DADOS, PRIVACIDADE E PERSECUÇÃO PENAL: CINCO ESTUDOS

FGV DIREITO SP
ESCOLA DE DIREITO DE SÃO PAULO

DataPrivacyBR

Produtos do Projeto Multidisciplinar desenvolvido na
Escola de Direito da Fundação Getúlio Vargas – FGV-SP

DADOS, PRIVACIDADE E PERSECUÇÃO PENAL: CINCO ESTUDOS

COODENADORAS

Professora Dra. Eloísa Machado de Almeida

Professora Dra. Heloisa Estellita

ASSISTENTE

Douglas Henrique Norkevicius

FGV-DIREITO SP

2021

AUTORES

Ana Carolina Dias
Ana Beatriz Santos Pires
André Bialski
Andrey Fortes
Antonio Piva
Antonio Vento
Beatriz Baccaro
Beatriz Crisostomo
Eduardo Messina
Frederico Amaral
Gabriela Cavagnoli
Gabriela Cotello
Glendha Visani
Isabella Matusita
Juliana Reimberg
Leticia Gongora
Maria Julia Gonçalves
Nicolas Haspo
Nicole Pudo Gomes
Oliver Wiegerinck
Paula Rodovalho

APRESENTAÇÃO

A emergência do direito à proteção de dados pessoais, enquanto direito autônomo, tem promovido a reconfiguração de uma série de relações e negócios jurídicos.

Não é diferente no campo do Direito Penal, entendido em um sentido amplo. Afinal, em um Estado de Direito, os direitos fundamentais e o devido processo legal são elementos conformadores da atividade persecutória do Estado e o reconhecimento de um novo direito impõe novos parâmetros a serem observados também pelas autoridades incumbidas da inteligência, da segurança pública, da persecução e da execução penais. E isso sem prejuízo da exceção estabelecida na Lei Geral de Proteção de Dados (Lei nº 13.709/2018, art. 4º, III) e da lamentável inexistência, entre nós, de uma lei geral de proteção de dados em matéria penal, pois os fundamentos limitadores estão lançados já na Constituição Federal.

Neste cenário, em que um novo direito emerge e ainda lhe falta toda disciplina legal infraconstitucional, pensar a intersecção entre persecução penal e proteção de dados pessoais se mostra tarefa bastante desafiadora. Tarefa esta que se torna ainda maior quando trazida para a realidade institucional brasileira, marcada por uma herança ditatorial de violações sistemáticas a direitos fundamentais.

Porém, nenhum problema é grande demais quando enfrentado coletivamente. Esta foi a proposta do Projeto Multidisciplinar Segurança Pública e Proteção de Dados, conduzido com alunos e alunas do programa de graduação da FGV Direito SP, no primeiro semestre de 2021: encarar casos para os quais não há resposta e pensar sobre eles com criatividade e ousadia.

A seleção dos casos, dos seus aspectos e a forma como seriam abordados foi feita pelas alunas e alunos, como é próprio da metodologia dos projetos, que coloca professores em posição de facilitadores de um percurso que é escolhido e trilhado pelas alunas e alunos com o máximo de autonomia. Uma outra marca dos projetos é a interação com parceiros externos, experts no tema escolhido. Esta publicação dá testemunho de como é decisiva a colaboração de diversas organizações civis e experts em proteção de dados para o alcance de abordagens e soluções criativas, especialmente numa matéria nova e carente de regulação em lei como a aqui tratada. Essas organizações e experts foram nominalmente mencionados em cada um dos cinco estudos que compõem esta obra.

O resultado das inéditas reflexões de alunas e alunos é agora publicado pela mãos do DATA PRIVACY BRASIL, parceira inestimável nesse empreendimento, com a pretensão de contribuir para a discussão dos contornos do direito à proteção de dados no Brasil.

Como professoras neste percurso, só nos resta agradecer às alunas e aos alunos, à monitora Bárbara Simão, aos estagiários Douglas Norkevicius e Fabrício Lacerda e aos parceiros e experts que possibilitaram a produção deste trabalho, do qual muito nos orgulhamos.

Boa leitura!

Eloísa Machado de Almeida e Heloisa Estellita

PREFÁCIO

Nos últimos anos, o ensino por projetos tem ganhado destaque quando se fala de metodologias ativas de ensino em cursos superiores. Embora ainda não seja tão popular nos cursos jurídicos, tem havido uma maior abertura a abordagens multidisciplinares.

