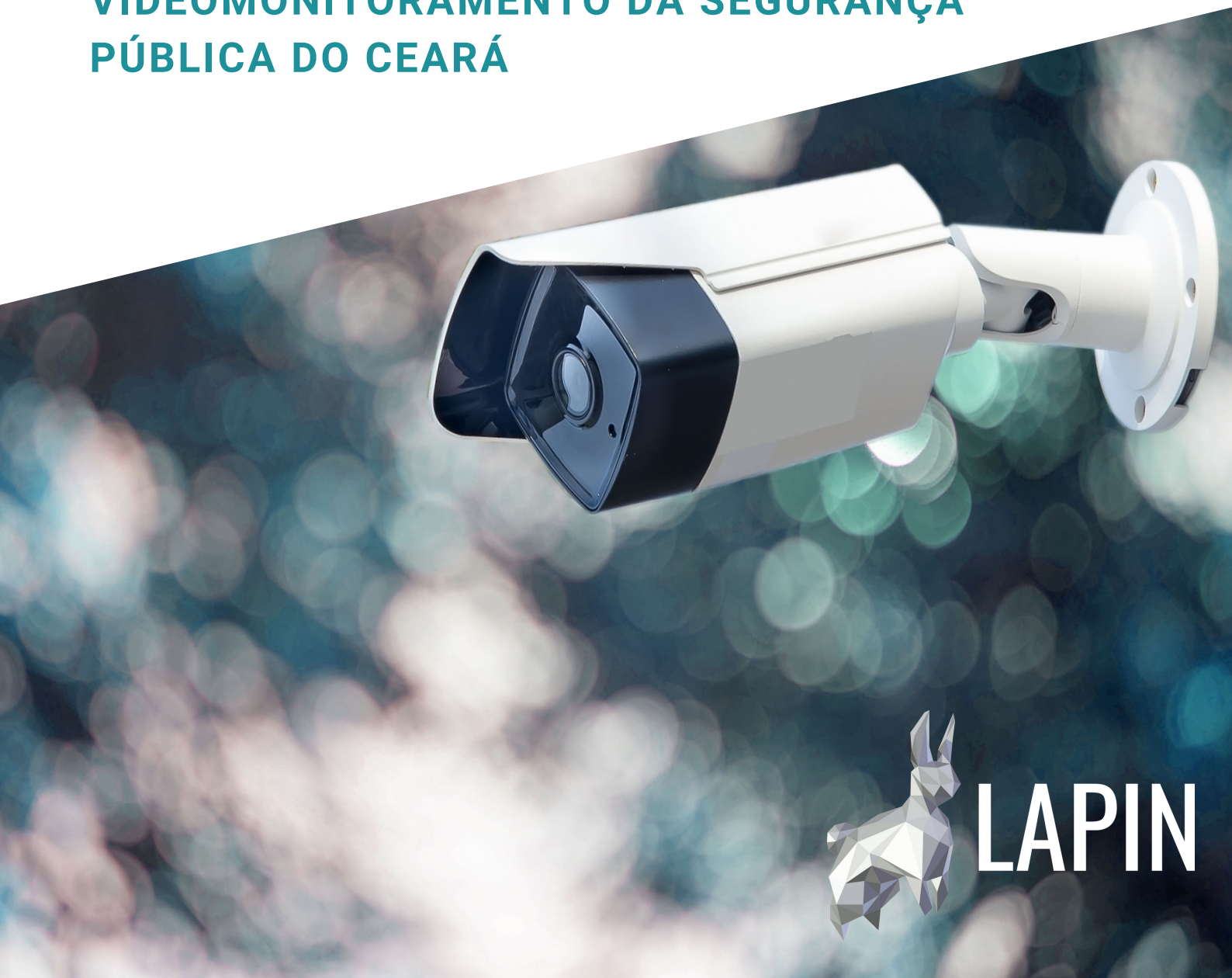
2020 | DEZEMBRO

NOTA TÉCNICA

PL Nº 42/2020

SOBRE O USO COMPARTILHADO DE IMAGENS DE CÂMERAS PRIVADAS COM O SISTEMA DE VIDEOMONITORAMENTO DA SEGURANÇA PÚBLICA DO CEARÁ



LAPIN

Realização:

Laboratório de Políticas Públicas e Internet - LAPIN

Autoria

Eduarda Costa Almeida

Felipe Rocha da Silva

Henrique Bawden Silverio de Castro

Revisão

Amanda Espiñeira

José Renato Laranjeira de Pereira

Imagem de Capa:

เฉลิมพล ศรีสังข์, Pixabay

LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

lapin.org.br
@lapin.br
/lapinbr
/lapinbr

Sobre esta nota técnica

Está em discussão na Assembléia Legislativa do Estado do Ceará o PL nº 42/2020, de autoria do Governo do Estado, que dispõe sobre o uso compartilhado, em tempo real, de imagens de câmeras privadas com o sistema de videomonitoramento da segurança pública do Ceará.

O Laboratório de Políticas Públicas e Internet - LAPIN elaborou esta nota técnica para apresentar suas considerações sobre o tema, trazendo reflexões sobre tópicos do PL que **afetam diretamente o exercício de direitos como privacidade e proteção de dados por indivíduos**.

Dentre estes tópicos, destacamos o uso de conceitos amplos e indeterminados que podem ser aproveitados para interesses alheios ao de segurança pública. Outro ponto de preocupação é a falta de adequação ao sistema principiológico e aos direitos dos titulares de dados presentes no quadro regulatório nacional de proteção de dados pessoais.

