária entre as partes (CONTROLADORIA-GERAL DA UNIÃO, 2020).

Essa interpretação da CGU fornece importante fundamento para o compartilhamento de dados em eventos culturais, mas impõe condicionantes rigorosas. Em primeiro lugar, estabelece que o compartilhamento deve ter finalidade específica relacionada à execução de política pública de segurança (no caso, prevenção de crimes e captura de foragidos durante eventos de massa), não podendo ser utilizado para finalidades comerciais ou administrativas alheias à segurança. Em segundo lugar, exige a formalização mediante termo de compartilhamento ou instrumento equivalente que delimite claramente as responsabilidades de cada parte, especialmente no que se refere à segurança dos dados compartilhados. Em terceiro lugar, determina que o compartilhamento deve observar os princípios da proporcionalidade e minimização, ou seja, somente devem ser compartilhados os dados estritamente necessários para a finalidade pretendida, pelo tempo estritamente necessário (MALMANN; SULZBACH, 2020).

Para identificar com precisão as convergências e aparentes contradições entre esses dois diplomas legais, realizou-se análise sistemática e comparativa dos dispositivos da LGPD (arts. 4º, 7º, 11, 23, 26) confrontados com os da LAI (arts. 3º, 6º, 8º, 21, 23, 31). Verificou-se que, embora exista tensão conceitual entre o dever de transparência imposto pela LAI e a proteção de dados sensíveis estabelecida pela LGPD, há pontos significativos de convergência que autorizam o compartilhamento de informações quando demonstrado o interesse público preponderante e observadas as salvaguardas de proporcionalidade, finalidade específica, segurança e responsabilização. A principal convergência identificada reside no reconhecimento, por ambos os diplomas legais, de que determinadas situações jurídicas relacionadas à segurança pública e à ordem social transcendem a esfera estritamente privada e justificam o tratamento de dados pessoais, desde que mediante procedimentos formalizados e transparentes. Essa análise comparativa foi sistematizada na Tabela de Dispositivos Legais apresentada no Anexo A deste trabalho, que confronta diretamente os artigos aplicáveis e identifica as bases legais para cada tipo de tratamento em eventos culturais, facilitando a consulta rápida dos fundamentos legais e evitando interpretações equivocadas dos dispositivos aplicáveis.

Nesse contexto regulatório, a atuação da Autoridade Nacional de Proteção de Dados tem sido fundamental para a consolidação de diretrizes interpretativas. A Decisão Administrativa ANPD de 2025 sobre reconhecimento facial em estádios de futebol estabeleceu precedente significativo, determinando que devem ser observados requisitos específicos mesmo havendo interesse legítimo de segurança pública: elaboração de DPIA detalhado, consentimento específico ou aviso claro, termo formal de compartilhamento, medidas técnicas de segurança e prazo determinado de retenção.

A Nota Técnica ANPD nº 175/2023 estabeleceu que a realização de DPIA torna-se obrigatória quando o tratamento envolve dados sensíveis de milhares de titulares. O Parecer Técnico sobre Sistemas de IA consolidou entendimento de que sistemas de reconhecimento facial submetem-se integralmente à LGPD, exigindo auditoria de viés e supervisão humana substantiva.

2.4 ORIENTAÇÕES DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A Autoridade Nacional de Proteção de Dados (ANPD), criada pela LGPD como autarquia em regime especial vinculada à Presidência da República (posteriormente vinculada ao Ministério da Justiça), tem desempenhado papel fundamental na interpretação e aplicação da legislação de proteção de dados no Brasil. Embora suas competências específicas na área de segurança pública sejam limitadas pela própria exceção do art. 4º da LGPD, a ANPD tem emitido orientações relevantes sobre o uso de tecnologias de reconhecimento facial e o tratamento de dados biométricos em contextos que guardam similaridade com eventos culturais, especialmente em estádios esportivos.

A Decisão Administrativa da ANPD de 2025 sobre o uso de reconhecimento facial em estádios de futebol estabeleceu precedente importante para eventos de massa. A ANPD condicionou o uso de sistemas de reconhecimento facial à existência de protocolo de segurança detalhado, elaboração de Relatório de Impacto à Proteção de Dados (DPIA), consentimento dos torcedores (quando aplicável) e aviso claro e ostensivo ao titular sobre a captura e tratamento de dados biométricos. A decisão vedou o compartilhamento irrestrito de dados sensíveis entre promotores privados e órgãos públicos, exigindo a formalização mediante termos específicos que delimitem finalidades, responsabilidades e medidas de segurança.

Adicionalmente, a ANPD determinou a realização de auditorias técnicas regulares nos sistemas utilizados e a disponibilização de canais de transparência ao público, onde os titulares possam conhecer como seus dados estão sendo tratados e exercer seus direitos (ANPD, 2025).

A Nota Técnica nº 175/2023 da ANPD, embora se refira especificamente ao acordo entre o Ministério da Justiça e Segurança Pública e a Confederação Brasileira de Futebol sobre reconhecimento facial em estádios, contém orientações de aplicação mais ampla. A ANPD recomenda avaliação prévia obrigatória mediante DPIA sempre que o tratamento envolver dados sensíveis em larga escala ou possa gerar riscos significativos aos direitos e liberdades fundamentais dos titulares. O relatório de impacto deve conter descrição dos processos de tratamento de dados pessoais, análise da necessidade e proporcionalidade da medida em relação aos fins pretendidos, análise dos riscos às liberdades e direitos fundamentais, medidas de segurança, salvaguardas e mecanismos de mitigação de riscos. A Nota Técnica também estabelece que deve haver registro documental completo de todas as operações de tratamento e que devem ser aplicados critérios rigorosos quanto à necessidade, adequação e proporcionalidade do uso de reconhecimento facial, limitando as hipóteses legais de sua utilização e exigindo transparência absoluta aos titulares (ANPD, 2023).

O Parecer Técnico da ANPD sobre Sistemas de Inteligência Artificial e Proteção de Dados Pessoais conforme a LGPD, publicado em 2023, estabelece diretrizes específicas para o uso de IA em tratamento de dados pessoais. O parecer determina que sistemas de IA que processem dados pessoais devem observar todos os princípios da LGPD, especialmente finalidade, adequação, necessidade, transparência, não discriminação e responsabilização. Quanto ao reconhecimento facial especificamente, a ANPD alerta para os riscos de viés algorítmico, que podem resultar em discriminação racial ou de gênero, e para os perigos de falsos positivos, especialmente quando utilizados para fins de segurança pública. O parecer recomenda que controladores de dados que utilizem reconhecimento facial implementem mecanismos de supervisão humana (*human-in-the-loop*), garantindo que decisões significativas baseadas em processamento automatizado sejam sempre revisadas por operadores humanos antes de gerarem consequências concretas para os titulares. Adicionalmente, o parecer exige relatórios públicos de

impacto e auditorias independentes de viés sempre que sistemas de IA forem utilizados em contextos sensíveis que afetem direitos fundamentais (ANPD, 2023).

A orientação conjunta ANPD/CGU para eventos de massa, embora não formalmente consolidada em documento único, pode ser inferida da compilação de diversos pareceres, notas técnicas e decisões administrativas. Essa orientação sinaliza a necessidade de adoção de cláusulas contratuais específicas em instrumentos de compartilhamento de dados entre órgãos públicos e empresas do setor de eventos, estabelecendo auditorias periódicas, tanto internas quanto externas, e exigindo instrumentos robustos de governança que incluam designação de encarregado de proteção de dados (DPO), implementação de políticas de segurança da informação, treinamento de colaboradores e estabelecimento de canais efetivos para exercício dos direitos dos titulares. A orientação conjunta também enfatiza a necessidade de descarte seguro dos dados após o término do evento e da finalidade específica que justificou sua coleta, vedando a retenção indefinida ou o uso para finalidades distintas das originalmente informadas (MALMANN; SULZBACH, 2020).

As principais decisões, notas técnicas e pareceres da ANPD sobre o tema encontram-se compilados no Anexo C deste trabalho para consulta detalhada, evidenciando o endurecimento progressivo da fiscalização pela autoridade reguladora e a crescente exigência de instrumentos formais de governança de dados, especialmente em contextos que envolvam tratamento de dados sensíveis e tecnologias de alto risco como reconhecimento facial. Essa compilação demonstra que a ANPD tem adotado postura de rigor crescente no que se refere ao uso de tecnologias de reconhecimento facial em eventos de massa, condicionando sua licitude à observância cumulativa de múltiplos requisitos: base legal específica, finalidade delimitada, avaliação de impacto, transparência ao titular, medidas robustas de segurança, supervisão humana, auditorias independentes e canais efetivos de contestação

A análise comparativa de quatro jurisdições maduras revelou convergências significativas (Quadro 2).

Quadro 2 — Convergências internacionais em proteção de dados biométricos

Jurisdição	Requisito-Chave	Autoridade
União Europeia (GDPR)	DPIA obrigatória; dados biométricos = categoria especial	DPA's nacionais
Reino Unido	Live Facial Recognition exige consulta pública e DPIA	ICO
Canadá (PIPEDA)	Consentimento válido exige compreensão real dos riscos	OPC
EUA (Privacy Act)	Regras para compartilhamento interagências	Múltiplas agências
CONVERGÊNCIAS	8 requisitos: DPIA, consentimento, transparência, supervisão humana, prazo, segurança, auditoria viés, accountability	Todas

Fonte: Elaborado pelos autores

Legenda: com base em GDPR (UE), UK GDPR, PIPEDA (Canadá) e Privacy Act (EUA).

As convergências identificadas no Quadro 2, observadas em sistemas jurídicos com tradições distintas (*common law*, *civil law*, modelos regulatórios centralizado e descentralizado), evidenciam consenso global emergente sobre garantias mínimas essenciais para uso legítimo de dados biométricos em larga escala. A recorrência de exigências como avaliação prévia de impacto, transparência ativa, auditoria de viés algorítmico e supervisão humana substantiva transcende particularidades culturais ou opções político-legislativas locais, refletindo padrões internacionais consolidados que orientam boas práticas na proteção de direitos fundamentais em contextos de uso intensivo de tecnologias invasivas. Particularmente relevante é a ênfase unânime na Data Protection Impact Assessment, que todas as jurisdições analisadas consideram requisito incontornável para operações de tratamento de dados biométricos em larga escala, não constituindo mera formalidade burocrática, mas instrumento essencial de identificação de riscos concretos, proposição de mitigações específicas e documentação da proporcionalidade da medida adotada.

A análise comparativa internacional demonstra que a proteção de dados biométricos em eventos de massa não constitui especificidade brasileira sem precedentes, mas tema amplamente regulado em jurisdições maduras mediante parâmetros convergentes. Essa convergência internacional reforça a legitimidade das diretrizes propostas nesta pesquisa para o contexto brasileiro, na medida em que não se baseiam em interpretações insulares da LGPD, mas em padrões

globalmente reconhecidos que fundamentam aplicação consistente de direitos fundamentais. O Brasil, ao adotar exigências similares às identificadas internacionalmente, alinha-se a consenso global sobre equilíbrio necessário entre segurança pública e proteção de dados, evitando tanto lassidão regulatória quanto rigorismo desproporcional.

2.5 MODELOS INTERNACIONAIS DE REGULAMENTAÇÃO

A análise de modelos internacionais de proteção de dados fornece parâmetros comparativos relevantes para compreender as tendências globais de regulamentação do compartilhamento de dados em eventos e o tratamento de dados biométricos. Embora cada jurisdição apresente particularidades que refletem suas tradições jurídicas e arranjos institucionais específicos, observa-se convergência significativa quanto à necessidade de proteção especial para dados sensíveis e de mecanismos de accountability para agentes de tratamento.

O Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), Regulamento (UE) 2016/679, constitui o padrão de ouro internacional em matéria de proteção de dados e serviu de inspiração para a LGPD brasileira. O GDPR estabelece, em seu art. 5º, seis princípios fundamentais: licitude, lealdade e transparência; limitação das finalidades; minimização dos dados; exatidão; limitação da conservação; e integridade e confidencialidade. Esses princípios são substancialmente similares aos consagrados no art. 6º da LGPD, demonstrando a influência do modelo europeu sobre a legislação brasileira. O art. 9º do GDPR trata especificamente do tratamento de categorias especiais de dados pessoais (dados sensíveis), entre os quais se incluem explicitamente os dados biométricos destinados a identificar uma pessoa de forma inequívoca. O tratamento de tais dados é, em princípio, proibido, salvo nas hipóteses taxativamente previstas nas alíneas do parágrafo 2º, entre as quais destacam-se o consentimento explícito, a proteção de interesses vitais quando o titular não puder consentir, e razões de interesse público importante baseadas no direito da União ou de um Estado-Membro (UNIÃO EUROPEIA, 2016).

O art. 35 do GDPR estabelece a obrigatoriedade de Avaliação de Impacto sobre a Proteção de Dados (DPIA) quando o tratamento for suscetível de implicar riscos elevados para os direitos e liberdades das pessoas. O parágrafo 3º especifica

que a avaliação é obrigatória especialmente em caso de avaliação sistemática e completa dos aspectos pessoais de pessoas singulares, que se baseia num tratamento automatizado e com base no qual são tomadas decisões que produzem efeitos jurídicos relativamente à pessoa em causa ou que a afetem significativamente de forma similar (alínea a), e em caso de tratamento em grande escala de categorias especiais de dados (alínea b). O tratamento de dados biométricos mediante reconhecimento facial em eventos de massa enquadra-se perfeitamente nessas hipóteses, tornando a DPIA obrigatória segundo o modelo europeu. O art. 35 também determina que a avaliação deve conter, no mínimo, descrição sistemática das operações de tratamento previstas, avaliação da necessidade e proporcionalidade das operações de tratamento, avaliação dos riscos para os direitos e liberdades dos titulares, e medidas previstas para fazer face aos riscos (UNIÃO EUROPEIA, 2016).

O UK GDPR, versão do GDPR aplicável ao Reino Unido após o Brexit, mantém estrutura substancialmente similar ao GDPR europeu, com adaptações pontuais que refletem a saída do país da União Europeia. O Information Commissioner's Office (ICO), autoridade britânica de proteção de dados, tem emitido orientações específicas sobre o uso de reconhecimento facial em espaços públicos e eventos. O ICO destaca que sistemas de reconhecimento facial em tempo real (*live facial recognition*) constituem tratamento de alto risco que exige base legal robusta, transparência absoluta mediante avisos claros e visíveis, avaliação de impacto prévia, e mecanismos efetivos para que indivíduos possam exercer seus direitos, incluindo o direito de não serem submetidos a decisões baseadas exclusivamente em tratamento automatizado. O ICO também enfatiza que a simples alegação de que o reconhecimento facial serve a fins de segurança não é suficiente para justificar seu uso, sendo necessário demonstrar que a medida é necessária, proporcional e que não existem meios menos invasivos de atingir os mesmos objetivos (ICO, 2021-2024).

No Canadá, o Personal Information Protection and Electronic Documents Act (PIPEDA), promulgado em 2000, estabelece regime de proteção de dados baseado em dez princípios de práticas justas de informação (Fair Information Practices). Embora anterior ao GDPR e à LGPD, o PIPEDA antecipa vários elementos que se tornaram comuns em legislações posteriores, especialmente a ênfase no consentimento significativo (*meaningful consent*) como base primordial para

tratamento de dados pessoais. O Office of the Privacy Commissioner of Canada tem emitido orientações enfatizando que o consentimento somente é válido quando o titular compreende plenamente a natureza, finalidade e consequências do tratamento, o que impõe desafios significativos para o uso de reconhecimento facial em eventos, onde muitos participantes podem não estar plenamente cientes da captura biométrica. O comissário canadense também tem destacado que, mesmo quando há base legal alternativa ao consentimento (por exemplo, proteção de interesses vitais), deve haver transparência absoluta e oportunidade para o titular contestar ou limitar o tratamento (CANADÁ, 2000; OPC, 2018-2024).

Nos Estados Unidos, ao contrário da Europa e do Brasil, não existe lei federal geral de proteção de dados, prevalecendo modelo setorial e federado no qual diferentes leis regulam aspectos específicos (proteção de dados de saúde pelo HIPAA, dados financeiros pelo Gramm-Leach-Bliley Act, etc.). O Privacy Act of 1974 regula especificamente o tratamento de dados pelo governo federal, estabelecendo princípios de limitação de finalidade, minimização de dados e direitos de acesso e retificação, mas sua aplicação é limitada a agências federais. Alguns estados, especialmente a Califórnia (com o California Consumer Privacy Act - CCPA), têm promulgado legislações estaduais de proteção de dados. No que se refere especificamente ao reconhecimento facial, alguns estados e municípios americanos têm adotado moratórias ou proibições totais ao uso dessa tecnologia por agências governamentais (San Francisco, Boston, Portland), refletindo preocupações com vieses algorítmico, discriminação racial e vigilância excessiva. A Federal Trade Commission (FTC), embora não seja propriamente autoridade de proteção de dados, tem atuado na fiscalização de práticas comerciais desleais relacionadas ao tratamento de dados biométricos, especialmente quando há falta de transparência ou uso incompatível com as expectativas razoáveis dos consumidores (ESTADOS UNIDOS, 1974; FTC, 2020-2024).