Na nossa Escola, temos o privilégio de, com apoio institucional, ter colegas docentes incansáveis em inovar, que se dedicam a refletir sobre a própria prática e a enfrentar esses novos desafios – inclusive em tempos tão incertos e disruptivos como este em que estamos vivendo, de ensino emergencial remoto devido à pandemia.

Romper com as práticas tradicionais do Direito está no *ethos* da FGV Direito SP. Logo, a abordagem de ensino por projetos, pautada na aprendizagem pela experiência, tem como ponto central o engajamento de docentes e estudantes em compreender questões sociais significativas, complexas e atuais.

Tais problemas são da realidade que os cerca, envolvendo questões jurídicas e interdisciplinares. Isso é o que o ensino por projetos propõe, que os estudantes se debrucem sobre essas questões, a fim de construir soluções reais, para problemas reais, de uma realidade a qual pertence.

Mas, não é um aprender fazendo simplesmente por fazer, de modo periférico ao conteúdo ou apenas para cumprir tarefas. Por meio dessa abordagem, desenvolvem-se habilidades interpessoais fundamentais, para além da construção de conhecimento técnico jurídico e de outras áreas. Essas chamadas *soft skills* devem fazer parte dos objetivos de aprendizagem, não como um item adicional ou uma disciplina, mas enquanto estratégia para um aprendizado mais significativo do conteúdo programático.

Sim, passar a enxergar o conteúdo técnico não mais hierarquizado nem no topo de importância em relação ao desenvolvimento de competências interpessoais é uma mudança drástica no processo de ensino e aprendizagem.

E o ensino por projetos permite justamente trabalhar a aprendizagem técnica de modo convergente às habilidades interpessoais: cooperação, empatia, trabalho em equipe, inteligência emocional, liderança, gestão de pessoas, de tempo e de projetos.

Ao desafiar estudantes a colaborar com outras pessoas, lidando com diferentes perspectivas, a fim de construir uma solução viável a problemas complexos que nossa sociedade, em constante transformação, enfrenta é um modelo de ensino que proporciona uma jornada de aprendizagem significativa e dinâmica.

Pode ser que o projeto dure apenas alguns dias, meses, um semestre, um ano ou mais. Ainda, pode envolver apenas uma disciplina, várias, ou uma grade curricular inteira. Independentemente do tempo e modo como é implementado, trata-se de uma abordagem de ensino centrada no estudante.

O ensino por projetos dá voz e escolha aos estudantes. A partir do que constatam da realidade em que estão imersos, eles mesmos definem quais questões são relevantes e querem investigar. O conhecimento construído é aplicado ao mundo real, terá uma serventia. Assim, o processo não está todo definido de antemão pelo docente, mas se trata de uma construção de responsabilidade coletiva.

Além disso, tais construções são fundamentalmente propositivas, gerando discussões, dados e recomendações úteis à sociedade. Em diversas camadas e dimensões, todas as pessoas saem transformadas desse processo. Além de os alunos e as alunas aprofundarem ativamente sua compreensão sobre o Direito, também realizam contribuições sociais concretas e relevantes, havendo um sentido nessa jornada.

Assim, o papel docente é de facilitar esse processo, auxiliando e incentivando estudantes ao longo de todo o projeto, mas sem tirar deles e delas a autoridade para definir os problemas e soluções. É um método ativo de ensino, pautado na colaboração e menos hierárquico, de forma que o protagonismo seja dos próprios estudantes, que se envolvem profundamente na construção de seu próprio conhecimento.

E os projetos multidisciplinares da FGV Direito SP são desenhados por projetos. Eles têm o objetivo de permitir que estudantes desenvolvam competências necessárias a qualquer profissão ou atividade profissional. Dessa forma, oferecem a possibilidade de se engajarem em projetos de natureza multidisciplinar, enfrentando desafios complexos, e proporcionam um ambiente para que eles e elas sejam responsáveis pelo seu próprio aprendizado, treinando habilidades e construindo seu conhecimento de forma autônoma e independente, por meio de experiências práticas.

Construir esses caminhos, como as competentes professoras Eloísa Machado de Almeida de Almeida e Heloísa Estellita fizeram no primeiro semestre de 2021 no **Projeto Multidisciplinar Segurança Pública e Proteção de Dados**, no programa de graduação da Escola de Direito de São Paulo da Fundação Getulio Vargas, exige uma dedicação e um planejamento intensos.