Neste documento, contrastamos o PL nº 42/2020 com a Lei Geral de Proteção de Dados (LGPD) e apresentamos perspectivas do Direito Europeu. O objetivo é aprofundar o debate sobre como o PL afeta a proteção de dados de indivíduos em território cearense, o que se faz necessário para garantir o respeito a direitos e liberdades fundamentais no Estado.

Quem somos nós

O Laboratório de Políticas Públicas e Internet (LAPIN) é um *think tank* de composição multidisciplinar com sede na capital federal brasileira. Seu objetivo é apoiar o desenvolvimento de políticas públicas voltadas para a regulação das tecnologias digitais por meio da pesquisa e da conscientização da sociedade.

SUMÁRIO

I - Introdução

O Projeto de Lei nº 42/2020, apresentado pelo Governo do Estado do Ceará à Assembleia Legislativa, "*dispõe sobre o uso compartilhado, em tempo real, com o sistema de videomonitoramento da segurança pública estadual de imagens de câmeras privadas captadas do ambiente externo a imóveis, públicos e privados, situados no estado do Ceará, e dá outras providências*" .

Nos últimos anos, têm se multiplicado as proposições legislativas que buscam regular o uso de tecnologias de videomonitoramento para os fins de segurança pública. A título de exemplo, menciona-se a Lei Distrital nº 6390/2019[1] aprovada pela Câmara Legislativa do Distrito Federal, o PL nº 391/2019[2] da Assembléia Legislativa de Minas Gerais e o PL nº 341/2019[3] da Assembleia Legislativa do Rio de Janeiro.

Em geral, o que há de comum entre esses atos normativos é a proposição de mecanismos de monitoramento constante de indivíduos, em alguns casos inclusive com o intuito de identificá-los automaticamente, como ocorre por meio de sistemas de reconhecimento facial. No entanto, tais obrigações têm sido criadas sem trazer consigo regras que permitam o uso da tecnologia em consonância com princípios e garantias previstos na LGPD, que possui uma incidência reflexa a normas que envolvam o tratamento de dados pessoais para fins de segurança pública.

---

[1] BRASIL. Lei Distrital nº 6390/2019: Cria o Programa Cidade Segura - PCS e dá outras providências. Disponível em:http://www.dodf.df.gov.br/index/visualizar-arquivo/?pasta=2019%7C10_Outubro%7CDODF%20188%2002-10-2019%7C&arquivo=DODF%20188%2002-10-2019%20INTEGRA.pdf. Acessado em: 28 de set. 2020.

[2] BRASIL. Projeto de Lei nº 391/2019: Dispõe sobre a obrigatoriedade de implantação de tecnologia de reconhecimento facial em locais públicos, no âmbito do Estado. Minas Gerais: 2019. Disponível em: https://www.almg.gov.br/atividade_parlamentar/tramitacao_projetos/interna.html?a=2019&n=391&t=PL. Acessado em: 28 de set. 2020.

[3] BRASIL. Projeto de Lei nº 341/2019: dispõe sobre a obrigatoriedade de concessionários do serviço público de administração de terminais rodoviários, instalação de câmeras de segurança com tecnologia de reconhecimento facial de suspeitos e procurados da justiça nos locais que determina e dá outras providências. Rio de Janeiro: 2019. Disponível em: http://alerjln1.alerj.rj.gov.br/scpro1923.nsf/0c5bf5cde95601f903256caa0023131b/5db5f3d2098193ca832583d100739827?OpenDocument&Highlight=0,341%2F2019. Acessado em: 28 de set. 2020.

A mesma carência existe no PL nº 42/2020. Como será demonstrado a seguir, o texto proposto prevê um **compartilhamento desproporcional de imagens de câmeras privadas**. Além disso, não são discriminados os princípios legais e os direitos dos titulares que norteiam a disciplina de proteção de dados pessoais, nem mecanismos de salvaguarda para garantir a segurança e a minimização desses dados, **violando tanto a LGPD quanto o direito à autodeterminação informativa, declarado direito fundamental autônomo pelo Supremo Tribunal Federal**[4]. Por fim, argumentamos que o PL também não é compatível com o que tem sido proposto tanto no Brasil quanto no plano internacional como boas práticas de proteção de dados.

[4] BRASIL. Supremo Tribunal Federal. ADI nº 6.387/DF. Relatora: Rosa Weber. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 13 de nov. 2020.

II- Da Necessidade de Adequação entre o Projeto de Lei e a Lei Geral de Proteção de Dados

II.1 Da LGPD

A Lei Geral de Proteção de Dados (LGPD), apesar de não se aplicar para fins exclusivos de segurança pública, dispõe, em seu art. 4º, §1º[5], que a legislação específica que regular a matéria deverá **"*prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.*"**

Isso significa que a LGPD fixou pilares que devem ser respeitados por qualquer ato normativo que regule tecnologias que envolvam o tratamento de dados pessoais para o fim de segurança pública, o que se aplica a legislações específicas a serem elaboradas como o PL nº 42/2020, a saber:

a) previsão de medidas proporcionais e estritamente necessárias ao atendimento do interesse público (Art. 4º, § 1º);
b) observância aos princípios gerais da LGPD (art. 6º);
c) observância aos direitos dos titulares de dados (art. 18); e
d) previsão de tutela por parte de pessoa jurídica de direito público dos dados tratados por pessoa de direito privado para finalidade de segurança pública (Art. 4º, § 2º).