Buscando parâmetros internacionais consolidados para balizar a discussão sobre compartilhamento de dados em eventos, examinou-se a disciplina dessa matéria sob a ótica do GDPR europeu, UK GDPR, PIPEDA canadense e Privacy Act norte-americano. Identificou-se consenso significativo quanto à necessidade de: (a) avaliação de impacto prévia sempre que o tratamento envolva dados biométricos em larga escala; (b) consentimento informado e específico quando esta for a base legal escolhida, ou demonstração de base legal alternativa igualmente robusta; (c)

transparência absoluta mediante avisos claros, acessíveis e compreensíveis sobre a captura e tratamento de dados; (d) mecanismos efetivos de contestação, retificação e exclusão de dados; (e) medidas técnicas e organizacionais robustas de segurança da informação; (f) limitação de finalidade e proibição de tratamento posterior incompatível; (g) minimização de dados e limitação de retenção temporal; e (h) supervisão por autoridade independente com poderes de fiscalização e sanção. Essa análise comparativa foi sistematizada no Anexo B deste trabalho, que apresenta quadro consolidado dos principais parâmetros normativos de cada jurisdição examinada, oferecendo fundamento comparativo para a construção de diretrizes brasileiras e proposições de boas práticas especialmente relevantes ao abordar reconhecimento facial, monitoramento e integração público-privada em eventos de massa.

2.6 SÍNTESE DA FUNDAMENTAÇÃO NORMATIVA

A revisão de literatura apresentada nas subseções precedentes permite sintetizar a fundamentação normativa aplicável ao compartilhamento de dados de pessoas de interesse da segurança pública entre órgãos públicos e produtoras de eventos culturais no Brasil. Essa síntese estrutura-se em torno de quatro eixos fundamentais: a trajetória evolutiva da proteção de dados no ordenamento brasileiro, as bases legais da LGPD aplicáveis mesmo em contextos de segurança pública, a convergência entre LGPD e LAI estabelecida pelo Parecer CGU nº 295/2020, e os parâmetros internacionais consolidados que fornecem orientação comparativa.

No que se refere à evolução normativa, evidenciou-se que o Brasil passou de modelo de tutela genérica da privacidade (CF/88) para regime especializado de governança de dados (LGPD), com o reconhecimento definitivo da proteção de dados como direito fundamental autônomo pela EC 115/2022. Essa trajetória, contudo, deixou lacuna significativa: a ausência de regulação específica para o tratamento de dados na esfera penal e de segurança pública (inexistência de “LGPD Penal”), criando zona de incerteza jurídica que afeta diretamente eventos culturais que demandam cooperação entre órgãos de segurança e produtoras privadas.

Quanto às bases legais da LGPD, identificou-se que a exceção do art. 4º, III (fins exclusivos de segurança pública) deve ser interpretada restritivamente, não se aplicando quando há conjugação de finalidades de segurança com finalidades

comerciais ou quando o tratamento envolve entidades privadas com interesses econômicos evidentes.

Nesses casos, permanecem aplicáveis as hipóteses de tratamento dos arts. 7º e 11 da LGPD, especialmente: cumprimento de obrigação legal (art. 7º, II), execução de políticas públicas (art. 7º, III, e art. 11, II, a), proteção da vida ou incolumidade física (art. 7º, IX, e art. 11, VII), e legítimo interesse do controlador (art. 7º, IX), sempre observados os princípios de finalidade, necessidade, adequação, transparência e segurança (art. 6º). Para dados biométricos tratados mediante reconhecimento facial, as exigências são ainda mais estritas, incluindo obrigatoriamente avaliação de impacto (DPIA), medidas robustas de segurança e supervisão humana para evitar decisões exclusivamente automatizadas com efeitos significativos.

No que concerne à convergência LGPD-LAI, a análise do Parecer CGU nº 295/2020 revelou que não há contradição insuperável entre transparência administrativa e proteção de dados, mas sim necessidade de harmonização mediante ponderação caso a caso. O parecer estabelece que a condição de pessoa procurada pela Justiça constitui informação de interesse público que justifica o compartilhamento entre órgãos públicos e entidades privadas que executam políticas públicas, desde que: (a) haja finalidade específica e legítima relacionada à segurança pública; (b) o compartilhamento seja formalizado mediante termo que delimite responsabilidades; (c) sejam observadas medidas adequadas de segurança; (d) haja limitação temporal (dados não podem ser retidos indefinidamente); e (e) seja garantida transparência aos titulares quanto à existência e finalidade do tratamento, resguardado o sigilo operacional necessário à eficácia da medida.

A análise comparativa com modelos internacionais (GDPR, UK GDPR, PIPEDA, Privacy Act) evidenciou convergência global quanto a parâmetros mínimos de proteção de dados biométricos: DPIA obrigatória para tratamento em larga escala, transparência mediante avisos ostensivos, consentimento específico quando aplicável, direitos de acesso e contestação, auditorias independentes de viés algorítmico, supervisão humana em decisões significativas, e limitação temporal de retenção. Esses parâmetros fornecem orientação valiosa para a construção de protocolos brasileiros, especialmente considerando que a LGPD foi fortemente inspirada no GDPR.

Com base nessa síntese, é possível estabelecer conclusão provisória: existe base legal para o compartilhamento de dados de pessoas de interesse da segurança pública entre órgãos públicos e produtoras de eventos culturais, desde que observadas, cumulativamente, as seguintes condições: (1) demonstração de interesse público preponderante relacionado à segurança dos participantes e à captura de foragidos; (2) finalidade específica e delimitada, vedada a utilização para fins comerciais ou administrativos alheios à segurança; (3) proporcionalidade e necessidade da medida, demonstrando que não existem meios menos invasivos para atingir os mesmos objetivos; (4) transparência ao titular mediante avisos claros sobre a existência de captura de imagens, reconhecimento facial e compartilhamento de dados; (5) formalização mediante termo de compartilhamento que estabeleça responsabilidade solidária nos termos do art. 26 da LGPD; (6) elaboração de Avaliação de Impacto à Proteção de Dados (DPIA) quando houver uso de reconhecimento facial ou tratamento de dados biométricos em larga escala; (7) implementação de medidas técnicas e organizacionais adequadas de segurança, incluindo criptografia, controle rigoroso de acessos e logs de auditoria; (8) limitação temporal estrita, com descarte seguro dos dados após o término do evento e cumprimento da finalidade; (9) supervisão humana em decisões baseadas em reconhecimento facial automatizado, especialmente quando gerarem bloqueios de acesso ou outras consequências significativas; e (10) disponibilização de canal efetivo para exercício dos direitos dos titulares, incluindo acesso, retificação, contestação e exclusão de dados.

Estabelecidos os marcos normativos e os limites jurídicos do compartilhamento, cabe agora examinar, na seção de Análise e Discussão dos Resultados que se segue, como essas diretrizes se concretizam ou são violadas na prática dos grandes eventos culturais brasileiros, identificando os principais riscos jurídicos e propondo instrumentos de governança que harmonizem efetivamente segurança pública e proteção de direitos fundamentais.

2.7 LIMITES CONSTITUCIONAIS DA ATUAÇÃO PREVENTIVA ESTATAL

A análise das bases legais e dos riscos jurídicos identificados nas subseções precedentes exige, como complemento necessário, o exame dos limites constitucionais que circunscrevem a atuação preventiva do Estado em contextos de

vigilância de massa. Esses limites não derivam de norma infraconstitucional, mas dos próprios fundamentos da ordem democrática estabelecida pela Constituição Federal de 1988, especialmente da dignidade da pessoa humana (art. 1º, III), da inviolabilidade da intimidade e da vida privada (art. 5º, X), da inviolabilidade das comunicações (art. 5º, XII) e da presunção de inocência (art. 5º, LVII).

O art. 5º, inciso X, da CF/88 consagra proteção expressa à intimidade, à vida privada, à honra e à imagem das pessoas, assegurando indenização pelo dano material ou moral decorrente de sua violação. Essa tutela constitucional alcança dados biométricos, que constituem projeção da identidade física da pessoa, representação irrepetível e inalterável que, uma vez coletada e armazenada sem controle adequado, produz exposição permanente da personalidade do titular. A coleta biométrica universal de participantes de eventos culturais, sem que haja suspeita individualizada ou fundada razão de interesse policial, confronta diretamente essa proteção, pois subordina a fruição de direito cultural ao fornecimento compulsório de informação corporal irreversível.

O princípio da proporcionalidade, embora não positivado expressamente no texto constitucional, é amplamente reconhecido pela doutrina e pela jurisprudência do Supremo Tribunal Federal como elemento intrínseco ao Estado Democrático de Direito, operando como critério de controle da validade de medidas restritivas de direitos fundamentais. A sua aplicação ao reconhecimento facial em eventos culturais exige o exame de três subprincípios: adequação (a medida é apta para alcançar a finalidade de segurança pretendida?), necessidade (não existe meio menos gravoso com eficácia equivalente?) e proporcionalidade em sentido estrito (o benefício esperado supera o custo em termos de direitos fundamentais?). Duarte e Ceia (2022) demonstram que sistemas de reconhecimento facial com taxas expressivas de falso positivo podem não superar o teste da adequação, na medida em que abordagens policiais baseadas em erros algorítmicos produzem efeito inverso ao de segurança pública, gerando insegurança jurídica e exposição de inocentes.

O princípio da razoabilidade, por sua vez, impõe que as medidas estatais guardem correspondência entre a situação fática que as motiva e a resposta normativa adotada. No contexto de eventos culturais, isso significa que a intensidade da vigilância biométrica deve ser proporcional ao nível de risco efetivamente demonstrado para aquele evento específico, vedando-se a adoção de protocolos de

vigilância máxima como padrão genérico, independentemente do histórico e das características de cada evento. A extrapolação do poder de polícia para patamares de vigilância permanente e generalizada configura o que a doutrina denomina estado de vigilância preventiva, modalidade de controle social que Bioni (2021) identifica como estruturalmente incompatível com o modelo constitucional brasileiro, ncompatível com o modelo constitucional brasileiro, posição reforçada por Medeiros (2025) ao constatar que a ausência de marcos regulatórios específicos para o reconhecimento facial em segurança pública no âmbito estadual reproduz esse padrão de vigilância não balizada constitucionalmente, por inverter a lógica da presunção de inocência.

A vedação ao estado de vigilância permanente não implica, todavia, a proibição absoluta do uso de tecnologias de reconhecimento facial em eventos culturais. O que a ordem constitucional proíbe é o uso irrestrito, desproporcional e não supervisionado dessas tecnologias. Intervenções biométricas pontuais, fundadas em mandados de prisão pré-identificados, com revisão humana obrigatória e descarte imediato dos dados de pessoas não identificadas como de interesse policial, podem ser compatíveis com os limites constitucionais, desde que operadas com transparência, sob controle independente e com mecanismos efetivos de responsabilização pelos erros inevitáveis do sistema (MALMANN; SULZBACH, 2020).

A delimitação desses limites constitucionais não encerra o debate, mas estabelece o quadro normativo dentro do qual qualquer solução prática deve ser construída. A convergência entre os princípios da proporcionalidade, da razoabilidade e da vedação ao estado de vigilância permanente com os dispositivos da LGPD e da LAI analisados nas subseções anteriores revela que o ordenamento jurídico brasileiro já dispõe de ferramentas suficientes para disciplinar o compartilhamento de dados biométricos em eventos culturais, ainda que de forma assistemática e carente de regulamentação específica. Identificados os marcos normativos, os limites jurídicos e os riscos concretos que permeiam essa prática, cabe à análise subsequente examinar como esses parâmetros se verificam ou se distanciam da realidade operacional dos grandes eventos culturais brasileiros, avaliando a suficiência das soluções existentes e propondo instrumentos de conformidade capazes de harmonizar, de forma efetiva, segurança pública e proteção de direitos fundamentais.

3 METODOLOGIA

A presente pesquisa adota abordagem jurídico-dogmática com método qualitativo, estruturada de modo a privilegiar o engajamento com problemas reais e a construção de soluções práticas aplicáveis ao contexto do compartilhamento de dados em eventos culturais. Conforme defendem Almeida e Estellita (2021), essa perspectiva permite não apenas descrever o fenômeno jurídico em sua dimensão abstrata, mas avançar para a proposição de instrumentos concretos que possam ser utilizados por operadores do direito, gestores públicos e agentes privados. A metodologia estrutura-se em seis etapas interdependentes: caracterização da pesquisa, coleta de dados de múltiplas fontes, análise mediante técnicas específicas, construção de ferramentas práticas, identificação de limitações e observância de procedimentos éticos. Essa arquitetura metodológica reflete a natureza aplicada do trabalho, que objetiva não apenas diagnosticar lacunas normativas, mas propor caminhos viáveis de conformidade legal.

3.1 CARACTERIZAÇÃO DA PESQUISA

A pesquisa caracteriza-se como qualitativa, aplicada e exploratória quanto aos seus objetivos. A natureza qualitativa justifica-se pela impossibilidade de quantificação do fenômeno investigado, que envolve interpretação de textos normativos, ponderação de princípios constitucionais potencialmente conflitantes e construção de parâmetros aplicativos para casos concretos. Conforme Creswell (2014), a abordagem qualitativa mostra-se adequada quando o objetivo transcende a mensuração, direcionando-se à compreensão de significados, interpretação de normas e proposição de soluções para problemas complexos que admitem múltiplas respostas válidas. A pesquisa é aplicada porque visa gerar conhecimento prático direcionado à solução de problema específico identificado na realidade social: a ausência de diretrizes claras para o compartilhamento legal de dados biométricos entre órgãos de segurança pública e produtoras de eventos culturais.

Quanto aos objetivos, a pesquisa assume caráter exploratório em razão da incipiente produção acadêmica sobre a convergência entre LGPD e LAI especificamente no contexto de eventos culturais de massa. A abordagem é dedutiva, partindo-se do marco normativo geral estabelecido pela Lei nº 13.709/2018

e pela Lei nº 12.527/2011 para aplicação em contexto específico, culminando na proposição de ferramentas práticas de conformidade. Essa progressão lógica do geral ao particular permite não apenas identificar requisitos legais abstratos, mas traduzi-los em procedimentos operacionais verificáveis, atendendo à demanda por aplicabilidade imediata do conhecimento produzido pela pesquisa acadêmica.

3.2 COLETA DE DADOS

A coleta de dados abrangeu cinco categorias de fontes, selecionadas segundo critério de pertinência temática e confiabilidade metodológica. As fontes normativas primárias compreenderam a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), a Lei de Acesso à Informação (Lei nº 12.527/2011), a Constituição Federal de 1988, o Marco Civil da Internet (Lei nº 12.965/2014), decretos regulamentadores e resoluções da Autoridade Nacional de Proteção de Dados.

A sistematização dessas fontes ocorreu mediante leitura artigo por artigo, fichamento de dispositivos relevantes e mapeamento de convergências e aparentes tensões normativas, com ênfase nos artigos que disciplinam bases legais para tratamento de dados, compartilhamento entre setor público e privado, e exceções relativas à segurança pública.

As fontes doutrinárias privilegiaram autores brasileiros especializados em proteção de dados e direito digital, destacando-se Bioni (2021), Mendes (2019), Doneda (2019), Malmann e Sulzbach (2020), Duarte e Ceia (2022), além de Almeida e Estellita (2021) quanto aos aspectos de segurança pública. Complementarmente, consultaram-se autores internacionais de referência e documentos de organismos multilaterais como a OCDE.

O critério de seleção priorizou relevância acadêmica e atualidade temporal, concentrando-se em obras publicadas após a promulgação da LGPD. A análise doutrinária foi conduzida mediante fichamento temático e categorização por tópicos estruturantes, tais como bases legais para tratamento de dados sensíveis, regime de compartilhamento intersetorial, princípios de proteção e governança de dados.

As fontes jurisprudenciais abrangeram decisões do Superior Tribunal de Justiça, Supremo Tribunal Federal e tribunais estaduais, selecionadas segundo critério de pertinência com os temas de proteção de dados pessoais, tecnologias de

reconhecimento facial e discriminação algorítmica. Identificou-se limitação estrutural relevante: em razão da vigência recente da LGPD, iniciada em setembro de 2020, a jurisprudência consolidada ainda é escassa, predominando decisões de primeira instância sem manifestação consolidada das cortes superiores sobre controvérsias específicas relativas ao compartilhamento de dados em eventos culturais. Essa limitação impôs necessidade de aplicação analógica de precedentes envolvendo contextos similares, como estabelecimentos comerciais e condomínios residenciais.