Os produtos elaborados pelos grupos de estudantes representam bem o sucesso da metodologia de ensino por projetos, no qual se aprofundaram em temas como segurança pública, direitos fundamentais, Lei Geral de Proteção de Dados Pessoais e a esfera penal.

Foram cinco grupos de alunos e alunas, que construíram os projetos: *Uma ANPD para a proteção de dados na segurança pública e na persecução penal?*, por Andrey Fortes, Frederico Amaral e Nicolas Haspo; *Reconhecimento facial no metrô de São Paulo*, por Ana Carolina Souza Dias, Antonio Piva, Beatriz Crisostomo, Beatriz Baccaro e Paula Rodovalho; *Transparência no tratamento de dados por unidades de inteligência financeira*, por André Bialski, Antonio Vento, Eduardo Messina e Oliver Wiegerinck; *Alvos predeterminados: um estudo de caso sobre a implementação da tecnologia de reconhecimento facial na Bahia*, por Ana Beatriz Santos, Gabriela Cavagnoli, Gabriela Cotello, Glendha Visani e Leticia Gongora; e *Vigilância massiva pós-pandemia. Covid-19: análise dos aplicativos de combate à pandemia e seus impactos à proteção de dados e à privacidade no pós-pandemia*, por Isabella Matusita, Juliana Reimberg, Maria Julia Gonçalves e Nicole Pudo.

Os produtos, resultados desse projeto multidisciplinar, vão desde coleta e avaliação de dados aprofundadas à análise de legislação, nacional e internacional, políticas de reconhecimento facial, inteligência artificial e segurança pública.

O reflexo da realização de pesquisa aprofundadas sobre a temática e o envolvimento dos alunos e das alunas em temas que lhe interessam, é a alta qualidade das propostas. Por meio de desafios concretos atuais e significativos, convergiu-se a construção ativa e sólida do próprio conhecimento e o desenvolvimento de habilidades interpessoais.

Ao longo dessa jornada, a abordagem de ensino por projetos possibilitou que os(as) estudantes desenvolvessem competências fundamentais para assumirem um papel ativo não somente em sala de aula, mas fundamentalmente de cidadãos no mundo.

Se realmente acreditamos que um curso de Direito deve contribuir para a formação de cidadãos melhores e profissionais jurídicos capazes de realizar uma reflexão profunda sobre os problemas da realidade que os(as) cerca, com um olhar crítico a respeito do papel do Direito na sociedade e que consigam dialogar com profissionais de áreas multidisciplinares, o ensino por projetos cumpre esse objetivo.

Marina Feferbaum
Professora e Coordenadora do Centro de Ensino e Pesquisa em Inovação e da área de Metodologia de Ensino da Escola de Direito de São Paulo da Fundação Getulio Vargas (CEPI FGV Direito SP)

Julho de 2021

POSFÁCIO

Talvez uma das maiores falhas da Lei Geral de Proteção de Dados do Brasil foi não ter deixado claro que, pelo menos, algumas de suas garantias também deveriam ser aplicadas aos contextos de segurança pública e atividades de investigação e repressão de infrações penais. A redação ambígua do seu artigo quarto ("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") não deixa claro se os princípios gerais de proteção de dados, previstos no artigo sexto, já poderiam ser aplicados independentemente de uma legislação específica de proteção de dados na esfera penal.

A redação em grifo pode ser lida de tal forma que os princípios e os direitos já previstos na LGPD devem ser observados em conjunto quando da aplicação de uma lei específica, ou podem ser analisados de maneira a já determinarem a sua aplicação imediata, mesmo na ausência da novel norma. Diante dessa dubiedade, diversas têm sido as interpretações, divergindo entre os autores que defendem a sua aplicabilidade, e aqueles que doutrinam que tudo dependeria de uma nova lei, a já nascente LGPD Penal.

Essa discussão ganhou novos contornos com a histórica decisão do Supremo Tribunal Federal que reconheceu o direito fundamental à proteção de dados em 2020 - o apelido caso "IBGE" - e, mais recentemente, com a aprovação da proposta de Emenda à Constituição 17/2019 em 2021. Como aferir se o manejo de dados para fins de segurança pública e para fins de persecução penal consiste em uma interferência proporcional desse novo direito fundamental, senão aplicando como barreira de contenção os princípios e garantindo os direitos básicos dos titulares de dados?