Como será apresentado a seguir, nenhum desses pilares estão presentes no PL nº 42/2020, o que demonstra sua incompatibilidade com o direito à proteção de dados pessoais, conforme descrito na LGPD.

[5] **Art. 4º, § 1º** - O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

II.2 Do juízo de proporcionalidade e necessidade

Considerar a proporcionalidade de uma coleta de dados passa inevitavelmente por um teste caso a caso de se os benefícios obtidos superam os riscos envolvidos no tratamento desses dados. Questões a serem trabalhadas se referem principalmente a:

a) quais os benefícios a serem obtidos pelo tratamento;
b) quais riscos devem ser prevenidos;
c) qual a finalidade almejada;
d) qual informação é relevante;
e) com quem ela será compartilhada;
f) qual informação deve ser compartilhada;
g) se podem as informações ser compartilhadas ou armazenadas por períodos mais curtos;
h) quais serão os efeitos desse tratamento para indivíduos e para a sociedade.[6]

No entanto, o projeto não parece cumprir tais requisitos. Não está claro por que poderia ser útil ter as imagens de todas as câmeras do Estado do Ceará, que serão milhares, acessíveis em tempo real pelas forças de segurança pública. Não há indicativos de existir efetivo policial nos quadros da Secretaria de Segurança do Estado para monitorar 24h por dia cada uma das milhares de câmeras existentes na cidade. Ainda que haja, existe alguma previsão de que isso não irá afetar o efetivo para as atividades de rua? Parece improvável

É exatamente o juízo de proporcionalidade que impõe restrições ao exercício das atividades das autoridades, propondo um equilíbrio entre o objetivo almejado e os

[6] THOMAS, Richard; WALPORT, Mark. Data sharing review report. Ministry of Justice UK, Londres, 2008, p.14. Disponível em: https://amberhawk.typepad.com/files/thomas-walport-datasharingreview2008.pdf. Acesso em 13 de nov. 2020.

meios utilizados[7]. Sem as devidas limitações, o tratamento de dados pessoais tende a ser permeado por abusos e riscos aos titulares de dados.

A análise de proporcionalidade é tão importante para operações de tratamento de dados pessoais em contextos de segurança pública que o Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal apresentado recentemente pela Comissão de Juristas designada pelo Presidente da Câmara dos Deputados Rodrigo Maia prevê a existência de um princípio específico voltado à proporcionalidade. Ele se refere à necessidade de haver "compatibilidade do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento".

Em relação às diretrizes descritas acima acerca da proporcionalidade, o PL nº 42/2020 não estabelece limitações ao compartilhamento de imagens de câmeras privadas com o sistema de videomonitoramento da Segurança Pública estadual. Na verdade, as disposições do projeto de lei são bem amplas e preveem a obrigação do compartilhamento, **em tempo real**, de todas as imagens capturadas por câmeras privadas referentes ao ambiente externo a imóveis do Estado do Ceará.

Além disso, conforme o art. 1º, §5º do PL, as imagens capturadas por câmeras privadas poderão ainda ser repassadas a órgãos de segurança pública de outras esferas do governo e a pessoas físicas e jurídicas estranhas a Administração Pública, desde que o interesse da segurança pública assim exija, mediante devida motivação. Considerando a vagueza e a consequente dificuldade em se definir o que é de interesse público, o dispositivo abre espaço para a arbitrariedade de os agentes públicos compartilharem as imagens para agentes de tratamento estranhos à finalidade inicial para a qual os dados foram coletados.

Além disso, a proteção de dados e a privacidade, mesmo sendo direitos da personalidade, devem ser enxergadas também a partir de uma perspectiva social. Afinal, o que permite a uma pessoa que se relacione com sua comunidade e se expresse de forma livre, exercendo sua liberdade de associação e expressão, é o

[7]EDPS. Data Protection: Necessity & Proportionality. Disponível em: https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en?page=1#:~:text=Proportionality%20is%20a%20general%20principle%20of%20EU%20law.&text=In%20addition%2C%20when%20assessing%20the,processing%20is%20collected%20and%20processed. Acesso em 13 de nov. 2020.

poder que ela tem de controlar os fluxos de informações a respeito de si própria daqueles que ela não quer que acessem determinadas esferas de sua vida.[8] Nesse sentido, esses direitos devem ser vistos não como estritamente individuais, mas também possuidores de uma esfera comunitária, motivo pelo qual também são tidos como bens de interesse público.[9]

É importante frisar que não existem garantias de que o compartilhamento massivo dessas imagens realmente reduzirá as taxas de criminalidade. De acordo com estudo realizado por Lawson et al., a eficácia da utilização de videomonitoramento na redução das práticas ilícitas é limitada, com relação custo-benefício consideravelmente inferior àquela obtida, por exemplo, apenas pela instalação de iluminação urbana[10]. Além disso, é questionável se o uso compartilhado e em tempo real das câmeras privada com o sistema de videomonitoramento da segurança pública é **estritamente necessário** ao atendimento do interesse público.

O Supremo Tribunal Federal (STF) já se manifestou sobre a inconstitucionalidade do compartilhamento desproporcional de dados no âmbito estatal no julgamento da Ação Direta de Inconstitucionalidade nº 6.837/DF ajuizada contra a Medida Provisória (MP) 954/2020[11]. Na ocasião, a Suprema Corte reconheceu o direito fundamental à proteção de dados pessoais e asseverou a necessidade dos diversos órgãos do poder público de observar os princípios e fundamentos relativos à proteção de dados e à privacidade.