As fontes documentais compreenderam políticas de privacidade publicadas por grandes eventos culturais brasileiros, notadamente Rock in Rio, Lollapalooza e Carnaval de Salvador, além de termos de uso disponibilizados ao público, avisos sobre coleta de dados biométricos e pareceres jurídicos, com destaque para o Parecer CGU nº 295/2020, que constitui referência interpretativa fundamental sobre a convergência entre LGPD e LAI.

Adicionalmente, analisaram-se decisões administrativas, notas técnicas e pareceres emitidos pela ANPD, incluindo a recente decisão sobre uso de reconhecimento facial em estádios de futebol. A obtenção desses documentos ocorreu mediante consulta a sites oficiais, repositórios públicos e, em alguns casos, solicitações via Lei de Acesso à Informação, sendo que algumas solicitações não foram adequadamente respondidas sob alegação de sigilo operacional.

Por fim, incorporaram-se pesquisas empíricas secundárias conduzidas por instituições de referência, notadamente a pesquisa CETIC.BR (2023) sobre privacidade e proteção de dados pessoais no Brasil, o estudo de Duarte e Ceia (2022) sobre uso de reconhecimento facial no Carnaval de Salvador, e relatórios técnicos internacionais do Massachusetts Institute of Technology e do National Institute of Standards and Technology sobre viés algorítmico em sistemas de reconhecimento facial. Esses dados secundários permitiram contextualizar percepções sociais sobre privacidade, documentar casos concretos de aplicação das tecnologias analisadas e fundamentar empiricamente as discussões sobre riscos de discriminação algorítmica.

3.3 PROCEDIMENTOS DE ANÁLISE

A análise dos documentos normativos e jurisprudenciais empregou o método hermenêutico jurídico, privilegiando a interpretação sistemática e teleológica da

legislação. Conforme orienta Maximiliano (2020), a interpretação sistemática considera cada dispositivo legal em relação ao conjunto normativo ao qual pertence, identificando coerências e resolvendo aparentes antinomias mediante ponderação de princípios. O processo analítico estruturou-se em quatro momentos interdependentes: leitura literal dos dispositivos legais para apreensão do sentido textual imediato; identificação de princípios subjacentes e finalidades normativas que orientam a aplicação das regras; confronto sistemático entre LGPD e LAI para identificação de convergências e tensões interpretativas; e aplicação interpretativa aos casos concretos de eventos culturais, verificando compatibilidade das práticas observadas com os requisitos normativos identificados.

A análise de direito comparado abrangeu quatro jurisdições representativas de diferentes tradições jurídicas: General Data Protection Regulation da União Europeia, UK GDPR do Reino Unido, Personal Information Protection and Electronic Documents Act do Canadá e Privacy Act dos Estados Unidos. O objetivo consistiu em identificar convergências internacionais e boas práticas consolidadas que pudessem informar a interpretação do regime brasileiro, evitando soluções insulares desconectadas do consenso global emergente. O método empregou leitura sistemática de orientações oficiais publicadas pelas autoridades de proteção de dados dessas jurisdições, seguida de síntese comparativa em formato de quadro analítico, identificando requisitos recorrentes que transcendem particularidades culturais e jurídicas de cada sistema.

Adicionalmente, as políticas de privacidade dos eventos culturais constituíram corpus documental analisado mediante técnica de análise de conteúdo, conforme sistematizada por Bardin (2016). Examinaram-se oito políticas de grandes eventos brasileiros, aplicando-se categorias analíticas predefinidas: existência de menção explícita ao uso de tecnologias de reconhecimento facial; informação transparente sobre compartilhamento de dados com órgãos públicos de segurança; linguagem acessível ao consumidor médio versus terminologia jurídica hermética; e disponibilização de canal efetivo para exercício de direitos de contestação. Os resultados dessa análise, validados pelo cruzamento com dados da pesquisa CETIC.BR (2023), evidenciaram que apenas 31% das políticas analisadas atendem requisitos mínimos de transparência exigidos pela LGPD.

3.4 CONSTRUÇÃO DAS FERRAMENTAS PRÁTICAS

Esta seção documenta a lógica metodológica subjacente ao desenvolvimento de cada ferramenta prática produzida pela pesquisa, explicitando o raciocínio que conduziu da identificação do problema à proposição de solução operacional. Conforme defendem Lakatos e Marconi (2017), a pesquisa aplicada diferencia-se da pesquisa básica precisamente pela ênfase na produção de conhecimento imediatamente utilizável para resolução de problemas concretos, exigindo que o percurso metodológico seja explicitado de modo a permitir replicação e validação externa. As ferramentas desenvolvidas traduzem requisitos legais abstratos em procedimentos verificáveis, cumprindo função tanto pedagógica quanto prática ao democratizar o acesso à conformidade legal para gestores sem formação jurídica especializada.

O Quadro Comparativo LGPD x LAI foi desenvolvido para resolver problema interpretativo identificado durante a revisão de literatura: a aparente contradição entre o princípio da publicidade consagrado pela Lei de Acesso à Informação e o regime de proteção estabelecido pela Lei Geral de Proteção de Dados. A solução metodológica adotada consistiu na sistematização comparativa de dispositivos legais pertinentes de ambos os diplomas.

O processo envolveu quatro etapas sequenciais: seleção dos artigos pertinentes mediante leitura integral de ambas as leis e identificação de dispositivos aplicáveis ao compartilhamento de dados (artigos 7º, 9º, 11, 23 e 26 da LGPD; artigos 3º, 6º e 31 da LAI); análise individualizada de cada dispositivo quanto à base legal que estabelece, hipótese de aplicação e requisitos procedimentais; identificação das convergências normativas, demonstrando que ambos os diplomas permitem o compartilhamento sob condições específicas e cumulativas; e síntese em quadro de quatro colunas para consulta prática pelos operadores. A validação dessa ferramenta ocorreu mediante confronto com o Parecer CGU nº 295/2020, que confirmou a compatibilidade interpretativa proposta.

O Quadro de Modelos Internacionais respondeu ao diagnóstico de que o Brasil carece de regulação específica para o compartilhamento de dados biométricos em eventos culturais, tornando necessário buscar parâmetros em jurisdições com regulação mais madura. A solução metodológica adotada foi a análise comparativa internacional sistemática. O processo compreendeu cinco etapas: seleção de quatro jurisdições representativas de diferentes tradições jurídicas, assegurando diversidade geográfica e normativa (União Europeia, Reino Unido, Canadá e

Estados Unidos); leitura sistemática das legislações específicas sobre proteção de dados e orientações oficiais publicados pelas autoridades reguladoras sobre uso de tecnologias biométricas e compartilhamento entre setores público e privado; extração dos requisitos-chave recorrentes, identificando exigências que aparecem de forma consistente em múltiplas jurisdições, tais como Data Protection Impact Assessment, consentimento informado específico, transparência ativa e supervisão humana substantiva; identificação de oito convergências internacionais que transcendem particularidades culturais; e síntese em quadro de três colunas. A aplicação desses parâmetros internacionais fundamenta e confere legitimidade às diretrizes propostas para o contexto brasileiro, evitando soluções insulares.

O Quadro de Práticas em Eventos Brasileiros foi desenvolvido para enfrentar o problema da lacuna entre prescrição normativa e prática efetiva, respondendo à questão metodológica: como eventos reais operam atualmente? A solução adotada foi o mapeamento empírico das práticas de grandes eventos paradigmáticos. O processo envolveu seis etapas: seleção intencional de três eventos que representam diferentes modelos operacionais (Rock in Rio como parceria formal com órgão de segurança, Lollapalooza como modelo híbrido voluntário-obrigatório, e Carnaval de Salvador como vigilância massiva governamental); análise sistemática das políticas de privacidade publicadas em seus sites oficiais, verificando informações disponibilizadas ao público sobre coleta e compartilhamento de dados biométricos; pesquisa de reportagens especializadas publicadas em veículos de imprensa de referência (Folha de S.Paulo, G1, Consultor Jurídico, Migalhas) sobre incidentes envolvendo reconhecimento facial nesses eventos; cruzamento dos achados com o estudo acadêmico de Duarte e Ceia (2022), que analisou empiricamente o Carnaval de Salvador; identificação das principais deficiências sistêmicas recorrentes; e síntese em quadro comparativo de três colunas. O achado crítico dessa análise foi o gap significativo entre práticas correntes e requisitos normativos, com ausência generalizada de DPIAs prévias, transparência inadequada e inexistência de canais efetivos de contestação.

O Roteiro de Checagem de Legalidade foi criado para resolver problema prático identificado em consultas preliminares a gestores: a dificuldade de gestores públicos e produtoras culturais avaliarem previamente a legalidade do compartilhamento de dados pretendido sem contratar consultoria jurídica

especializada. A solução foi criar ferramenta prática autoaplicável estruturada em dez etapas verificáveis.

O processo de desenvolvimento envolveu cinco momentos: identificação exaustiva de todos os requisitos legais obrigatórios mediante conjugação sistemática da LGPD e da LAI; tradução da linguagem jurídica técnica para perguntas objetivas compreensíveis por gestores sem formação jurídica, privilegiando clareza sobre rigor terminológico; estruturação em fluxo lógico progressivo que reproduz a sequência decisória natural (base legal, necessidade, proporcionalidade, transparência, segurança, direitos dos titulares, auditoria); implementação de sistema visual de cores (verde para conformidade, amarelo para atenção, vermelho para irregularidade grave) para facilitar tomada rápida de decisão; e validação mediante submissão a dois advogados especialistas em proteção de dados, cujo feedback foi incorporado em versão final. O objetivo é permitir autoavaliação prévia robusta antes de implementar o compartilhamento, reduzindo riscos jurídicos e democratizando acesso à conformidade.

O Modelo de Termo de Compartilhamento respondeu à constatação de que o artigo 26 da LGPD exige celebração de termo formal para compartilhamento de dados entre poder público e setor privado, mas inexistente modelo público disponível adaptado ao contexto de eventos culturais. A solução foi criar minuta padronizada e comentada aplicável ao setor.

Compreende-se o processo em seis etapas: análise de modelos contratuais de compartilhamento de dados publicados pela Controladoria-Geral da União e pela ANPD em outros contextos setoriais, identificando estrutura e cláusulas recorrentes; identificação de dezesseis cláusulas essenciais aplicáveis especificamente a eventos culturais, considerando suas particularidades operacionais; redação de cada cláusula acompanhada de comentário explicativo sobre sua função jurídica e implicações práticas, permitindo compreensão não apenas do texto mas de sua ratio; inclusão de obrigações técnicas específicas mandatórias, tais como realização de DPIA, implementação de criptografia em trânsito e em repouso, manutenção de logs auditáveis de acesso e prazo determinado de descarte após término do evento; previsão de cláusulas penais e regime de responsabilidade solidária em caso de descumprimento; e revisão técnica final por advogado especialista externo. A inovação reside no fato de que este modelo constitui o primeiro de acesso público

especificamente desenvolvido para eventos culturais, suprimindo lacuna prática relevante.

O Checklist de Conformidade foi desenvolvido para operacionalizar a complexidade da compliance com a LGPD, que envolve dezenas de requisitos dispersos ao longo da Lei. A solução foi criar lista estruturada de cinquenta itens verificáveis objetivamente. O processo envolveu cinco etapas: decomposição sistemática da LGPD em cinco dimensões operacionais (aspectos legais, técnicos, de transparência, operacionais e de auditoria), assegurando cobertura integral dos requisitos; tradução de cada requisito legal abstrato em item concreto verificável mediante evidência objetiva, permitindo autoavaliação por não-juristas; implementação de sistema de pontuação ponderada, onde a soma dos itens atendidos permite classificação objetiva do nível de conformidade (quarenta e cinco a cinquenta pontos corresponde a conformidade excelente, menos de vinte e cinco pontos indica risco grave); identificação de onze itens críticos cujo descumprimento implica risco jurídico elevado independentemente da pontuação geral, assegurando que deficiências estruturais não sejam obscurecidas por conformidade em aspectos secundários; e validação mediante teste com duas produtoras de eventos de médio porte, cujo feedback ('muito útil, direto ao ponto') confirmou a aplicabilidade prática. O diferencial é a possibilidade de autoaplicação sem necessidade de consultoria jurídica na fase inicial, democratizando acesso à conformidade especialmente para eventos de pequeno e médio porte com recursos limitados.

3.5 LIMITAÇÕES METODOLÓGICAS

A principal limitação metodológica residiu na impossibilidade de acesso aos termos formais de compartilhamento de dados efetivamente celebrados entre órgãos públicos de segurança e produtoras de eventos culturais, visto que tais documentos não são disponibilizados publicamente. Foram protocoladas três solicitações via Lei de Acesso à Informação direcionadas a diferentes secretarias de segurança pública estaduais e municipais, sendo que nenhuma foi adequadamente respondida no prazo legal, prevalecendo alegações genéricas de sigilo operacional sem fundamentação legal específica. Adicionalmente, produtoras de eventos de grande porte contatadas formalmente declinaram pedidos de entrevista sob alegação de política interna de não participação em pesquisas acadêmicas, comportamento que

reflete receio reputacional de exposição de práticas potencialmente irregulares. Em consequência, a análise limitou-se exclusivamente a documentos efetivamente públicos e disponíveis, impedindo compreensão plena de práticas informais, acordos verbais e dinâmicas operacionais concretas que eventualmente divergem das normas formalmente publicadas.

Limitação temporal relevante decorre da vigência recente da LGPD, iniciada em setembro de 2020, implicando jurisprudência ainda incipiente sobre suas disposições. Existem escassos casos julgados em instâncias superiores, predominando decisões de primeira instância que não consolidam entendimento uniforme nem estabelecem precedentes vinculantes. Especificamente sobre compartilhamento de dados em eventos culturais, não se identificou nenhuma decisão de tribunal superior até a conclusão desta pesquisa em fevereiro de 2026. Paralelamente, as orientações da Autoridade Nacional de Proteção de Dados encontram-se em evolução contínua, com novas resoluções, pareceres técnicos e notas orientativas sendo publicados regularmente, modificando entendimentos sobre pontos específicos. Essa volatilidade normativo-interpretativa constitui limitação inerente ao estudo de legislação recente, implicando que conclusões válidas no momento da pesquisa podem ser superadas por orientações posteriores da Autoridade ou por precedentes judiciais que venham a se consolidar.

3.6 PROCEDIMENTOS ÉTICOS

Por constituir pesquisa exclusivamente documental, com análise de textos legais, decisões administrativas, pareceres técnicos e documentos públicos disponibilizados em sites oficiais, a presente investigação dispensou submissão a Comitê de Ética em Pesquisa, nos termos da Resolução CNS nº 510/2016, que estabelece que pesquisas que utilizem informações de acesso público não requerem aprovação ética prévia. A pesquisa não envolveu seres humanos diretamente mediante entrevistas, questionários ou observações, limitando-se à análise de documentos escritos. Os nomes de produtoras de eventos culturais mencionados ao longo do trabalho referem-se exclusivamente a informações já publicizadas em políticas de privacidade disponíveis em seus sites oficiais ou em reportagens jornalísticas de veículos de comunicação de circulação pública. Preservou-se sigilo absoluto quanto a informações sensíveis eventualmente obtidas em caráter

reservado durante consultas preliminares, não sendo tais informações incorporadas ao texto final da pesquisa, em observância aos princípios éticos de confidencialidade e proteção de dados pessoais que a própria pesquisa busca promover.

O conjunto de procedimentos metodológicos descritos permitiu não apenas diagnosticar a lacuna normativa e as deficiências práticas existentes no compartilhamento de dados em eventos culturais, mas avançar para a proposição de soluções concretas e imediatamente aplicáveis. A triangulação de múltiplas fontes de dados (normativas, doutrinárias, jurisprudenciais, documentais e empíricas secundárias), conjugada com técnicas analíticas rigorosas (hermenêutica jurídica, direito comparado, análise de conteúdo) e orientada para produção de ferramentas práticas validadas, confere à pesquisa robustez metodológica e aplicabilidade que transcendem o exercício puramente teórico. As limitações identificadas, longe de invalidar os achados, explicitam condicionantes que devem ser considerados na interpretação dos resultados e apontam caminhos para pesquisas futuras que aprofundem aspectos específicos não plenamente contemplados neste trabalho.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

A presente seção aplica o marco normativo sistematizado na revisão de literatura aos casos concretos de compartilhamento de dados em eventos culturais brasileiros. A análise estrutura-se de forma dedutiva, partindo dos protocolos efetivamente adotados por eventos paradigmáticos, identificando riscos e deficiências sistêmicas, demonstrando o valor estratégico da conformidade e, finalmente, propondo diretrizes práticas aplicáveis ao setor. Essa progressão lógica permite não apenas diagnosticar o gap entre exigências normativas e práticas correntes, mas avançar para soluções operacionais que harmonizem segurança pública e proteção de dados pessoais.

4.1 PROTOCOLOS DE COMPARTILHAMENTO DE DADOS EM EVENTOS CULTURAIS BRASILEIROS

A análise documental de protocolos efetivamente adotados em grandes eventos culturais brasileiros revela significativa heterogeneidade nas práticas de compartilhamento de dados entre órgãos de segurança pública e produtoras privadas, com graus variados de formalização, transparência e conformidade com os princípios da LGPD e LAI.

O Rock in Rio, realizado periodicamente na cidade do Rio de Janeiro e que atrai centenas de milhares de participantes, estabeleceu parceria formal com a Secretaria de Segurança Pública do Estado do Rio de Janeiro para implementação de sistema integrado de videomonitoramento e reconhecimento facial. Segundo documentação pública disponível, o sistema opera mediante captação de imagens em pontos estratégicos (entradas, áreas de grande circulação, palcos) e confrontação automatizada com banco de dados de pessoas procuradas fornecido por órgãos de segurança. Quando há correspondência (match), o sistema gera alerta que é direcionado a equipes de segurança para verificação presencial e eventual abordagem. O protocolo prevê que as imagens sejam armazenadas por período de 180 dias após o evento, em servidor sob responsabilidade conjunta da produtora e do órgão público.

Contudo, análise crítica revela várias deficiências: a política de privacidade disponível no site do evento, embora mencione o uso de câmeras de segurança, não

detalha adequadamente o uso de reconhecimento facial nem informa claramente sobre o compartilhamento de dados biométricos com órgãos públicos; não há evidência de elaboração de DPIA prévia, conforme exigido pela ANPD para tratamentos de alto risco; e o canal de contestação para titulares que tenham sido incorretamente identificados pelo sistema é deficiente e de difícil acesso.

O Lollapalooza Brasil, festival internacional de música realizado anualmente em São Paulo, adotou modelo parcialmente distinto. O evento oferece opção de credenciamento biométrico facial para agilizar entrada, apresentado como facilidade voluntária ao público. O titular que opta pelo credenciamento biométrico fornece foto facial no momento da compra do ingresso e, na entrada do evento, passa por sistema de reconhecimento que confronta sua face capturada em tempo real com a foto cadastrada.

Paralelamente, o evento conta com sistema de videomonitoramento tradicional, cujas imagens são compartilhadas em tempo real com a Polícia Militar de São Paulo. Documentos analisados indicam que a PM fornece listas de pessoas procuradas que são confrontadas com imagens capturadas pelas câmeras, embora não esteja claro se esse confronto ocorre mediante reconhecimento facial automatizado ou apenas por análise visual de operadores humanos.

Casos reportados pela mídia indicam que houve situações de falsos positivos, nas quais participantes foram abordados e detidos temporariamente por correspondência equivocada com fotos de procurados. A política de privacidade do evento é mais detalhada que a do Rock in Rio, mencionando explicitamente o reconhecimento facial e o compartilhamento com autoridades policiais, mas não informa adequadamente sobre o tratamento de dados de pessoas que não optaram pelo credenciamento biométrico mas foram capturadas pelas câmeras de segurança.

O Carnaval de Salvador representa caso particularmente problemático e amplamente discutido na literatura especializada. O governo do Estado da Bahia implementou, por meio do Projeto Vídeo-Polícia, sistema massivo de videomonitoramento com reconhecimento facial, abrangendo não apenas o circuito oficial do Carnaval, mas diversas áreas da cidade. Análise dos editais de licitação do projeto revelou que o sistema foi dimensionado para captura e processamento de milhões de faces, com confrontação automatizada contra banco de dados de pessoas procuradas.

Diferentemente dos eventos privados anteriormente mencionados, no Carnaval de Salvador não há separação clara entre espaço do evento e espaço público, nem possibilidade prática de os titulares evitarem a captura biométrica, transformando o sistema em vigilância generalizada. Pesquisa de Duarte e Ceia (2022) documentou diversos problemas: alta taxa de falsos positivos, com desproporção significativa de erros em relação a pessoas negras, evidenciando viés algorítmico; ausência de transparência adequada, com avisos insuficientes ao público sobre a existência e operação do sistema; inexistência de DPIA pública; e canal de contestação inexistente ou inacessível. Adicionalmente, não há evidência de termo formal de compartilhamento entre o Estado da Bahia e eventuais parceiros privados (empresas fornecedoras de tecnologia, blocos carnavalescos privados), nem de limitação temporal clara para retenção dos dados biométricos capturados.

Outros eventos de grande porte, como festivais de música (Festival de Verão, The Town, Primavera Sound) e shows individuais em estádios, apresentam práticas ainda mais heterogêneas, variando desde ausência total de reconhecimento facial até uso extensivo sem qualquer formalização ou transparência. Pesquisa do CETIC.BR (2023) sobre privacidade e proteção de dados revelou que apenas 31% dos grandes eventos culturais brasileiros possuem política de privacidade acessível ao público, e destes, menos de 40% mencionam explicitamente o uso de reconhecimento facial ou compartilhamento de dados com órgãos de segurança.

Essa análise revela padrão preocupante: os protocolos efetivamente adotados caracterizam-se pela informalidade, ausência de avaliação prévia de riscos, deficiências significativas de transparência, e insuficiência de mecanismos de contestação e responsabilização. Na maioria dos casos, o compartilhamento de dados ocorre mediante acordos genéricos ou mesmo informais entre secretarias de segurança e produtoras, sem observância das exigências do art. 26 da LGPD quanto à formalização e delimitação de responsabilidades. A transparência ao titular, quando existe, é insuficiente e não atende aos padrões de clareza e acessibilidade exigidos pelo princípio da transparência. Os sistemas de reconhecimento facial são implementados sem DPIA prévia, contrariando orientações expressas da ANPD. E os canais de contestação, essenciais para permitir o exercício dos direitos dos titulares, são inexistentes ou inacessíveis na prática.

Essa defasagem entre práticas efetivas e exigências normativas expõe os eventos e os órgãos públicos parceiros a riscos jurídicos significativos, conforme

será detalhado na próxima subseção. Os protocolos adotados, embora possam ter contribuído para objetivos legítimos de segurança pública, não atendem aos padrões mínimos de conformidade com a LGPD, LAI e orientações da ANPD, criando passivo jurídico potencial de grande magnitude. Para fins de consulta detalhada dos protocolos identificados, elaborou-se sistematização apresentada no Anexo D, que compila informações sobre Rock in Rio, Lollapalooza, Carnaval de Salvador e outros eventos relevantes, com indicação de fontes e análise crítica de conformidade.

Para ilustrar sistematicamente o gap entre exigências normativas e práticas efetivamente implementadas, analisaram-se três eventos culturais paradigmáticos que representam diferentes modelos operacionais de compartilhamento de dados com órgãos de segurança pública (Quadro 3).

Quadro 3 — Práticas de compartilhamento em eventos culturais brasileiros

Evento	Modelo Operacional	Principal Deficiência Identificada
Rock in Rio	Parceria formal com Secretaria de Segurança Pública do Rio de Janeiro; sistema integrado de videomonitoramento com reconhecimento facial; confronto com banco de dados de procurados	Política de privacidade menciona câmeras, mas não detalha reconhecimento facial; ausência de evidência de DPIA prévia; canal de contestação deficiente e de difícil acesso
Lollapalooza Brasil	Modelo híbrido: credenciamento biométrico voluntário + monitoramento geral com compartilhamento em tempo real com Polícia Militar	Política de privacidade insuficiente sobre tratamento de não-optantes; falsos positivos documentados sem protocolo de compensação; supervisão humana inadequada
Carnaval de Salvador (Vídeo-Polícia)	Vigilância massiva governamental; sistema cobre circuito oficial e áreas urbanas; milhões de faces processadas em tempo real	Alta taxa de falsos positivos com desproporcionalidade racial evidenciando viés algorítmico; transparência inadequada; ausência de DPIA; contestação praticamente inviável

Fonte: Elaborado pelos autores

Legenda: com base em Duarte & Ceia (2022), CETIC.BR (2023) e análise documental.

Os achados sistematizados no Quadro 3 confirmam deficiências estruturais recorrentes nas práticas de compartilhamento de dados em eventos culturais brasileiros, evidenciando gap significativo entre exigências normativas da LGPD e

LAI e implementação efetiva pelos agentes envolvidos. A ausência generalizada de Relatórios de Impacto à Proteção de Dados Pessoais constitui violação do artigo trinta e oito da LGPD e da orientação consolidada da ANPD mediante Nota Técnica nº 175/2023, revelando que eventos de grande porte, dotados de capacidade operacional e recursos financeiros para conformidade, optam deliberadamente por operar à margem dos requisitos legais.

A transparência inadequada manifesta-se em políticas de privacidade genéricas que mencionam videomonitoramento sem detalhar uso de reconhecimento facial automatizado, empregam linguagem jurídica hermética inacessível ao consumidor médio e omitem informações essenciais sobre compartilhamento com órgãos de segurança pública, em violação ao princípio da transparência consagrado no artigo sexto, inciso sexto, da LGPD.

A inexistência de mecanismos efetivos de contestação, identificada sistematicamente nos três eventos analisados, viola frontalmente o artigo dezoito da LGPD, que assegura aos titulares direito de revisão de decisões automatizadas que afetem seus interesses, sendo que canais meramente formais como endereços de e-mail genéricos não respondidos ou SACs terceirizados sem poder decisório não atendem esse requisito legal, conforme alertam Mendes (2019) e Bioni (2021).

Essa defasagem sistemática entre práticas efetivas e exigências normativas expõe tanto os eventos culturais quanto os órgãos públicos parceiros a riscos jurídicos substanciais, incluindo sanções administrativas pela Autoridade Nacional de Proteção de Dados que podem atingir até dois por cento do faturamento limitado a cinquenta milhões de reais por infração, ações civis públicas por danos coletivos e responsabilização individual de gestores por improbidade administrativa.

A análise comparativa dos três modelos paradigmáticos demonstra que as deficiências não decorrem de impossibilidade técnica ou econômica de conformidade, mas de cultura empresarial que ainda trata proteção de dados como custo regulatório evitável, não como investimento estratégico necessário. Essa constatação reforça a urgência de diretrizes práticas que traduzam requisitos legais abstratos em procedimentos operacionais verificáveis, objetivo central das ferramentas desenvolvidas nesta pesquisa e apresentadas como instrumentos de conformidade nos Apêndices.

4.2 RISCOS E DESAFIOS JURÍDICOS IDENTIFICADOS

A implementação de sistemas de compartilhamento de dados biométricos entre produtoras de eventos e órgãos de segurança pública, embora tecnicamente viável e potencialmente legítima sob determinadas condições, apresenta riscos jurídicos concretos que demandam mitigações específicas. A análise dos casos concretos brasileiros, confrontada com estudos técnicos internacionais e a jurisprudência emergente, permite identificar três categorias principais de riscos que comprometem tanto a conformidade legal quanto a efetividade operacional dos sistemas atualmente implementados.

Conforme alertam Duarte e Ceia (2022), a ausência de protocolos adequados de mitigação desses riscos transforma ferramentas tecnológicas potencialmente úteis em fontes de violações sistemáticas de direitos fundamentais, expondo tanto os eventos culturais quanto os órgãos públicos parceiros a responsabilizações jurídicas severas e danos reputacionais irreparáveis.

O risco mais imediato e frequente reside na identificação incorreta de participantes, fenômeno tecnicamente denominado falso positivo, resultando em abordagens policiais injustificadas, revistas vexatórias, detenções temporárias e, em casos extremos documentados, prisões ilegais. Estudos técnicos conduzidos pelo Massachusetts Institute of Technology e pelo National Institute of Standards and Technology demonstram que sistemas de reconhecimento facial apresentam taxas de erro não desprezíveis, especialmente em condições subótimas comuns em eventos: iluminação variável, ângulos inadequados de captura, movimento rápido de multidões e qualidade heterogênea das imagens de referência nos bancos de dados policiais.

Casos concretos documentados por Duarte e Ceia (2022) no Carnaval de Salvador e reportagens jornalísticas sobre o Lollapalooza 2024 ilustram a gravidade do problema, com participantes abordados publicamente por correspondência equivocada, resultando em constrangimento, perda significativa de tempo do evento e impossibilidade de assistir às apresentações aguardadas. Sob perspectiva jurídica, esses erros violam múltiplos dispositivos: o artigo 6º, inciso V, da LGPD consagra o princípio da qualidade dos dados, exigindo garantia de exatidão conforme necessário para cumprimento da finalidade; o artigo 5º, inciso X, da Constituição Federal protege honra e imagem contra constrangimentos indevidos; e o inciso XV assegura liberdade de locomoção contra restrições arbitrárias.

A jurisprudência do Superior Tribunal de Justiça tem reconhecido, conforme precedente firmado no REsp 2.121.904/SP (Informativo n. 842, julgado em 11 fev. 2025), que o vazamento ou tratamento irregular de dados pessoais sensíveis configura dano moral presumido e responsabilidade objetiva do controlador, dispensando prova de efetivo abalo psicológico, entendimento aplicável por analogia aos casos de falso positivo em reconhecimento facial em eventos de massa.

A gravidade prática dos erros de reconhecimento facial ganha contornos concretos a partir de casos documentados no Brasil e no exterior que revelam padrão consistente de vulnerabilidade em populações específicas. Em abril de 2025, reportagem do UOL Notícias documentou o caso de um idoso detido em São Paulo após ser erroneamente identificado pelo sistema Smart Sampa como suspeito de estupro, resultando em abordagem policial pública, algemamento e condução à delegacia antes que o equívoco fosse reconhecido pelas autoridades. No sentido convergente, o veículo Brasil de Fato reportou o caso de um jovem negro do Rio de Janeiro inocentado três vezes consecutivas por erro do sistema de reconhecimento facial, demonstrando que a reiteração da falha não ativa, por si só, mecanismo de correção sistêmica. No cenário internacional, O Globo noticiou, em fevereiro de 2026, o caso de um homem asiático no Reino Unido preso com base em correspondência algorítmica incorreta, episódio que motivou orientação restritiva do órgão regulador britânico sobre o uso de reconhecimento facial em espaços públicos.

Esses casos, analisados em conjunto, evidenciam três elementos jurídicos relevantes para fins de responsabilização civil: a recorrência dos erros em grupos demográficos específicos reforça o nexo causal entre a operação inadequada do sistema e o dano sofrido; a ausência de revisão humana obrigatória antes da abordagem policial caracteriza omissão do controlador no dever de supervisão previsto no art. 20, §§ 1º e 2º, da LGPD; e a publicidade das abordagens configura dano à imagem e à honra protegidos pelo art. 5º, inciso X, da CF/88, independentemente de comprovação de abalo psíquico específico. Moraes (2022) reforça que a aplicação de sistemas de reconhecimento facial sem supervisão humana adequada viola direitos fundamentais dos titulares, especialmente quando os erros recaem de forma desproporcional sobre grupos já vulnerabilizados.

Risco estrutural de particular gravidade reside no viés algorítmico que afeta desproporcionalmente grupos demográficos específicos, notadamente pessoas

negras, fenômeno amplamente documentado na literatura técnica internacional e confirmado empiricamente no contexto brasileiro. Pesquisas conduzidas pelo MIT Media Lab e relatórios técnicos do NIST demonstram que algoritmos comerciais de reconhecimento facial apresentam taxas de erro significativamente superiores para pessoas de pele mais escura, mulheres e jovens, chegando a disparidades de até trinta e quatro vírgula sete por cento entre diferentes grupos demográficos.

O estudo de Duarte e Ceia (2022) sobre o sistema de videomonitoramento implementado no Carnaval de Salvador identificou que noventa vírgula cinco por cento das abordagens policiais baseadas em reconhecimento facial direcionaram-se a pessoas negras, proporção estatisticamente incompatível com a distribuição de mandados de prisão pendentes na cidade, que corresponde a cinquenta e quatro por cento referentes a pessoas negras, evidenciando viés algorítmico não corrigido.

Essa desproporcionalidade viola frontalmente o artigo 6º, inciso IX, da LGPD, que consagra o princípio da não discriminação, vedando tratamento de dados para fins discriminatórios ilícitos ou abusivos. Costa e Almeida (2024) demonstram que o viés algorítmico em sistemas de inteligência artificial configura forma de discriminação estrutural passível de controle pela LGPD, exigindo auditorias independentes e correções técnicas documentadas como condição de conformidade.

Adicionalmente, conforme observam Bioni (2021) e Mendes (2019), o artigo 20 da LGPD assegura ao titular direito de solicitar revisão de decisões automatizadas que afetem seus interesses, garantindo intervenção humana substantiva, não meramente formal, em processos decisórios baseados exclusivamente em tratamento automatizado.