---

[8] RAAB, C. Privacy, Social Values and the Public Interest. Busch A, Hofmann J, editors, Politik und die Regulierung von Information. Baden-Baden: Nomos verlagsgesellschaft, Baden-Baden. 2012. p. 129-151. (Sonderheft).

[9] Stevens, Leslie & Black, Gillian. (2013). **Enhancing Data Protection and Data Processing in the Public Sector**: The Critical Role of Proportionality and the Public Interest. SCRIPT-ed. 10. 2013. 10.2966/scrip.100113.93.

[10] Lawson, Tony, Rogerson, Robert & Barnacle, Malcolm. A comparison between the cost effectiveness of CCTV and improved street lighting as a means of crime reduction. In: Computers, Environment and Urban Systems, 68, 2018, p.17-25. Disponível em: https://www.sciencedirect.com/science/article/pii/S0198971516304240 . Acesso em: 15 out. 2020. Na mesma linha: Phillips, Coretta. A Review of CCTV Evaluations: Crime Reduction Effects and Attitudes To Its Use. In: Crime Prevention Studies, volume 10, pp. 123-155. Disponível em: https://pdfs.semanticscholar.org/a6ad/72791a2e6e016ed64d75524810840b548653.pdf. Acesso em: 17 out. 2020; Piza, Eric L; Welsh, Brandon C.; Farrington, David P., Thomas, Amanda L. CCTV Surveillance for crime prevention: A 40-year systematic review with meta-analysis. In: Criminology & Public Policy. 2019; 18, p.135– 159; e

[11] BRASIL. Supremo Tribunal Federal. ADI nº 6.387/DF. Relatora: Rosa Weber. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 28 de set. 2020.

Portanto, observa-se na redação do PL conceitos imprecisos que, sem as devidas limitações, poderão ser utilizados para interesses escusos e incompatíveis com a disciplina de proteção de dados pessoais e da privacidade dos cidadãos. Como veremos adiante, também estão ausentes no PL mecanismos que garantam a observância de princípios basilares da disciplina de proteção de dados e de privacidade, bem como de garantias aos direitos dos titulares de dados.

II.3 Dos princípios gerais

a. Incompatibilidade com o princípio da finalidade

Além de não prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, o PL falha ao não dispor sobre os princípios do tratamento de dados pessoais previstos no art. 6º da LGPD.

De início, identifica-se que o PL não atende ao princípio da finalidade, já que **não prevê propósitos específicos, explícitos e informados**[12].

É específica a finalidade quando é possível identificar os limites da atividade dos agentes de tratamento, para que apenas sejam tratados dados necessários, adequados e relevantes. Para além de específico, é preciso que o propósito do tratamento dos dados seja explícito, ou seja, livre de ambiguidade, sendo que tanto os agentes de tratamento quando os titulares de dados possam compreendê-lo sem dificuldades[13]. Por fim, a finalidade ainda deve ser informada de maneira inteligível, levando em consideração as particularidades dos titulares de dados sujeitos ao tratamento em específico.

A despeito dos requisitos da finalidade expressos na LGPD, o texto do projeto de lei se limita a identificar a finalidade como "o interesse da segurança pública, para a

[12] LGPD. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
[13] EDPB. Guidelines 05/2020 on consent under Regulation 2016/679. 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acesso em 5 Nov. 2020. p. 7.

atividade de prevenção e elucidação de crimes" (§3 art. 1º), o que constitui uma finalidade ampla, abstrata, sujeita a ambiguidades e sem as informações necessárias à compreensão dos titulares.

Afinal, o que garante o cumprimento do interesse da segurança pública é uma miríade de ações, preventivas e repressivas. Uma coleta massiva de dados pessoais, como a que prevê o Projeto, não demonstra qual de fato é seu propósito, já que não há sequer garantias de que de fato o Estado tem a necessidade ou mesmo a capacidade de analisar todas essas imagens em tempo real.

A não conformidade com princípio da finalidade por si só já prejudica o princípio da adequação do tratamento dos dados pessoais[14]. Isso porque não se pode haver compatibilidade do tratamento com as finalidades informadas se essas finalidades não cumprem o requisito mínimo de serem específicas.

Além disso, considerando a coleta massiva de dados que o projeto pretende implementar, abre-se espaço para um cenário de vigilância desmedida do Estado sobre os indivíduos, o que pode levar a um sentimento generalizado de normalização da supervisão estatal e o consequente *chilling effect* dos titulares de dados.

Por *chilling effect* compreende-se o fenômeno no qual indivíduos temem exercitar o seu direito à liberdade de expressão, associação e reunião por receio de serem vigiados e consequentemente punidos por suas ações[15].