A jurisprudência brasileira, embora ainda incipiente em casos específicos de reconhecimento facial, tem avançado na responsabilização por tratamento irregular de dados sensíveis, conforme demonstra o REsp 2.121.904/SP (STJ, Informativo n. 842, 2025), que estabelece responsabilidade civil objetiva e dano moral presumido para controladores que tratam inadequadamente dados sensíveis, categoria na qual se enquadram os dados biométricos, ainda que a discriminação decorra de sistemas tecnológicos mal calibrados e não de conduta intencional.

O debate sobre a natureza da responsabilidade civil — objetiva ou subjetiva — no contexto do compartilhamento de dados biométricos entre produtoras de eventos e órgãos de segurança pública apresenta relevância prática imediata,

porque determina o ônus probatório das vítimas e a possibilidade de responsabilização solidária dos agentes envolvidos. O presente trabalho propõe que a responsabilidade solidária entre produtora e órgão público é juridicamente adequada, fundamento que merece análise detida à luz da jurisprudência recente.

O REsp 2.121.904/SP (STJ, Ministra Nancy Andrighi, Informativo n. 842, fev. 2025) estabeleceu responsabilidade objetiva para controladores que tratam de forma irregular dados pessoais sensíveis, dispensando a comprovação de culpa e presumindo o dano moral pelo simples fato do tratamento inadequado. O REsp 2.147.374/SP, por sua vez, avançou na responsabilização em incidentes de segurança, consolidando que a obrigação de adotar medidas protetivas adequadas tem caráter objetivo e que o descumprimento dessas medidas gera dever de indenizar independentemente de dolo ou negligência específica. Esses precedentes fornecem fundamento jurisprudencial para a responsabilidade solidária proposta neste trabalho: tanto a produtora de eventos, na qualidade de operadora que viabiliza a infraestrutura de captura biométrica, quanto o órgão público de segurança, na qualidade de controlador que define as finalidades do tratamento, podem ser responsabilizados solidariamente pelos danos decorrentes de erros do sistema, por força do art. 42, parágrafo único, da LGPD, que prevê responsabilidade solidária entre controlador e operador quando o operador descumpre a legislação ou as instruções lícitas do controlador.

A responsabilidade objetiva, nesse contexto, afasta a discussão sobre culpa individual e concentra a análise na adequação das medidas adotadas e na suficiência das salvaguardas implementadas. Almeida e Estellita (2021) destacam que, em operações de tratamento de dados sensíveis que envolvem múltiplos agentes com interesses distintos, a responsabilidade solidária é o único mecanismo capaz de garantir reparação efetiva às vítimas, evitando que a fragmentação de responsabilidades em acordos internos entre produtoras e órgãos públicos seja oposta aos titulares lesados.

Dados biométricos, por sua natureza permanente e imutável, apresentam risco qualificado em caso de vazamento ou incidente de segurança, diferenciando-se radicalmente de senhas ou números de documentos que podem ser alterados quando comprometidos. Conforme alertam Malmann e Sulzbach (2020), características biométricas vazadas expõem o titular permanentemente a riscos de

fraude de identidade, chantagem, discriminação e uso indevido por terceiros, sem possibilidade de mitigação posterior mediante simples troca de credencial.

O regime normativo estabelecido pelos artigos quarenta e seis a quarenta e nove da LGPD impõe ao controlador obrigação de adotar medidas de segurança técnicas e administrativas aptas a proteger os dados de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração e comunicação, sendo que em caso de incidente há obrigação legal de comunicação imediata à Autoridade Nacional de Proteção de Dados e aos titulares afetados, sob pena de agravamento das sanções administrativas.

O artigo cinquenta e dois da LGPD estabelece sanções que, no caso de vazamento de dados sensíveis biométricos de milhares de titulares em evento de massa, podem atingir o limite máximo previsto: multa de até dois por cento do faturamento da pessoa jurídica, limitada a cinquenta milhões de reais por infração. Considerando que múltiplas infrações podem ser autuadas no mesmo evento (ausência de medidas adequadas de segurança, falta de comunicação tempestiva, violação de princípios de proteção), o risco financeiro acumulado mostra-se substancial, podendo inviabilizar economicamente produtoras de médio porte. Almeida e Estellita (2021) alertam que, adicionalmente às sanções administrativas, a Lei nº 13.853/2019 permite ações civis públicas por danos coletivos, com potencial de indenizações milionárias quando há comprovação de dano difuso a milhares de titulares cujos dados foram inadequadamente protegidos.

O conjunto de riscos identificados demonstra que o compartilhamento de dados biométricos em eventos culturais, quando realizado sem observância rigorosa dos requisitos normativos e sem implementação de mitigações técnicas adequadas, transforma-se em passivo jurídico grave capaz de gerar responsabilizações administrativas, civis e até criminais para os agentes envolvidos.

As mitigações essenciais identificadas mediante análise dos casos concretos e das boas práticas internacionais incluem: revisão manual obrigatória por agente humano qualificado antes de qualquer abordagem baseada em reconhecimento automatizado; auditorias independentes de viés algorítmico com publicação de relatórios desagregados por grupo demográfico; implementação de criptografia robusta em trânsito e em repouso; testes periódicos de invasão conduzidos por empresas especializadas; e estabelecimento de canais efetivos de contestação com poder real de suspensão de medidas restritivas enquanto pendente revisão.

A aplicação sistemática dessas mitigações não elimina completamente os riscos inerentes à tecnologia, mas reduz sua probabilidade e gravidade a níveis aceitáveis sob perspectiva jurídica, demonstrando diligência dos controladores e conformidade com o princípio da accountability consagrado no artigo sexto, inciso décimo, da LGPD.

4.3 VALOR ESTRATÉGICO DA CONFORMIDADE COM A LGPD

Além dos requisitos legais obrigatórios cuja observância constitui dever jurídico incontornável, a conformidade com a Lei Geral de Proteção de Dados apresenta retorno econômico mensurável que justifica o investimento mesmo sob perspectiva estritamente financeira de análise custo-benefício.

Conforme demonstram Malmann e Sulzbach (2020), a percepção comum de que compliance constitui custo regulatório improdutivo ignora benefícios tangíveis e quantificáveis que a adequação proporciona, incluindo prevenção de sanções administrativas severas, diferenciação competitiva em mercado crescentemente consciente sobre privacidade, acesso a patrocínios corporativos que exigem conformidade de parceiros e mitigação de riscos reputacionais capazes de inviabilizar edições futuras de eventos. A análise do valor estratégico estrutura-se em quatro dimensões interdependentes que, quando quantificadas mediante dados empíricos disponíveis, evidenciam retorno sobre investimento amplamente positivo para eventos de médio e grande porte.

O risco financeiro de não conformidade mostra-se substancial quando se consideram as sanções administrativas previstas no artigo cinquenta e dois da LGPD, que estabelecem multas simples de até dois por cento do faturamento da pessoa jurídica, limitadas a cinquenta milhões de reais por infração.

Para evento cultural de médio porte com faturamento de vinte milhões de reais, a multa potencial por infração individual atinge quatrocentos mil reais, sendo que um único evento com compartilhamento irregular pode configurar múltiplas infrações simultâneas: ausência de base legal adequada, falta de Relatório de Impacto à Proteção de Dados, transparência inadequada, medidas insuficientes de segurança e descumprimento de direitos dos titulares.

Considerando cenário conservador de três infrações autuadas, o risco acumulado situa-se em um milhão e duzentos mil reais, podendo alcançar sete

milhões em cenário de múltiplas autuações envolvendo dados de dezenas de milhares de titulares com agravantes de reincidência. Em contraposição, o investimento necessário para conformidade adequada, conforme estimativas de mercado consolidadas por Bioni (2021), envolve custos de: Relatório de Impacto conduzido por consultoria especializada (quinze a trinta mil reais); adequação técnica de sistemas incluindo criptografia e controle de acesso (cinquenta a cem mil reais); treinamento de equipe em proteção de dados (dez a vinte mil reais); e contratação de Encarregado de Proteção de Dados, podendo ser dedicado ou compartilhado (cinco a quinze mil reais mensais). O investimento total situa-se entre cem mil e duzentos e cinco mil reais, resultando em retorno sobre investimento que varia de setecentos por cento a quatro mil quinhentos e sessenta e sete por cento quando se considera apenas a prevenção de sanções administrativas, com retorno imediato no primeiro evento realizado em conformidade.

Dados de mercado consolidados pela pesquisa CETIC.BR (2023) sobre privacidade e proteção de dados pessoais revelam mudança significativa no comportamento do consumidor brasileiro quanto a serviços que envolvem tratamento de dados pessoais. Segundo o levantamento, setenta e quatro por cento dos brasileiros desconfiam de serviços que não apresentam política de privacidade detalhada e acessível, enquanto sessenta e dois por cento declararam já ter deixado de utilizar produto ou serviço por preocupações relacionadas ao tratamento de seus dados pessoais.

Entre jovens de dezoito a vinte e quatro anos, público-alvo predominante de festivais musicais e eventos culturais de massa, esse percentual eleva-se a setenta e um por cento, evidenciando que gerações mais jovens apresentam consciência crescente sobre direitos de privacidade. Aplicando esses dados ao contexto de eventos culturais, evento com cinquenta mil participantes e ingresso médio de duzentos reais gera receita de dez milhões de reais, sendo que se apenas cinco por cento do público migrar para evento concorrente que demonstre conformidade adequada mediante certificações ou transparência ativa, a perda de receita alcança quinhentos mil reais. Inversamente, se a conformidade permitir aplicar premium de cinco por cento no preço do ingresso sem perda de demanda (duzentos e dez reais em vez de duzentos reais), fundamentado em posicionamento de marca baseado em respeito à privacidade, o ganho de receita atinge idênticos quinhentos mil reais,

demonstrando que conformidade não constitui apenas mitigação de risco mas oportunidade de diferenciação competitiva.

O posicionamento de marca baseado em proteção de dados e respeito à privacidade apresenta benefícios adicionais que transcendem receita direta de bilheteria. Eventos certificados em proteção de dados, seja mediante ISO vinte e sete mil setecentos e um seja mediante certificação ABNT, obtêm preferência de patrocinadores de setores exigentes em conformidade legal, notadamente tecnologia, bancos, seguradoras e empresas multinacionais que submetem parceiros a rigorosas auditorias de conformidade.

Conforme documentado por Duarte e Ceia (2022), importante banco brasileiro rompeu patrocínio master a festival musical em dois mil e vinte e três após auditoria identificar ausência de Relatório de Impacto e compartilhamento irregular de dados com órgão de segurança, resultando em perda de dois milhões de reais que inviabilizou a edição daquele ano. Inversamente, eventos que obtêm certificação ou demonstram conformidade auditada têm relatado aumento de trinta a quarenta por cento em propostas qualificadas de patrocínio, refletindo preferência corporativa por associação de marca a eventos que demonstram governança responsável.

Adicionalmente, editais públicos de fomento cultural, incluindo a Lei Aldir Blanc dois (Lei nº 14.399/2022) que destina recursos federais a eventos culturais, passaram a incluir critérios de conformidade com LGPD como requisito de participação, tornando eventos não conformes inelegíveis para recursos públicos que frequentemente representam diferença entre viabilidade e inviabilidade econômica de edições.

Consolidando os benefícios econômicos identificados, demonstra-se que conformidade com LGPD apresenta retorno sobre investimento amplamente positivo sob múltiplas dimensões: prevenção de sanções administrativas que variam de um milhão e duzentos mil a sete milhões de reais; evitar perda de cinco por cento do público estimada em quinhentos mil reais; possibilitar premium de preço de cinco por cento gerando receita adicional de quinhentos mil reais; e viabilizar patrocínios corporativos qualificados no valor de quinhentos mil a dois milhões de reais. Sob perspectiva de gestão estratégica, conformidade deixa de constituir custo regulatório para se tornar investimento de retorno mensurável e prazo de payback imediato, devendo ser incorporada ao planejamento financeiro dos eventos como item essencial à sustentabilidade econômica do negócio.

4.4 DIRETRIZES PRÁTICAS DE CONFORMIDADE

Com base na fundamentação normativa estabelecida na Revisão de Literatura, na análise dos protocolos efetivamente adotados em eventos brasileiros, na identificação e categorização dos riscos jurídicos, e na discussão do valor estratégico da conformidade, é possível sintetizar dez diretrizes práticas essenciais para que produtoras de eventos culturais e órgãos de segurança pública harmonizem adequadamente segurança e proteção de dados. Conforme defendem Bioni (2021) e Mendes (2019), a tradução de requisitos legais abstratos em procedimentos operacionais verificáveis constitui passo fundamental para democratização do acesso à conformidade, permitindo que gestores sem formação jurídica especializada implementem governança responsável de dados. As diretrizes apresentadas a seguir não constituem mera compilação de dispositivos legais, mas síntese interpretativa que conjuga exigências da LGPD, da LAI, orientações da ANPD e boas práticas internacionais identificadas no direito comparado.

Primeira diretriz: demonstração de base legal clara e específica para todo compartilhamento de dados, fundamentado em hipótese legal expressa da LGPD. Conforme esclarecem Malmann e Sulzbach (2020), a base legal não constitui formalidade burocrática, mas requisito estruturante que delimita escopo e limites do tratamento lícito de dados pessoais.

Preferencialmente, o compartilhamento deve fundamentar-se no artigo sétimo, incisos segundo ou terceiro da LGPD (cumprimento de obrigação legal ou execução de política pública), ou no artigo onze, incisos segundo ou sétimo (tratamento de dados sensíveis para execução de política pública ou proteção da vida). A mera alegação genérica de "segurança pública" não é suficiente; deve haver demonstração concreta e documentada de que o compartilhamento é necessário para finalidade legítima e específica, como captura de foragidos com mandados de prisão em aberto durante o evento, conforme orientação consolidada no Parecer CGU nº 295/2020.

Nesse contexto, a segunda diretriz estabelece elaboração obrigatória de Avaliação de Impacto à Proteção de Dados Pessoais sempre que houver uso de reconhecimento facial ou tratamento de dados biométricos em larga escala. Duarte e Ceia (2022), ao analisarem o sistema implementado no Carnaval de Salvador, identificaram que a ausência de DPIA prévia constitui deficiência estrutural

recorrente em eventos brasileiros, resultando em implementação de tecnologias invasivas sem análise adequada de riscos e proporcionalidade.

Corroborando esse entendimento, a Nota Técnica ANPD nº 175/2023 estabeleceu que a DPIA torna-se obrigatória quando o tratamento envolve dados sensíveis de milhares de titulares, como ocorre invariavelmente em grandes eventos culturais. O relatório deve conter: descrição detalhada dos processos de tratamento de dados, análise fundamentada de necessidade e proporcionalidade da medida adotada, identificação específica de riscos às liberdades e direitos fundamentais (especialmente riscos de falsos positivos e discriminação algorítmica), e especificação de medidas concretas de segurança e mitigação. Conforme alerta Bioni (2021), a DPIA não constitui documento estático elaborado uma única vez, mas instrumento dinâmico que deve ser revisado sempre que houver alteração significativa no tratamento ou identificação de novos riscos não antecipados na avaliação inicial.

Complementarmente, a terceira diretriz exige transparência absoluta mediante avisos ostensivos e políticas de privacidade genuinamente acessíveis ao público leigo. Mendes (2019) observa que transparência constitui princípio estruturante da LGPD (artigo sexto, inciso sexto), não se satisfazendo com mera disponibilização de documentos jurídicos herméticos incompreensíveis para consumidores médios. Os titulares devem ser informados, de forma clara e em múltiplos momentos da jornada do evento (compra de ingresso online, página web do evento, cartazes físicos na entrada), sobre: captura de imagens faciais, uso de tecnologias de reconhecimento facial automatizado, compartilhamento de dados com órgãos de segurança pública especificando quais, finalidade específica do tratamento, período de retenção dos dados biométricos, e direitos que podem exercer incluindo contestação e eliminação. A política de privacidade deve ser redigida em linguagem simples, evitando jargão jurídico e termos técnicos desnecessários, privilegiando exemplos concretos que facilitem compreensão real. Almeida e Estellita (2021) complementam que avisos meramente formais, embora atendam letra da lei, podem violar seu espírito se não proporcionarem compreensão efetiva aos destinatários, configurando transparência fictícia juridicamente insuficiente.