Vale ressaltar que as práticas de vigilância com finalidade política não se limitam aos países autoritários. Nesse sentido, o Supremo Tribunal Federal, no âmbito da Ação de Descumprimento de Preceito Fundamental - ADPF nª 722/DF de 2020, suspendeu todo e qualquer ato do Ministério da Justiça e Segurança Pública de produção ou compartilhamento de informações sobre a vida pessoal, as escolhas pessoais e políticas, as práticas cívicas de cidadãos, servidores públicos federais,

[14] LGPD. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

[15] PENNEY, Jonathon. Internet surveillance, regulation, and chilling effects online: a comparative case study. Internet Policy Review, vol. 6, ed. 2, 2017. Disponível em: https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case. Acesso em: 14 de nov. 2020.

estaduais e municipais identificados como integrantes de movimento político antifascista, professores universitários e quaisquer outros que, atuando nos limites da legalidade, exerçam seus direitos de livremente expressar-se, reunir-se e associar-se[16]. Portanto, vigilância sem as devidas limitações à finalidade pode prejudicar o exercício de direitos fundamentais como a liberdade de expressão e associação, conforme descrito acima.

b. Incompatibilidade com o princípio da necessidade

Para além do princípio da finalidade, o PL não estabelece quaisquer limitações do tratamento ao mínimo necessário para a consecução da finalidade de segurança pública, de modo a cumprir o princípio da necessidade[17]. Ao contrário, no lugar de estabelecer a abrangência dos dados pertinentes, proporcionais e não excessivos, **impõe o compartilhamento ilimitado e em tempo real das imagens de câmeras privadas**. Isso sem que haja qualquer ocorrência criminal prévia na região que motive um monitoramento de imagens que têm a capacidade de revelar aspectos da intimidade de todas as pessoas que passaram por determinado local e não somente daquelas alvo de investigações.

c. Incompatibilidade com os princípios da qualidade dos dados e da segurança

A não observância dos princípios da finalidade e necessidade tem como consequência direta o comprometimento do princípio da qualidade dos dados[18].

---

[16] BRASIL. Supremo Tribunal Federal. ADPF nº 722/DF. Relatora: Cármen Lúcia. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344764619&ext=.pdf. Acesso em: 13 de nov. 2020.

[17] LGPD. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

[18] LGPD. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Segundo a LGPD, **é necessário garantir aos titulares exatidão, clareza, relevância e atualização dos dados**, o que só se alcança por meio da precisa delimitação da finalidade e necessidade do tratamento dos dados, justamente o que o texto do PL não concretiza.

Ainda sobre a inobservância dos princípios da LGPD, **são ausentes no PL a previsão de quaisquer medidas técnicas e administrativas aptas a proteger as imagens de acesso não autorizado** e de situações acidentais ou ilícitas de alteração, comunicação ou difusão. Tais ferramentas são essenciais para o cumprimento do princípio da segurança disposto no inciso VII do art. 6º da LGPD.[19] No presente caso, considerando que as imagens das câmeras virão de milhares de locais distintos, a possibilidade de vazamento de dados é imensa, e nenhuma medida é prevista no Projeto para garantir a segurança desses dados.

d. Incompatibilidade com os princípios da transparência e da não discriminação

Já quanto ao princípio da transparência[20], o PL não fornece informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e sobre os respectivos agentes de tratamento. **Não há a previsão de duração, muito menos da forma com que os dados serão tratados**. Além disso, o PL não menciona o órgão responsável pelas decisões referentes ao tratamento das imagens.

É importante destacar que o uso compartilhado de imagens em tempo real pode revelar aspectos sensíveis da personalidade dos indivíduos cujas imagens forem captadas em vídeo. Câmeras posicionadas em frente a templos religiosos, casas de

[19] LGPD. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
VII - segurança: 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.
[20] LGPD. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

festas, hospitais, sindicatos e partidos políticos podem revelar dados sobre a convicção religiosa, a vida sexual, a saúde, a filiação a sindicato e a opinião política de pessoas. Por isso, o PL também falha ao não observar o princípio da não-discriminação disposto no inciso IX do art. 6º da LGPD[21], pois **não prevê medidas que mitiguem a realização do tratamento para fins discriminatórios, ilícitos ou abusivos**[22]**.**

e. Incompatibilidade com o princípio da prevenção

Aliado ao princípio da não-discriminação, é preciso ainda que o PL disponha de **medidas para prevenir a ocorrência de danos** em virtude do tratamento das imagens de videomonitoramento. A cogência de dessas medidas é prevista pelo princípio da prevenção, disposto no inciso VIII do art. 6º da LGPD[23].

Como consequência da não observância da proporcionalidade no tratamento das imagens de videomonitoramento, bem como da ausência de previsões que resguardem os princípios supracitados, depreende-se que o PL proposto pelo Governo do Estado do Ceará não demonstra a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas[24].

---

[21] LGPD. Art. 6 As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

[22] LGPD. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

[23] LGPD. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

[24] LGPD. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

II.4 Dos direitos do titular

Também não estão expressas na redação do texto legislativo medidas que assegurem aos titulares de dados o exercício dos direitos previstos na LGPD e que também se aplicam a tratamentos de dados para fins de segurança pública, conforme o supracitado art. 4º, §1º, LGPD.

De início, cabe destacar que a própria **ausência de uma indicação clara do órgão controlador dos dados** dificulta com que os cidadãos alvo das imagens capturadas saibam exatamente a qual órgão solicitar o exercício dos seus direitos. A quem o cidadão poderá se reportar para exercer seus direitos? À Polícia Civil? Militar? À Secretaria de Segurança Pública do Estado?

Além disso, ao não prever a observância dos direitos dos titulares, o PL não deixa claro, por exemplo, se ao indivíduos será assegurado o exercício de outros direitos previstos na LGPD, que também se aplicam a atividades de segurança pública, conforme seu art. 4º, §1º. São eles:

a. **acesso aos dados** coletados;
b. **correção de dados** incompletos, inexatos ou desatualizados;
c. **anonimização, bloqueio ou eliminação** de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
d. **acesso a informações** acerca das entidades públicas e privadas com as quais o controlador realizou uso compartilhado das imagens; e
e. **revisão de decisões** tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses.