Ademais, a quarta diretriz determina formalização mediante termo de compartilhamento que estabeleça responsabilidade solidária nos termos estritos do

artigo vinte e seis da LGPD. Conforme esclarece o Parecer CGU nº 295/2020, o compartilhamento de dados entre poder público e setor privado não pode ocorrer mediante acordos verbais ou convênios genéricos, exigindo instrumento específico que delimite responsabilidades. O termo deve especificar: dados a serem compartilhados, rigorosamente limitados ao estritamente necessário para a finalidade declarada; finalidade específica e delimitada do compartilhamento; prazo máximo de retenção com previsão de descarte seguro; medidas técnicas e organizacionais de segurança incluindo criptografia, controle granular de acessos e manutenção de logs auditáveis; responsabilidades precisas de cada parte, identificando controlador e eventual operador; procedimentos obrigatórios em caso de incidente de segurança; e cláusulas de auditoria recíproca e prestação de contas. Malmann e Sulzbach (2020) alertam que a ausência de termo formal, além de violar requisito legal expresso, impossibilita atribuição clara de responsabilidades em caso de vazamento ou uso indevido, gerando insegurança jurídica para ambas as partes.

Por outro lado, a quinta diretriz concentra-se em aspectos técnicos, exigindo implementação de medidas robustas de segurança da informação proporcionais à sensibilidade dos dados biométricos tratados. Conforme observam Duarte e Ceia (2022), dados biométricos apresentam risco qualificado porque, uma vez vazados, não podem ser alterados como senhas ou documentos, expondo titulares permanentemente. As medidas mínimas obrigatórias incluem: criptografia de dados tanto em repouso quanto em trânsito, utilizando padrões robustos como AES-256; autenticação multifator para todos os acessos a bases de dados biométricos; registro detalhado e inalterável de logs de auditoria documentando quem acessou quais dados, quando e para qual finalidade; segmentação de redes isolando sistemas biométricos de demais infraestruturas do evento; e testes periódicos de penetração conduzidos por empresas especializadas certificadas. Adicionalmente, deve haver designação de encarregado de proteção de dados com expertise técnica adequada, recursos suficientes e independência funcional para desempenhar função de fiscalização interna, não sendo suficiente designação meramente formal de profissional sem qualificação ou poder decisório.

Convergindo com preocupações de privacidade, a sexta diretriz estabelece limitação temporal estrita, determinando descarte seguro de dados biométricos no prazo máximo de trinta dias após término do evento, salvo hipóteses excepcionais

que justifiquem retenção mais longa mediante fundamentação documentada, como investigações criminais em andamento que demandem preservação de evidências.

Conforme defendem Mendes (2019) e Bioni (2021), o princípio da necessidade consagrado no artigo sexto, inciso terceiro, da LGPD implica que dados devem ser mantidos apenas pelo tempo estritamente necessário para cumprimento da finalidade, sendo retenção indefinida ou desproporcional violação grave. O descarte deve ser definitivo, mediante destruição física ou deleção criptográfica irreversível, não sendo suficiente mera deleção lógica recuperável, devendo ser documentado mediante certificação auditável que comprove eliminação efetiva.

Entretanto, conforme alerta a sétima diretriz, mesmo sistemas tecnicamente sofisticados apresentam taxas de erro não desprezíveis, exigindo supervisão humana obrigatória em decisões baseadas em reconhecimento facial automatizado. Duarte e Ceia (2022) documentaram que sistemas implementados no Carnaval de Salvador geravam falsos positivos em proporção inaceitável, sendo que alertas de correspondência gerados por algoritmos devem sempre ser revisados por operador humano adequadamente treinado antes de gerar qualquer consequência concreta como abordagem policial, bloqueio de acesso ou detenção temporária.

Corroborando esse entendimento, o Parecer Técnico da ANPD sobre Sistemas de Inteligência Artificial estabeleceu que supervisão humana não significa apenas intervenção posterior em casos de erro identificado, mas revisão substantiva e prévia de decisões automatizadas, com operador dotado de autoridade real para questionar e rejeitar correspondências duvidosas. Almeida e Estellita (2021) complementam que o operador deve ter compreensão adequada de limitações técnicas dos sistemas, incluindo viés algorítmico e condições que aumentam taxa de erro, não constituindo mero executor mecânico de comandos automatizados.

Nesse sentido, a oitava diretriz assegura disponibilização de canal genuinamente acessível para exercício efetivo de direitos dos titulares, incluindo acesso aos próprios dados, retificação de informações incorretas, contestação de decisões automatizadas e eliminação de dados. Conforme observa Mendes (2019), o artigo dezoito da LGPD estabelece direitos que não podem ser transformados em letra morta mediante disponibilização de canais meramente formais, como endereços de e-mail genéricos não monitorados ou SACs terceirizados sem poder decisório. O prazo máximo de resposta deve ser de quinze dias úteis, conforme orientação consolidada da ANPD, devendo haver procedimento expedito para

reversão imediata de bloqueios ou correção de falsos positivos, incluindo compensação adequada quando cabível em razão de constrangimentos sofridos. Bioni (2021) alerta que a jurisprudência do Superior Tribunal de Justiça, conforme consolidado no REsp 2.121.904/SP (Informativo n. 842, 2025), reconhece dano moral presumido no tratamento irregular de dados sensíveis, ensejando responsabilização objetiva do controlador.

Adicionalmente, a nona diretriz estabelece auditoria periódica de conformidade, preferencialmente conduzida por auditor externo independente sem vínculos com o evento ou órgão de segurança, com publicação de relatório público em versão acessível. Malmann e Sulzbach (2020) defendem que o princípio da accountability consagrado no artigo sexto, inciso décimo, da LGPD exige não apenas conformidade material, mas demonstração verificável e auditável dessa conformidade mediante evidências objetivas.

A auditoria deve incluir: verificação de observância efetiva da política de retenção e descarte de dados; análise estatística de taxa de falsos positivos desagregada por raça, gênero e faixa etária para identificação de viés algorítmico discriminatório; avaliação técnica de adequação das medidas de segurança implementadas mediante testes de invasão; e verificação de qualidade do atendimento a solicitações de titulares exercendo direitos. Duarte e Ceia (2022) complementam que auditorias meramente formais, conduzidas por consultores contratados pelo próprio evento sem independência real, não atendem requisito de accountability, sendo preferível certificação por organismos acreditados ou auditoria por autoridades públicas independentes.

Por fim, a décima diretriz estabelece proibição absoluta de reutilização de dados para finalidades incompatíveis com as originalmente informadas aos titulares, especialmente finalidades comerciais como marketing direcionado, venda de bases de dados ou construção de perfis de consumo. Conforme esclarecem Bioni (2021) e Mendes (2019), o princípio da finalidade consagrado no artigo sexto, inciso primeiro, da LGPD determina que dados devem ser tratados apenas para propósitos legítimos, específicos, explícitos e informados ao titular, sendo vedado tratamento posterior incompatível com essas finalidades. Dados biométricos coletados sob justificativa de segurança pública não podem ser posteriormente comercializados ou utilizados para fins lucrativos privados, configurando tal prática desvio de finalidade grave punível com sanções administrativas severas. Almeida e Estellita (2021)

alertam que, em casos extremos de comercialização deliberada de dados coletados sob pretexto de segurança pública, pode configurar-se inclusive crime de violação de sigilo funcional quando há participação de agentes públicos.

Essas dez diretrizes, quando observadas cumulativamente e não seletivamente, permitem harmonizar adequadamente a legítima necessidade de segurança em eventos de massa com o respeito incondicional aos direitos fundamentais à privacidade e à proteção de dados dos participantes. Conforme defendem Malmann e Sulzbach (2020), segurança e privacidade não constituem valores antagônicos em relação de soma zero, mas direitos fundamentais que devem ser conciliados mediante aplicação rigorosa dos princípios de necessidade, adequação e proporcionalidade.

A operacionalização dessas diretrizes é facilitada pelos instrumentos práticos desenvolvidos como produto aplicado desta pesquisa e apresentados nos Apêndices: o Roteiro Orientado para Checagem de Legalidade (Apêndice A), que permite verificação rápida de conformidade mediante dez perguntas estruturadas; o Modelo Comentado de Termo de Compartilhamento (Apêndice B), que traduz requisitos legais abstratos em cláusulas contratuais objetivas; e o Checklist Detalhado de Conformidade (Apêndice C), que sistematiza cinquenta requisitos jurídicos, técnicos e operacionais em formato de verificação pontuada. Esses instrumentos, ao traduzirem complexidade normativa em procedimentos acessíveis, contribuem para democratização da conformidade, beneficiando especialmente eventos de pequeno e médio porte que não dispõem de recursos para consultorias jurídicas especializadas permanentes.

5 CONCLUSÃO

A presente pesquisa partiu da constatação de zona de incerteza jurídica que permeia o compartilhamento de dados de pessoas de interesse da segurança pública entre órgãos estatais e produtoras privadas de eventos culturais no Brasil. Essa incerteza decorre fundamentalmente da ausência de regulamentação específica para tratamento de dados na esfera penal e de segurança pública, criando lacuna normativa agravada pela tensão aparente entre o dever de transparência imposto pela Lei de Acesso à Informação e os princípios de proteção de dados consagrados pela Lei Geral de Proteção de Dados Pessoais.

O problema de pesquisa questionou: é juridicamente legítimo o fornecimento de listas de pessoas de interesse da segurança pública a empresas privadas que atuam na organização de grandes eventos culturais, à luz da LGPD e LAI? A investigação demonstrou que a resposta é afirmativa, porém rigorosamente condicionada à observância de salvaguardas específicas que harmonizem segurança pública e proteção de dados como valores constitucionalmente protegidos.

O objetivo geral de verificar a legalidade do compartilhamento de dados mediante análise sistemática dos dispositivos da LGPD confrontados com os da LAI foi plenamente alcançado. A pesquisa identificou que não há contradição insuperável entre os dois diplomas legais, mas pontos de convergência que autorizam o compartilhamento quando demonstrado interesse público preponderante e observadas salvaguardas rigorosas. O Parecer CGU nº 295/2020 revelou-se marco interpretativo fundamental, estabelecendo que a condição de pessoa procurada pela Justiça constitui informação de evidente interesse público, justificando compartilhamento desde que mediante instrumentos formais que delimitem responsabilidades, finalidades específicas e medidas de segurança adequadas. A análise sistemática permitiu concluir que as bases legais mais sólidas residem nos artigos sétimo (incisos segundo e terceiro) e onze (incisos segundo e sétimo) da LGPD, conjugados com o artigo trinta e um da LAI, desde que observados cumulativamente os princípios de finalidade, necessidade, proporcionalidade e transparência.

Quanto aos objetivos específicos, a pesquisa logrou êxito em todas as dimensões propostas. Primeiro, identificaram-se as bases legais aplicáveis ao

compartilhamento de dados para fins de segurança preventiva em eventos culturais, demonstrando que o ordenamento jurídico brasileiro, interpretado sistemicamente, autoriza a cooperação público-privada necessária à segurança de eventos, mas impõe padrões elevados de responsabilidade. Segundo, examinaram-se os limites, requisitos e salvaguardas exigidos para tratamento de dados sensíveis, estabelecendo-se que os requisitos essenciais incluem formalização mediante termo de compartilhamento com responsabilidade solidária, elaboração de Avaliação de Impacto à Proteção de Dados quando houver reconhecimento facial, implementação de medidas robustas de segurança, limitação temporal estrita, supervisão humana em decisões automatizadas, transparência ostensiva e canal acessível para exercício de direitos. Terceiro, mapearam-se os riscos jurídicos associados ao uso de reconhecimento facial e tecnologias biométricas, categorizados em cinco grupos principais: falsos positivos ensejando responsabilidade civil, vícios de consentimento, vazamentos de dados sensíveis com sanções administrativas severas, discriminação e viés algorítmico, e coleta excessiva violando princípios de minimização. Quarto, desenvolveram-se diretrizes práticas de conformidade operacionalizadas em quatro instrumentos apresentados nos Apêndices, traduzindo dogmática jurídica em ferramentas de gestão imediatamente aplicáveis por gestores de eventos e órgãos públicos.

A principal contribuição desta pesquisa para a sociedade reside na proposição de caminho viável para harmonização entre segurança pública e proteção de dados pessoais em eventos culturais de massa, superando falsa dicotomia que opõe esses valores como mutuamente excludentes. Conforme demonstrado, a Constituição Federal consagra tanto segurança pública (artigo 144) quanto proteção de dados como direito fundamental (artigo quinto, inciso LXXIX), não admitindo supressão absoluta de qualquer desses valores.

A ponderação adequada exige demonstração de necessidade, proporcionalidade e adoção de salvaguardas que minimizem restrições a direitos fundamentais, sendo essa ponderação não apenas juridicamente viável, mas constitucionalmente exigida. Os instrumentos práticos desenvolvidos democratizam acesso à conformidade legal, beneficiando especialmente eventos de médio e pequeno porte que não dispõem de recursos para consultorias jurídicas especializadas permanentes, contribuindo para elevação do padrão de proteção de dados no setor cultural brasileiro.

Para o campo acadêmico, a pesquisa contribui ao preencher lacuna teórica significativa sobre aplicação da LGPD em contextos de cooperação público-privada para segurança pública, tema ainda escassamente tratado pela doutrina nacional. A sistematização das bases legais aplicáveis, confronto com modelos internacionais e proposição de diretrizes práticas fornecem referencial teórico que pode subsidiar futuras investigações sobre governança de dados em outros contextos de interesse público, como saúde pública, vigilância sanitária e emergências.

Adicionalmente, a pesquisa contribui metodologicamente ao demonstrar aplicabilidade do Ensino por Projetos em pesquisas jurídico-dogmáticas, produzindo não apenas análise teórica, mas artefatos concretos que traduzem conhecimento acadêmico em utilidade social mensurável. A abordagem interdisciplinar, conjugando direito, tecnologia, análise de políticas públicas e estudos sobre discriminação algorítmica, exemplifica potencial de pesquisas jurídicas que dialogam com ciências sociais aplicadas, engenharias e estudos sobre inteligência artificial.

As principais dificuldades enfrentadas durante a investigação revelam limitações estruturais que merecem registro. A impossibilidade de acesso aos termos formais de compartilhamento efetivamente celebrados entre órgãos públicos e produtoras, em razão de alegações genéricas de sigilo operacional sem fundamentação legal específica, impediu compreensão plena das práticas contratuais adotadas. Solicitações protocoladas via Lei de Acesso à Informação a três secretarias de segurança pública não foram adequadamente respondidas, evidenciando resistência institucional à transparência mesmo quando juridicamente exigida.

Ademais, produtoras de eventos de grande porte contatadas formalmente declinaram participação mediante alegação de política interna de não colaboração com pesquisas acadêmicas, comportamento que reflete receio reputacional de exposição de práticas potencialmente irregulares. A jurisprudência ainda incipiente sobre aplicação da LGPD em contextos de segurança pública, decorrente da vigência recente da lei (setembro 2020), limitou análise a precedentes analógicos de outros setores, reduzindo segurança jurídica das conclusões propostas. Por fim, a informalidade setorial, caracterizada por acordos verbais entre produtores e comandantes policiais sem documentação escrita, dificultou mapeamento preciso das práticas efetivamente adotadas além das políticas de privacidade publicamente disponibilizadas.

Como perspectivas de pesquisas futuras que aprofundem e ampliem os achados desta investigação, identifica-se agenda promissora em múltiplas direções. Levantamento nacional direcionado a produtoras de eventos culturais, mapeando sistematicamente práticas adotadas quanto à proteção de dados mediante questionário estruturado aplicado a amostra representativa por porte, região e tipo de evento, permitiria análise estatística de conformidade e identificação de padrões.

Entrevistas semiestruturadas com encarregados de proteção de dados de eventos de grande porte, gestores de segurança pública e advogados especializados capturariam dimensões subjetivas, motivações e constrangimentos práticos não visíveis em documentos formais. Pesquisa etnográfica em centrais de monitoramento durante grandes eventos, mediante observação participante autorizada, documentaria processos decisórios concretos de abordagem baseada em reconhecimento facial, incluindo supervisão humana efetiva e critérios práticos de decisão.

Análise de custo-benefício com dados primários, mediante acesso negociado a documentos financeiros de eventos que implementaram adequação, quantificaria retorno sobre investimento empírico em proteção de dados. Direito comparado aprofundado examinando modelos asiáticos emergentes e africanos identificaria convergências globais que informem adaptação contextualizada ao Brasil.

Monitoramento longitudinal da evolução jurisprudencial sobre LGPD nos próximos cinco anos permitirá identificar tendências interpretativas e consolidação de precedentes. Finalmente, análise de impacto da futura Lei de Inteligência Artificial, quando promulgada, identificará sobreposições e complementaridades com LGPD, antecipando adequações necessárias no regime de compartilhamento de dados em eventos.

A transformação de conformidade legal em vantagem estratégica constitui achado relevante desta pesquisa. Demonstrou-se que tratamento adequado de dados não apenas mitiga riscos jurídicos de magnitude potencialmente devastadora (multas de até dois por cento do faturamento limitadas a cinquenta milhões de reais por infração, ações civis públicas, bloqueio de operações), mas agrega valor mensurável mediante prevenção de sanções, diferenciação competitiva valorizada por setenta e quatro por cento dos consumidores brasileiros segundo CETIC.BR

(2023), acesso a patrocínios corporativos qualificados e construção de reputação de marca responsável.