Não há qualquer indicação a como e frente a quem serão observados esses direitos. Observa-se, desse modo, incongruências entre as disposições do PL e a disciplina legal de proteção de dados pessoais reconhecidas no ordenamento jurídico brasileiro.

II.5 Do tratamento de dados pessoais por ente privados para fins de segurança pública

Outro ponto a ser levantado é o que dispõe o §2º do art. 4º da Lei Geral de Proteção de Dados, segundo o qual é vedado o tratamento de dados pessoais por entes privados para fins de segurança pública, **exceto quando se trata de procedimento sob tutela de pessoa jurídica de direito público**.

O tratamento de dados pessoais realizado por câmaras privadas para o propósito de segurança privada é juridicamente tutelado de forma distinta daquele realizado para fins de segurança pública. Como foi abordado nas subseções anteriores (ver II. 2, II. 3 e II. 4), o tratamento de dados pessoais na segurança pública deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados os princípios gerais de proteção e os direitos do titular previstos na LGPD (§1º do art. 4º).

Portanto, o §2º do art. 4º da LGPD, ao prever a obrigatoriedade de tutela de pessoa jurídica de direito público, o faz justamente para que os dados inicialmente tratados por entes privados, para finalidades outras que não a segurança pública, possam ser tratados para essa nova finalidade sem incorrer em risco de violar os requisitos disposto no §1º do art. 4º da LGPD.

Cabe ressaltar que não há uma definição precisa na LGPD sobre como se daria a tutela por parte da pessoa jurídica de direito público, procedimento que deverá ser regulamentado pela Autoridade Nacional de Proteção de Dados (ANPD) ou pela autoridade competente definida em uma futura lei de proteção de dados para atividade de segurança pública e de persecução penal[25].

De todo modo, uma leitura acerca do termo "tutela" no âmbito do Direito Público traz a noção de um encargo imposto a um ente que toma a responsabilidade

[25]AGÊNCIA CÂMARA DE NOTÍCIAS. Rodrigo Maia recebe anteprojeto para controle de dados de investigações criminais. Braília, 05 de nov. de 2020. Disponível em: https://www.camara.leg.br/noticias/694562-anteprojeto-sobre-uso-de-dados-na-seguranca-publica-deve-ficar-pronto-em-novembro/. Acesso em: 26 de nov. de 2020.

sobre as ações de um segundo ente, guiando suas ações e sendo responsabilizado pelas diretrizes que der e pelas ações que o ente tutelado realizar.

Ao se analisar o PL nº 42/2020, verifica-se que não há qualquer tipo de tutela pelos órgãos de segurança do Estado do Ceará. O projeto prevê somente o uso pelo Estado dos dados coletados por particulares que serão compartilhados em tempo real com o Poder Público. Não há qualquer tipo de acompanhamento sobre o procedimento de coleta, sobre quais dados serão coletados, sobre regulamentação ou sobre quem será responsabilizado civilmente por seu uso, mas meramente a previsão de que haverá o aproveitamento pelo poder público dos dados coletados por entes privados.

Nesse sentido, o PL se limita a dispor, no § 1º do art. 3º, que a SSPDS orientará proprietários, inquilinos ou síndicos sobre como proceder para o compartilhamento das imagens. Assim, há uma previsão de que o Estado fará uma orientação técnica sobre os modos de compartilhamento, mas não há previsões sobre o regime de tutela nem sobre o seu conteúdo.

Portanto, o tratamento de dados pessoais por entes privados para fins de segurança pública que o PL busca impor não está em conformidade com a obrigação de estabelecer procedimentos de tutela por parte da pessoa jurídica de direito público. Ao não prever um modelo de tutela por parte da administração pública estadual, mas tão somente uma coleta sem filtros dos dados tratados por pessoas físicas e jurídicas, **o PL nº 42/2020 cria uma situação de descompasso com a LGPD, cujo caráter federal coloca o PL em estado de ilegalidade, caso venha a ser aprovado.**

III - A regulação da videovigilância no contexto europeu

Cabe aqui analisar como a experiência europeia, cuja normatização em proteção de dados serviu de inspiração à LGPD, regula esse tema. Em 2020, o Comitê de Proteção de Dados Pessoais (EDPB) emitiu nova versão do documento intitulado "Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo". O estudo aponta algumas diretrizes e indicações sobre o processamento de dados pessoais coletados por câmeras de vigilância que analisam justamente o crescente uso de câmeras nos espaços urbanos.

Diante das prováveis violações de direitos fundamentais, como a privacidade, o EDPB indica que a "videovigilância não é por definição uma necessidade quando existem outros meios para alcançar o objetivo subjacente. Caso contrário, corremos o **risco de mudar as normas culturais, levando à aceitação da falta de privacidade como o princípio geral**".[26]

Uma das recomendações do Comitê, que inclusive se aproxima do regime jurídico brasileiro analisado nesta Nota Técnica, é que "antes de instalar um sistema de videovigilância, o responsável pelo tratamento deve sempre examinar criticamente se esta medida é, em primeiro lugar, adequada para atingir o objetivo desejado e, em segundo lugar, adequada e necessária às respectivas finalidades".[27]

A Diretriz do EDPB afirma que "questões de proteção de dados inerentes a cada situação e a análise jurídica podem diferir em função da tecnologia utilizada"[28] e isto

[26] EDPB. Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo. 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf. Acesso em 4 out. 2020. p. 6

[27] EDPB. Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo. 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf. Acesso em 4 out. 2020. p. 10

[28] EDPB. Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo. 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf. Acesso em 4 out. 2020. p. 6

está associado ao risco do tratamento daquele dado, de modo que algumas tecnologias possuem um risco de violação de direitos e discriminação mais elevado.