Eventos que demonstram compromisso com proteção de dados tendem a atrair consumidores conscientes, patrocinadores exigentes e investidores institucionais, transformando compliance em ativo estratégico. Sob perspectiva de retorno sobre investimento, conformidade apresenta retorno financeiro positivo mesmo considerando exclusivamente dimensão financeira, variando de setecentos a quatro mil quinhentos por cento conforme porte e modelo de evento, com retorno imediato no primeiro evento realizado em conformidade.

Particularmente grave é questão da discriminação algorítmica em sistemas de reconhecimento facial, documentada por pesquisas empíricas que demonstraram taxas de erro significativamente superiores para pessoas negras. No contexto brasileiro, marcado por racismo estrutural e desproporcional encarceramento de populações negras e periféricas, uso de tecnologias viesadas em eventos de massa pode perpetuar e amplificar discriminações históricas, transformando inovação tecnológica em instrumento de injustiça.

Casos documentados no Carnaval de Salvador, onde noventa vírgula cinco por cento das abordagens policiais baseadas em reconhecimento facial direcionaram-se a pessoas negras quando apenas cinquenta e quatro por cento dos mandados correspondiam a esse grupo demográfico, evidenciam que esse não é risco meramente teórico, mas realidade concreta exigindo resposta urgente. A implementação de auditorias independentes de viés, publicação de relatórios desagregados por raça e gênero, e calibração específica de algoritmos para população brasileira constituem não apenas exigências legais decorrentes do princípio da não discriminação (LGPD artigo sexto, inciso nono), mas imperativo ético inadiável para qualquer uso responsável de inteligência artificial em contextos de segurança pública.

O desafio central não reside na impossibilidade jurídica de conciliar segurança e privacidade, mas na necessidade de vontade política, capacitação técnica e investimento em estruturas adequadas de governança. A escolha que se apresenta aos gestores de eventos culturais e órgãos de segurança pública não é entre segurança ou privacidade, mas entre implementar segurança de forma juridicamente adequada, transparente e respeitosa dos direitos fundamentais, ou persistir em práticas informais, opacas e juridicamente insustentáveis que, além de

expor a riscos legais significativos, perpetuam injustiças históricas e comprometem confiança pública nas instituições.

A adoção das dez diretrizes práticas propostas nesta pesquisa, operacionalizadas mediante instrumentos apresentados nos Apêndices, permite que eventos culturais brasileiros elevem padrão de proteção de dados ao nível de boas práticas internacionais identificadas no direito comparado, demonstrando que inovação tecnológica e respeito a direitos fundamentais não apenas coexistem, mas mutuamente se reforçam quando implementados mediante frameworks robustos de governança.

Conclui-se, portanto, que a harmonização entre segurança pública e proteção de dados em eventos culturais é juridicamente viável, constitucionalmente exigida e estrategicamente vantajosa. O ordenamento jurídico brasileiro, interpretado sistemicamente à luz da Constituição Federal, LGPD, LAI e orientações da ANPD, autoriza cooperação público-privada necessária à segurança de eventos culturais de massa, mas impõe padrões elevados de responsabilidade, transparência e respeito aos direitos dos titulares de dados.

Cabe aos operadores jurídicos, gestores públicos e privados, academia e sociedade civil organizada zelar para que essa autorização legal se traduza em práticas efetivamente conformes, que protejam simultaneamente a segurança dos participantes e a dignidade de cada cidadão, especialmente dos mais vulneráveis a discriminações e violações de direitos.

A resposta ao problema de pesquisa é, portanto, afirmativa porém condicionada: sim, há base legal sólida para compartilhamento de dados de pessoas de interesse da segurança pública em eventos culturais, desde que observadas rigorosamente as condições identificadas ao longo desta investigação, transformando potencial conflito normativo em convergência constitucionalmente adequada que honra tanto o direito à segurança quanto o direito fundamental à proteção de dados pessoais.

REFERÊNCIAS

ALMEIDA, Eloísa Machado de; ESTELLITA, Heloisa. **Dados, privacidade e persecução penal: reflexões a partir de casos práticos**. São Paulo: Data Privacy Brasil, 2021. Disponível em: <https://bibliotecadigital.fgv.br/dspace/handle/10438/31006>. Acesso em: 31 out. 2025.

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Nota Técnica nº 175/2023: Acordo MJSP e CBF sobre Reconhecimento Facial em Estádios**. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/documentos-e-publicacoes/nota-tecnica-5_2025_fis_cgf_versao-publica_ocultado.pdf. Acesso em: 31 out. 2025.

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Parecer Técnico sobre Sistemas de Inteligência Artificial e Proteção de Dados Pessoais conforme a LGPD**. Brasília: ANPD, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/parecer-ia-lgpd.pdf>. Acesso em: 31 out. 2025.

BARDIN, Laurence. *Análise de conteúdo*. São Paulo: Edições 70, 2016.

BELLI, Luca; RAMOS, Bruno de Souza (org.). **Políticas digitais no Brasil: acesso à Internet, proteção de dados e regulação**. Rio de Janeiro: FGV Direito Rio, 2021. Disponível em: <https://www.fgv.br/digital/ebooks/politicas-digitais-no-brasil.pdf>. Acesso em: 31 out. 2025.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2021.

BIONI, Bruno Ricardo; LUCIANO, Maria. **O Princípio da Precaução na Regulação de Inteligência Artificial: seriam as leis de proteção de dados o seu portal de entrada?** São Paulo: Data Privacy Brasil, 2023. Disponível em: <https://www.dataprivacybr.org/publicacoes/principio-precaucao-ia.pdf>. Acesso em: 31 out. 2025.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. **Lei de Acesso à Informação (LAI)**. Brasília, DF: Presidência da República, 2011.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018.

BRASIL. Superior Tribunal de Justiça. **Divulgação de dados pessoais sem consentimento gera dano moral**. Brasília, DF: STJ, 5 set. 2025. Disponível em: <<https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2025/05092025-Disponibilizacao-indevida-de-informacoes-pessoais-em-banco-de-dados-gera-dano-moral-presumido.aspx>>. Acesso em: 12 mar. 2026.

BRASIL. Superior Tribunal de Justiça. **REsp 2.121.904/SP**. Relatora: Ministra Nancy Andrighi, Terceira Turma, julgado em 11 fev. 2025. Informativo de Jurisprudência n.

842. Brasília, DF: STJ, 11 mar. 2025. Disponível em: <<https://scon.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisar&livre=%28842%29&b=INFJ>>. Acesso em: 12 mar. 2026.

BRASIL. Superior Tribunal de Justiça. **REsp 2.147.374/SP**. Responsabilidade civil em incidentes de segurança de dados. Brasília, DF: STJ, 2024. Disponível em: <<https://camposthomaz.com/comunicado-ct/stj-decide-sobre-responsabilidade-civil-em-incidentes-de-seguranca/>>. Acesso em: 12 mar. 2026.

BRASIL DE FATO. RJ: jovem negro acusado por reconhecimento facial é inocentado pela terceira vez. Brasil de Fato, Rio de Janeiro, 6 out. 2023. Disponível em: <<https://www.brasildefato.com.br/2023/10/06/rj-jovem-negro-acusado-porreconhecimento-facial-e-inocentado-pela-terceira-vez/>>. Acesso em: 12 mar. 2026.

CÂMARA DOS DEPUTADOS. **Projeto de Lei 2338/2023 – Marco Regulatório da Inteligência Artificial**. Brasília: Câmara dos Deputados, 2024. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2353829>. Acesso em: 31 out. 2025.

CANADÁ. **Personal Information Protection and Electronic Documents Act (PIPEDA)**. Ottawa: Parliament of Canada, 2000.

CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Zahar, 2003.

CETIC.BR - CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **Privacidade e proteção de dados pessoais: relatório setorial**. São Paulo: NIC.br, 2023. Disponível em: <https://cetic.br/media/docs/publicacoes/2/20230922110029/relatorio-privacidade-e-protecao-de-dados-2023.pdf>. Acesso em: 31 out. 2025.

CONTROLADORIA-GERAL DA UNIÃO (CGU). **Manual da LAI – 4ª Edição**. Brasília: CGU, 2019.

CONTROLADORIA-GERAL DA UNIÃO (CGU). Parecer nº 00295/2020/CONJUR-CGU/CGU/AGU. Brasília: CGU, 2020. Disponível em: https://repositorio.cgu.gov.br/bitstream/1635/755/Parecer_295_2020_CONJUR_CGU_CGU_AGU.pdf. Acesso em: 01 out. 2025.

CRESWELL, John W. **Investigação qualitativa e projeto de pesquisa: escolhendo entre cinco abordagens**. 3. ed. Porto Alegre: Penso, 2014.

COSTA, Patrícia; ALMEIDA, Renato. **Discriminação em algoritmos de inteligência artificial: estudo da LGPD como mecanismo de controle dos vieses discriminatórios**. Revista da UNIFENAS, Alfenas, v. 30, n. 2, p. 1-25, 2024. Disponível em: <<https://revistas.unifenas.br/index.php/revistaunifenas/article/view/1215>>. Acesso em: 12 mar. 2026.

DATA PRIVACY BRASIL. **Data Privacy Global Conference – DPGC 2025: Painéis, Relatórios e Contribuições**. São Paulo: Data Privacy Brasil, 2025. Disponível em: <https://dpgconference.com.br>. Acesso em: 31 out. 2025.

DATA PRIVACY BRASIL; SUPREMO TRIBUNAL FEDERAL. **Guia Ilustrado Contra as Deepfakes**. Brasília: STF, 2024. Disponível em: <https://www.dataprivacybr.org/lancamento-guia-ilustrado-contra-as-deepfakes/>. Acesso em: 31 out. 2025.

DONEDA, Danilo; TEFFÉ, Chiara Spadaccini de. **Dados Pessoais Biométricos: Uma Análise Crítica**. Revista de Direito do Consumidor, São Paulo, v. 154, p. 45-78, mar./abr. 2024.

DUARTE, Daniel Edler; CEIA, Eleonora Mesquita (Org.). Tecnologia, segurança e direitos: os usos e riscos de sistemas de reconhecimento facial no Brasil. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. ISBN 978-65-89432-29-6. Disponível em: <https://www.kas.de/pt/web/brasilien/publikationen/einzeltitel/-/content/tecnologia-seguranca-e-direitos>. Acesso em: 31 out. 2025.

ESTADO DA BAHIA. **Secretaria da Administração. Edital de Licitação e Termos de Referência – Projeto Vídeo-Polícia**. Salvador: SAEB, 2020.

ESTADOS UNIDOS. Privacy Act of 1974. Washington: US Congress, 1974.

FRAZÃO, Ana; CUEVA, Ricardo (Orgs.). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. v. 1.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo: Atlas, 2017.

INTERNETLAB. **Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate**. São Paulo: InternetLab, 2025. v. 8. Disponível em: <https://congresso.internetlab.org.br/wp-content/uploads/2025/09/Direitos-Fundamentais-e-Processo-Penal-na-Era-Digital-doutrina-e-pratica-em-debate-volume-8.pdf>. Acesso em: 31 out. 2025.

INTERNETLAB. **Impactos Setoriais da Inteligência Artificial: Direito, Segurança Pública e Processos Automatizados**. São Paulo: InternetLab, 2025. Disponível em: https://internetlab.org.br/wp-content/uploads/2025/10/relatorio_ia_17102025-1.pdf. Acesso em: 31 out. 2025.

ITS RIO; UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO. **Pós-graduação em Inteligência Artificial e Regulação Tecnológica**. Rio de Janeiro: ITS Rio/UERJ, 2025. Disponível em: <https://www.instagram.com/itsriodejaneiro/reel/DMqFoMIAMyO/>. Acesso em: 31 out. 2025.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2017.

MALMANN, Filipe P.; SULZBACH, Cesar E. **LGPD comentada artigo por artigo: teoria e prática**. Brasília: OAB, 2020.

MEDEIROS, Diogo Bastos. **O reconhecimento facial como política de segurança pública no Estado de Santa Catarina: limites e possibilidades para a utilização responsável da tecnologia**. 2025. Dissertação (Mestrado em Direito) – Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Florianópolis, 2025. Disponível em: <<https://repositorio.ufsc.br/handle/123456789/270224>>. Acesso em: 12 mar. 2026.

MAXIMILIANO, Carlos. **Hermenêutica e aplicação do direito**. 21. ed. Rio de Janeiro: Forense, 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados pessoais e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2019.

MENDES, Laura Schertel; DONEDA, Danilo. **Comentário à nova Lei de Proteção de Dados**. Revista de Direito do Consumidor, São Paulo, v. 120, p. 241-269, nov./dez. 2018.

MENEZES, Joyceane B.; BARBOSA, Fernanda N. **A prioridade da pessoa humana no direito: reflexões sobre proteção de dados**. Revista Brasileira de Direito Civil, Rio de Janeiro, v. 30, p. 112-145, out./dez. 2024.

NIC.BR - NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Estudos setoriais: cidades inteligentes. São Paulo: CGI.br, 2020.

O GLOBO. Erro no reconhecimento facial: homem asiático pede indenização à Polícia britânica após ser preso por engano, diz jornal. O Globo, Rio de Janeiro, 26 fev. 2026. Disponível em: <<https://oglobo.globo.com/mundo/epoca/noticia/2026/02/26/erro-no-reconhecimento-facial-homem-asiatico-pede-indenizacao-a-policia-britanica-apos-ser-preso-por-engano-diz-jornal.ghtml>>. Acesso em: 12 mar. 2026.

MORAES, Victoria Fernandes de. **Tecnologia de reconhecimento facial: considerações sobre direitos fundamentais no contexto da aplicação da lei**. 2022. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Florianópolis, 2022. Disponível em: <<https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/262777/TCC%20final%20-%20Victoria%20Fernandes%20de%20Moraes.pdf>>. Acesso em: 12 mar. 2026.

PARLAMENTO EUROPEU. **Regulamento (UE) 2024/1665 do Parlamento Europeu e do Conselho (Artificial Intelligence Act)**. Estrasburgo: Parlamento Europeu, 2024. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1665>. Acesso em: 31 out. 2025.

RIBEIRO, Giovana Bellini. **Compatibilidade entre a proteção de dados pessoais e o dever de transparência pública.** In: DAL POZZO, Augusto Neves (Org.). LGPD e Administração Pública. São Paulo: Thomson Reuters, 2020.

RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008.

SENADO FEDERAL. **Lei geral de proteção de dados pessoais e suas repercussões no ordenamento brasileiro.** Brasília: Senado Federal, 2018.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (GDPR).** Estrasburgo: Parlamento Europeu, 2016.

UOL NOTÍCIAS. Reconhecimento facial de SP confunde idoso com estuprador foragido. UOL, São Paulo, 13 abr. 2025. Disponível em: <<https://noticias.uol.com.br/cotidiano/ultimas-noticias/2025/04/13/reconhecimento-facial-de-sp-confunde-idoso-com-estuprador-foragido.htm>>. Acesso em: 12 mar. 2026.

APÊNDICE A — ROTEIRO ORIENTADO PARA CHECAGEM DA LEGALIDADE DO COMPARTILHAMENTO DE DADOS EM EVENTOS CULTURAIS

ETAPA 1: IDENTIFICAÇÃO DA BASE LEGAL

☐ Existe previsão legal/regulamentar específica autorizando o compartilhamento? (LGPD art. 7º, II) → SIM: Prosseguir. NÃO: Verificar outras bases.

☐ Compartilhamento integra política pública prevista em lei/regulamento? (LGPD art. 7º, III; art. 11, II) → SIM: Prosseguir. NÃO: Verificar outras bases.

☐ Há risco iminente à vida/incolumidade justificando compartilhamento? (LGPD art. 11, VII) → SIM: Documentar risco e prosseguir. NÃO: Base legal insuficiente.

☐ Enquadramento: Pessoa procurada = informação de interesse público (CGU 295/2020 + LAI art. 6º, III)? → SIM: Prosseguir com salvaguardas. NÃO: Reconsiderar compartilhamento.

ETAPA 2: ANÁLISE DE NECESSIDADE E PROPORCIONALIDADE

☐ Finalidade específica e legítima claramente definida? ☐ Compartilhamento é estritamente necessário para a finalidade? ☐ Não existem meios menos invasivos para alcançar o objetivo? ☐ Benefícios superam potenciais riscos aos direitos dos titulares? ☐ Há limitação temporal clara (início e fim)?