Considerando que, aliado à videovigilância por câmaras simples, a implementação de tecnologias de reconhecimento facial se encontra em fase de expansão no Brasil[29], o que confere um caráter ainda mais intrusivo da atividade das forças policiais, cabe analisar os riscos adicionais que uma eventual aplicação de técnicas de reconhecimento facial às imagens de câmeras de CCTV podem representar à privacidade.

De acordo com o EDPB, o reconhecimento facial possui um elemento peculiar que deve ser observado pelas autoridades públicas para que haja as salvaguardas e proteções necessárias. O Comitê evidencia que um "software utilizado para identificação, reconhecimento ou análise facial tem um desempenho diferente em função da idade, do género e da etnia da pessoa que está a ser identificada".

Tendo em vista que a sociedade brasileira é miscigenada e diversa, usar tecnologias de vigilância imoderada atingiria alguns grupos de forma desproporcional, principalmente tendo em vista a possibilidade de existência de viéses discriminatórios na aplicação da tecnologia.

III.1 - Discriminação algorítmica

Sobre a existência de viés algorítmico, estudos sobre o uso de RF sinalizam aspectos discriminatórios na concepção da tecnologia e nos dados que utiliza para treinar. O desempenho dos algoritmos de RF são prejudicados se os dados utilizados para treinamento da tecnologia, templates faciais, não forem representativos[30] . Por

[29]LAVADO, Thiago. Aumento do uso de reconhecimento facial pelo poder público no Brasil levanta debates sobre limites da tecnologia. G1, fev. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/02/21/aumento-do-uso-de-reconhecimento-facial-pelo-poder-publico-no-brasil-levanta-debate-sobre-limites-da-tecnologia.ghtml. Acesso em: 01 de dez. 2020.

[30] KLARE, Brendan et al. Face Recognition Performance: Role of Demographic Information. IEEE Transactions on information forensics and security, vol. 7, n. 6, p. 1789- 1801, 2012. p. 1791

isso, a autoridade de proteção de dados do Reino Unido (ICO, sigla inglês)[31] pontua que o sistema de RF pode possuir viés discriminatório se as faces que foram utilizadas no treinamento do algoritmo não tiverem uma representatividade equilibrada da população, ou seja, não observe as variações de cor e etnia.

Logo, a taxa de precisão e acurácia será diferente para rostos que o sistema não foi treinado e, por isso, não está familiarizado. Dessa forma, resta evidente que o uso de câmeras de videomonitoramento e sistemas de RF deve observar as limitações técnicas dos dispositivos, ainda mais Brasil, país conhecido pela diversidade da população: estudo da Rede de Observatórios de Segurança identificou que **90,5% das pessoas presas porque foram flagradas pelas câmeras de reconhecimento facial no Brasil eram negras**[32]. Isso demonstra como essas tecnologias podem ser utilizadas para gerar encarceramento em massa de uma população que já é naturalmente mais visada pelo sistema penal.

III. 2 - Diretiva 2016/680, União Europeia

Ainda na perspectiva europeia, a **Diretiva 2016/680** da União Europeia é relevante para perceber como o tratamento e a proteção de dados se aplica ao contexto europeu de matéria penal como ações para promoção de segurança pública e para investigação criminal. A nível de comparação, o Regulamento Geral de Proteção de Dados da UE - RGPD, assim como a LGPD, reporta-se a uma outra lei para previsão de normas para proteção de dados em matéria de segurança pública, e essa legislação é a Diretiva 2016/680. Por isso, é interessante observar como se dá a proteção de dados nesse contexto de segurança e as similaridades entre o que dispõe a Diretiva europeia e o §1º do art. 4º da LGPD.

---

[31] INFORMATION COMMISSIONER'S OFFICE (ICO). ICO investigation into how the police use facial recognition technology in public places. 2019. Disponível em: https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-2019 p. 33

[32] Rede de Observatórios de Segurança. Retratos da Violência: Cinco meses de monitoramento, análises e descobertas, 2019. Disponível em http://observatorioseguranca.com.br/wp-content/uploads/2019/11/1relatoriorede.pdf

A Diretiva parte da premissa de que **"é crucial assegurar um nível elevado e coerente de proteção dos dados pessoais das pessoas singulares".** Ou seja, mesmo no contexto de segurança pública, é fundamental garantir a proteção de dados dos investigados, a integridade dessas informações e o uso devido ao mesmo tempo em que se garante o interesse público. Dessa forma, a Diretiva estabelece alguns princípios e direitos do titular de dados que devem ser analisados nesta nota tendo em vista o disposto no PL que tramita da Assembléia Legislativa do Ceará.

A Diretiva 2016/680 assegura ao titular o **direito de acesso** às informações pessoais contidas em um banco de dados, bem como de retificação da informação incorreta e de apagamento dos dados diante de condições previstas em lei. Além disso, ela garante que dados desatualizados, inexatos ou incompletos não sejam disponibilizados para que nenhuma autoridade de justiça tome decisão fundamentada em dados imprecisos (Artigo 7º, 2, Diretiva 2016/680).