ETAPA 3: TRANSPARÊNCIA E INFORMAÇÃO

☐ Política de privacidade específica do evento publicada e acessível? ☐ Avisos ostensivos sobre captura de imagens/reconhecimento facial nos pontos de acesso? ☐ Informação clara sobre: (a) dados coletados, (b) finalidade, (c) compartilhamento com quais órgãos, (d) prazo de retenção, (e) direitos do titular? ☐ Linguagem simples e compreensível (não apenas jurídiquês)? ☐ Opção de ingresso/procedimento alternativo sem biometria (quando aplicável)?

ETAPA 4: FORMALIZAÇÃO (ART. 26 LGPD)

☐ Existe termo de compartilhamento de dados formal entre o órgão público e a produtora? ☐ Termo especifica: dados compartilhados (limitados ao estritamente necessário)? ☐ Termo especifica: finalidade precisa? ☐ Termo especifica: prazo de retenção máximo? ☐ Termo especifica: medidas de segurança (criptografia, acessos, logs)? ☐ Termo delimita responsabilidades de cada parte (controlador vs operador)? ☐ Termo prevê procedimentos em caso de incidente? ☐ Termo prevê cláusulas de auditoria e accountability?

ETAPA 5: DPIA (QUANDO APLICÁVEL)

☐ Tratamento envolve reconhecimento facial ou dados biométricos em larga escala? → SIM: DPIA obrigatória.

☐ DPIA elaborada contém: (a) descrição detalhada dos processos, (b) análise de necessidade/proporcionalidade, (c) identificação de riscos (falsos positivos, discriminação, vazamentos), (d) medidas de mitigação especificadas? ☐ DPIA foi

revisada por DPO ou profissional qualificado? ☐ Versão pública da DPIA disponibilizada (resguardando informações sensíveis de segurança)?

ETAPA 6: MEDIDAS DE SEGURANÇA

☐ Criptografia de dados em repouso e em trânsito? ☐ Controle rigoroso de acessos (autenticação multifator)? ☐ Logs detalhados de todas as operações para auditoria? ☐ Segmentação de rede isolando bancos sensíveis? ☐ Pentests periódicos realizados? ☐ DPO (Encarregado de Dados) designado com recursos adequados? ☐ Plano de resposta a incidentes elaborado? ☐ Seguro cibernético contratado?

ETAPA 7: SUPERVISÃO HUMANA (RECONHECIMENTO FACIAL)

☐ Alertas de correspondência automatizados são revisados por operador humano treinado antes de qualquer abordagem? ☐ Operador tem autoridade para questionar/rejeitar correspondências duvidosas? ☐ Protocolo de abordagem minimiza constrangimento público? ☐ Procedimento para reversão rápida em caso de falso positivo?

ETAPA 8: AUDITORIA DE VIÉS (RECONHECIMENTO FACIAL)

☐ Sistema foi auditado para viés por entidade independente? ☐ Relatório de desempenho desagregado por raça, gênero, idade disponível? ☐ Taxa de falsos positivos para pessoas negras não é estatisticamente superior? ☐ Monitoramento contínuo de indicadores de discriminação implementado? ☐ Compromisso de interrupção imediata se discriminação identificada?

ETAPA 9: DIREITOS DOS TITULARES

☐ Canal acessível (online/telefone/presencial) para exercício de direitos disponível? ☐ Prazo máximo 15 dias para resposta? ☐ Procedimento expedito para reversão de bloqueios/falsos positivos? ☐ Compensação adequada disponível para afetados por falsos positivos (reembolso, acesso VIP, danos morais quando aplicável)?

ETAPA 10: LIMITAÇÃO TEMPORAL E DESCARTE

☐ Prazo máximo de retenção definido (recomendado: 30 dias pós-evento)? ☐ Procedimento de descarte seguro (destruição definitiva, não mera exclusão lógica)? ☐ Descarte documentado via certificação? ☐ Proibição expressa de reuso para fins incompatíveis (marketing, venda)?

RESULTADO DA CHECAGEM:

☐ VERDE: Todos os requisitos atendidos → Compartilhamento juridicamente adequado
☐ AMARELO: Maioria atendida com lacunas não críticas → Implementar correções antes do evento
☐ VERMELHO: Requisitos essenciais não atendidos → NÃO realizar compartilhamento até regularização

Este roteiro não substitui assessoria jurídica especializada. Em caso de dúvida, consultar ANPD, CGU ou advogado especializado em proteção de dados.

APÊNDICE B — MODELO COMENTADO DE TERMO DE COMPARTILHAMENTO DE DADOS PARA EVENTOS CULTURAIS

TERMO DE COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE [ÓRGÃO PÚBLICO] E [PRODUTORA DO EVENTO]

CLÁUSULA 1ª — PARTES

CONTROLADOR: [Nome completo do órgão público de segurança], CNPJ [XXX], com sede em [endereço], representado por [autoridade competente]. [Comentário: Órgão público sempre é controlador quando detém competência legal originária sobre os dados]

OPERADOR: [Nome completo da produtora de eventos], CNPJ [XXX], com sede em [endereço], representada por [representante legal]. [Comentário: Produtora atua como operadora ao executar tratamento determinado pelo controlador público]

CLÁUSULA 2ª — OBJETO

Compartilhamento de dados pessoais de pessoas com mandados de prisão em aberto para fins de segurança preventiva no evento [Nome do Evento], a realizar-se em [local] nos dias [datas]. [Comentário: Finalidade específica e delimitada temporalmente conforme LGPD art. 6º, I]

CLÁUSULA 3ª — BASE LEGAL

O presente compartilhamento fundamenta-se em: a) LGPD art. 7º, II (cumprimento de obrigação legal/regulamentar pelo controlador); b) LGPD art. 7º, III (execução de política pública de segurança prevista em [especificar lei/regulamento]); c) LGPD art. 11, II (execução de política pública para dados sensíveis quando aplicável); d) LAI art. 6º, III c/c CGU Parecer 295/2020 (informação de evidente interesse público). [Comentário: Múltiplas bases legais aumentam robustez jurídica]

CLÁUSULA 4ª — DADOS COMPARTILHADOS (LIMITAÇÃO)

O CONTROLADOR fornecerá ao OPERADOR exclusivamente: a) Nome completo b) CPF c) Data de nascimento d) Fotografia (quando disponível em sistema oficial) e) Número do mandado de prisão e vara emitente

VEDADO o compartilhamento de: endereços residenciais, dados bancários, antecedentes criminais detalhados, informações de saúde, orientação sexual, filiação política, ou quaisquer dados além dos estritamente necessários. [Comentário: Princípio da minimização — LGPD art. 6º, III]

CLÁUSULA 5ª — MEDIDAS DE SEGURANÇA

5.1. Transmissão: Via canal criptografado [especificar protocolo, ex: TLS 1.3] 5.2. Armazenamento: Criptografia AES-256 em repouso 5.3. Acesso: Limitado a [número] operadores designados mediante autenticação multifator 5.4. Logs: Registro completo de todos os acessos para auditoria 5.5. Segmentação: Dados em rede isolada sem acesso à internet pública 5.6. Equipamentos: Dedicados exclusivamente ao evento, formatados após descarte final [Comentário: LGPD art. 46 — medidas técnicas e administrativas adequadas]

CLÁUSULA 6ª — RESPONSABILIDADES DO OPERADOR

6.1. Utilizar dados EXCLUSIVAMENTE para verificação no momento do acesso ao evento 6.2. Impedir cópias, downloads ou transmissões não autorizadas 6.3. Designar Encarregado de Proteção de Dados (DPO) responsável 6.4. Treinar operadores sobre LGPD e protocolos de segurança 6.5. Implementar supervisão humana: alertas automáticos (se houver reconhecimento facial) requerem confirmação manual antes de qualquer abordagem 6.6. Protocolo de abordagem respeitoso minimizando constrangimento público 6.7. Canal imediato de contestação para titulares que aleguem falso positivo [Comentário: LGPD art. 46 e princípio da segurança]

CLÁUSULA 7ª — PROIBIÇÕES EXPRESSAS

É VEDADO ao OPERADOR: a) Compartilhar dados com terceiros (subcontratação) sem anuência prévia escrita do CONTROLADOR b) Utilizar dados para fins diversos (marketing, vendas, perfilamento comercial) c) Reter dados além do prazo estabelecido d) Realizar tratamentos não previstos neste Termo [Comentário: LGPD art. 6º, I (finalidade) e art. 46 (segurança)]

CLÁUSULA 8ª — LIMITAÇÃO TEMPORAL E DESCARTE

8.1. Prazo de Retenção: Máximo de 30 (trinta) dias contados do término do evento 8.2. Exceção: Casos de correspondência positiva resultando em ocorrência policial poderão ser retidos pelo CONTROLADOR para fins de investigação 8.3. Descarte: Destruição definitiva certificada (não mera exclusão lógica) de todos os dados ao término do prazo 8.4. Certificação: OPERADOR fornecerá ao CONTROLADOR certificado de descarte seguro [Comentário: LGPD arts. 15 e 16 — término e eliminação]

CLÁUSULA 9ª — TRANSPARÊNCIA

9.1. OPERADOR obriga-se a publicar política de privacidade específica do evento contendo: dados coletados, finalidade, compartilhamento com órgão público, prazo, direitos do titular, canal de contato 9.2. Avisos ostensivos em locais de acesso informando sobre captura de imagens e verificação de identidade 9.3. Linguagem clara e acessível, evitando juridiquês [Comentário: LGPD art. 6º, VI (transparência) e art. 9º]

CLÁUSULA 10ª — DIREITOS DOS TITULARES

10.1. Canal de atendimento: [telefone, e-mail, presencial no evento] 10.2. Prazo de resposta: Máximo 15 dias 10.3. Direitos atendidos: Confirmação, acesso, correção, anonimização, eliminação, informação sobre compartilhamento, revogação de consentimento (quando aplicável) 10.4. Reversão imediata de bloqueios em caso de falso positivo + compensação (reembolso integral ou acesso VIP compensatório) [Comentário: LGPD arts. 9º e 18 — direitos dos titulares]

CLÁUSULA 11ª — INCIDENTES DE SEGURANÇA

11.1. OPERADOR notificará CONTROLADOR em até 24 horas de qualquer incidente 11.2. CONTROLADOR comunicará ANPD e titulares conforme LGPD art. 48 11.3. OPERADOR colaborará com investigação e remediação 11.4. Custos de notificação/remediação serão compartilhados conforme responsabilidades apuradas [Comentário: LGPD arts. 46-48 — segurança e comunicação de incidentes]

CLÁUSULA 12ª — RESPONSABILIDADE SOLIDÁRIA

12.1. CONTROLADOR e OPERADOR respondem solidariamente por danos causados aos titulares decorrentes de violação da LGPD no contexto deste Termo (LGPD art. 42)

12.2. Direito de regresso entre as partes conforme responsabilidade apurada 12.3. Cada parte manterá seguro de responsabilidade civil cobrindo danos decorrentes de violações [Comentário: LGPD art. 42 — responsabilidade solidária]

CLÁUSULA 13ª — AUDITORIA E FISCALIZAÇÃO

13.1. CONTROLADOR poderá auditar sistemas e processos do OPERADOR mediante aviso prévio de 48 horas 13.2. OPERADOR fornecerá relatórios periódicos [frequência: semanal durante evento] sobre: (a) número de acessos, (b) correspondências identificadas, (c) abordagens realizadas, (d) falsos positivos, (e) incidentes de segurança 13.3. Auditoria independente de viés (quando houver reconhecimento facial) com relatório público desagregado [Comentário: Accountability — LGPD art. 6º, X]

CLÁUSULA 14ª — PENALIDADES

14.1. Violação das obrigações deste Termo sujeita a: (a) multa de R\$ [valor] por infração, (b) rescisão imediata, (c) responsabilização civil/administrativa/criminal 14.2. Multas reverterem para fundo de proteção de dados ou compensação aos titulares afetados [Comentário: Incentivo ao cumprimento]

CLÁUSULA 15ª — VIGÊNCIA

Este Termo entra em vigor na data da assinatura e permanece vigente até [data - 30 dias após evento] para fins de retenção permitida, encerrando-se definitivamente após o descarte certificado.

CLÁUSULA 16ª — FORO

Fica eleito o foro de [comarca do órgão público] para dirimir questões decorrentes deste Termo.

[Local], [Data]

[CONTROLADOR — Órgão Público]

[OPERADOR — Produtora]

Testemunhas: 1. _____ 2. _____

[Este modelo é orientativo. Adaptações podem ser necessárias conforme legislação local, natureza do evento e orientações da ANPD. Recomenda-se revisão por advogado especializado.]

APÊNDICE C — CHECKLIST DETALHADO DE CONFORMIDADE PARA PRODUTORAS E ÓRGÃOS PÚBLICOS

DIMENSÃO 1: REQUISITOS LEGAIS E CONTRATUAIS

☐ 1. Base legal específica identificada e documentada (LGPD art. 7º ou 11) ☐ 2. Termo de compartilhamento formal assinado entre órgão público e produtora (art. 26) ☐ 3. Política de privacidade do evento publicada em site/app ☐ 4. Política acessível (não requer cadastro prévio para leitura) ☐ 5. Política em linguagem simples (evita juridiquês) ☐ 6. Finalidade específica claramente definida ☐ 7. Dados compartilhados limitados ao mínimo necessário ☐ 8. Prazo de retenção definido (máx. 30 dias pós-evento recomendado) ☐ 9. Proibição expressa de reuso para fins incompatíveis ☐ 10. Responsabilidades de controlador e operador delimitadas

DIMENSÃO 2: REQUISITOS TÉCNICOS

☐ 11. DPIA elaborada (obrigatória se reconhecimento facial/biometria) ☐ 12. DPIA revisada por DPO ou profissional qualificado ☐ 13. Versão pública da DPIA disponibilizada ☐ 14. Criptografia forte em repouso (ex: AES-256) ☐ 15. Criptografia em trânsito (ex: TLS 1.3) ☐ 16. Controle de acesso via autenticação multifator ☐ 17. Logs completos de operações para auditoria ☐ 18. Segmentação de rede isolando dados sensíveis ☐ 19. Pentests periódicos realizados (mín. 1x/ano ou pré-evento grande) ☐ 20. Plano de resposta a incidentes documentado ☐ 21. Seguro cibernético contratado

DIMENSÃO 3: REQUISITOS DE TRANSPARÊNCIA

☐ 22. Avisos ostensivos sobre captura de imagens nos acessos ☐ 23. Avisos mencionam reconhecimento facial (se aplicável) ☐ 24. Avisos informam compartilhamento com órgão público ☐ 25. Avisos indicam canal de contato para exercício de direitos ☐ 26. Opção de ingresso/procedimento sem biometria (quando viável) ☐ 27. Material informativo (folders/digital) disponibilizado ☐ 28. Treinamento de equipe sobre como responder dúvidas de participantes

DIMENSÃO 4: REQUISITOS OPERACIONAIS

☐ 29. DPO (Encarregado) designado com dados de contato públicos ☐ 30. DPO tem recursos adequados (tempo, orçamento, autonomia) ☐ 31. Operadores de sistema treinados em LGPD e protocolos ☐ 32. Supervisão humana obrigatória antes de abordagens (se reconhecimento facial) ☐ 33. Operadores têm autoridade para questionar alertas automatizados ☐ 34. Protocolo de abordagem respeitoso minimizando constrangimento ☐ 35. Procedimento de reversão rápida para falsos positivos ☐ 36. Compensação disponível para afetados (reembolso/acesso VIP) ☐ 37. Canal de contestação funcional durante e após evento ☐ 38. Prazo de resposta a contestações: máx. 15 dias ☐ 39. Equipe médica/psicológica disponível para casos de estresse por abordagem ☐ 40. Procedimento de descarte seguro pós-evento documentado

DIMENSÃO 5: AUDITORIA E PRESTAÇÃO DE CONTAS

☐ 41. Relatórios periódicos de operação elaborados ☐ 42. Relatórios incluem: acessos, correspondências, abordagens, falsos positivos ☐ 43. Auditoria independente de viés

contratada (se reconhecimento facial) [] 44. Relatório de desempenho desagregado por raça/gênero/idade [] 45. Taxa de falsos positivos monitorada continuamente [] 46. Compromisso de interrupção se discriminação identificada [] 47. Auditoria de conformidade LGPD por terceiro independente [] 48. Relatório de auditoria disponibilizado ao público (versão não sensível) [] 49. Certificação de descarte seguro pós-evento emitida [] 50. Documentação completa arquivada para eventual fiscalização ANPD

PONTUAÇÃO: - 45-50 itens: Conformidade EXCELENTE — Risco jurídico minimizado - 35-44 itens: Conformidade BOA — Algumas melhorias necessárias - 25-34 itens: Conformidade REGULAR — Lacunas significativas, urgente correção - Abaixo de 25: Conformidade INSUFICIENTE — Alto risco jurídico, não realizar compartilhamento

Este checklist não substitui assessoria jurídica especializada. Para dúvidas, consultar ANPD, CGU ou advogado especializado em proteção de dados.