A norma europeia, em seu artigo 13, também assegura que o responsável pelo tratamento de dados **comunique** ao titular algumas informações. O sujeito de dados deve ser informado sobre a finalidade do tratamento a que os dados pessoais se destinam e sobre o direito de solicitar a retificação de um dado pessoal que esteja incorreto no banco de dados.

Ainda, para que haja **transparência** no processamento de dados, cabe ao responsável informar o fundamento jurídico do tratamento e o prazo de conservação dos dados pessoais ou, no mínimo, os critérios para definição desse período e os possíveis destinatário dessas dados (Art. 13, nº 2, Diretiva 2016/680). Logo, busca-se nitidez na relação entre o titular dos dados e o responsável pelo tratamento.

Sobre os direitos dos titulares, o regulamento se atentou à possibilidade de adiamento, limitação ou não prestação aos sujeitos dos dados de algumas informações em situações específicas. Essas restrições só ocorrem se e enquanto tais medidas forem necessárias e proporcionais numa sociedade democrática, tendo devidamente em conta os direitos fundamentais, os interesses legítimos das pessoas e os fundamentos jurídicos pertinentes (Art. 13, nº 3, Diretiva 2016/680). Portanto,

sempre há uma ponderação entre a finalidade de segurança pública e os direitos fundamentais dos titulares de dados.

Para que o tratamento de dados ocorra de forma transparente e atenda aos princípios de proteção de dados, é necessário que o responsável pelo tratamento conserve um **registro das atividade de processamento e utilização dos dados**. Isto é, o processo de tratamento dos dados bem como o registro de todas as categorias de atividades realizadas devem ser documentados de forma transparente em nome de um responsável pelo tratamento (Art. 24, Diretiva 2016/680). Cabe também ao responsável informar, sem demora injustificada, aos titulares caso haja violação dos dados pessoais (Art. 31 da Diretiva 2016/680).

Quanto ao que deve ser informado e registrado pelo responsável do tratamento de dados, a Diretiva 2016/680, em seu artigo 13, assegura que se garanta ao titular o fornecimento de determinadas informações.

O sujeito de dados deve saber sobre a **finalidade** do tratamento a que os dados pessoais se destinam e sobre o direito de solicitar a retificação de um dado pessoal que esteja incorreto. Ainda, para que haja transparência no processamento de dados, cabe ao responsável **informar o fundamento jurídico do tratamento e o prazo de conservação dos dados** ou, no mínimo, os critérios para definição desse período e os possíveis destinatário dessas dados (Art. 13, nº 2, Diretiva 2016/680). Logo, deve-se buscar nitidez na relação entre o titular e o responsável pelo tratamento.

Por fim, o princípio da transparência é efetivado também por meio do desenvolvimento de uma avaliação de impacto do uso da tecnologia no âmbito da segurança pública. Caso o tratamento de dados possa resultar num elevado risco para os direitos e liberdades das pessoas naturais, observada a natureza, o âmbito, o contexto e a finalidade do tratamento, o art. 27 prevê a necessidade de elaboração da **Avaliação de Impacto sobre a Proteção de Dados**.

Ainda, a Avaliação deverá descrever (i) os riscos para os direitos e para as liberdades dos titulares dos dados, (ii) as medidas previstas para fazer face a esses riscos, (iii) as garantias dos sujeitos previstas em lei, (iv) as medidas de segurança e (v)

os mecanismos para assegurar a proteção dos dados pessoais (Art. 27 da Diretiva 2016/680).

Com isso, a Diretiva apresenta uma série de direitos do titular dos dados que garante a legitimidade do tratamento de dados para fins de segurança pública que não são descritos ou ao menos citados no Projeto de Lei. Além disso, no contexto europeu, os princípios de finalidade e de transparência são concretamente observados pelas forças policiais, como nas obrigações de exclusão dos dados pessoais depois de um período de tempo e informação do titular sobre o tratamento, obrigação que sequer aparece no PL 42/2020.

A exposição de tais pontos é útil para que identifiquemos a **eloquente ausência de salvaguardas no tratamento massivo de dados pessoais proposto pelo PL nº 42/2020.** Por isso, identifica-se que, no intuito de promover segurança pública, o PL não tomou nenhum dos cuidados mínimos de proteção de dados já previstos na lei brasileira e seguidos por países democráticos.

V - Conclusão

O PL nº 42/2020 pretende instaurar um mecanismo de vigilância massiva no Estado do Ceará a partir de uma perspectiva excessivamente intrusiva na esfera privada de indivíduos. Suas disposições não são proporcionais e não são justificadas de forma a serem vistas como necessárias ao atendimento do objetivo de segurança pública pretendido pelo Estado.

Além disso, o PL fere os princípios dispostos no art. 6º da LGPD ao não deixar claro finalidades específicas para os tratamentos de dados a serem realizados nem demonstrar um juízo de necessidade e adequação ao propósito almejado. Ainda, a redação do Projeto de Lei falha ao não prever mecanismos de transparência nem de tutela prévia por parte do Poder Público acerca do tratamento de dados pessoais feito por particulares e de responsabilização posterior.

Nessa linha, o PL não se adequa a diretrizes de boas práticas nacionais e internacionais, como as da União Europeia, no tema de proteção de dados para fins de segurança pública, de modo a proteger direitos fundamentais de indivíduos em território cearense.

Pelo exposto, o LAPIN se posiciona pela **rejeição do Projeto de Lei 42/2020** da forma como foi apresentado pelo Governo do Estado do Ceará.