A LGPD Penal ainda se encontra em seu anteprojeto. O anteprojeto, além de dirimir as dúvidas acima descritas, traz como uma das seus principais inovações a necessidade do desenvolvimento de relatórios de impacto à proteção de dados em situações no contexto penal em que o uso de dados pessoais pode ocasionar um risco alto para os direitos e liberdades individuais de indivíduos. O instrumento permite avaliar os riscos existentes e sugerir medidas de mitigação destes até um nível aceitável, tanto pela organização quanto pela sociedade.

Uma boa prática, em prol do interesse público, seria permitir a ampla discussão multissetorial desses riscos e a melhor forma de endereçá-los, ou, em algumas situações, de não aceitá-los, o que poderia levar a uma possível proibição e banimento do uso de algumas tecnologias. Não é por outra razão que a Associação Data Privacy Brasil de Pesquisa sugeriu a criação de um Conselho Nacional para reunir essa pluralidade de olhares e congregando os diferentes níveis da federação. A criação desse conselho – diferente daquele previsto no artigo 58-A da Lei Geral de Proteção – é necessário para que seus representantes possam quebrar o que foi chamado de "isolacionismo institucional" no campo da segurança pública. Daí porque uma composição quadripartite, com articulação da União, dos Estados e Municípios, bem como de representantes do sistema de justiça e da sociedade civil com expertise nesse campo em específico.

Uma outra consequência seria a quase compulsoriedade do emprego da metodologia conhecida como privacy by design, ou privacidade desde a concepção, que preconiza o respeito a padrões de proteção de dados e da privacidade desde a concepção e o desenvolvimento de produtos, serviços, funcionalidades e práticas. Tecnologias que antes eram emergentes, como o uso de reconhecimento facial na busca por foragidos e procurados da justiça, e que hoje se tornaram, em alguns lugares e cidades, comuns, e até mesmo objetos de campanhas políticas, muito poderiam se beneficiar da combinação entre relatórios de impacto e privacy by design. O banimento ao redor do mundo do uso dessa tecnologia no contexto penal em face da estrondosa margem de erro demonstra isso com facilidade.

Por isso mesmo, diante da adoção generalizada de novas tecnologias que têm como substrato o uso de informações pessoais e que põem em risco uma ampla gama de direitos fundamentais e humanos, é necessário não somente olhar para o hoje, mas também para o amanhã. É necessário evitar o erro de não prospectar e a imaginar os impactos em grande escala que tais novos usos podem trazer para a sociedade. Essa discussão é premente para garantirmos um futuro justo e adequado. Um futuro em que liberdades civis não sejam trocadas por facilidades, comodidades e eficiências. Tais trade offs não podem prevalecer sob o risco de um cenário inóspito e irreversível. O conteúdo deste livro deve servir de inspiração e orientação para que sejam desenvolvidas políticas públicas e práticas privadas menos intrusivas e cerceadoras de direitos. Ainda há tempo.

Bruno Bioni
Renato Leite Monteiro
Diretores-fundadores do Data Privacy Brasil

SUMÁRIO

ALVOS PREDETERMINADOS:

UM ESTUDO DE CASO SOBRE A IMPLEMENTAÇÃO DA TECNOLOGIA DE RECONHECIMENTO FACIAL NA BAHIA

ALVOS PREDETERMINADOS: UM ESTUDO DE CASO SOBRE A IMPLEMENTAÇÃO DA TECNOLOGIA DE RECONHECIMENTO FACIAL NA BAHIA

Ana Beatriz Santos Pires
Gabriela Cavagnoli
Gabriela Cotello
Glendha Visani
Leticia Gongora

RESUMO

Neste artigo se analisa a implementação da tecnologia de reconhecimento facial na cidade de Salvador, Bahia, explorando as suas principais implicações éticas e legais, sobretudo diante do possível viés racial na implementação e execução do projeto de segurança pública. Uma vez comprovado que tecnologias possuem o viés de quem as produz, uma sociedade construída na base de opressão e marginalização acaba por reforçar discriminações por meio dos próprios algoritmos.

ABSTRACT

This paper analyzes the implementation of video surveillance technology with facial recognition in the city of Salvador, Bahia, exploring its main ethical and legal implications, especially in the face of possible racial bias in the adoption, implementation and execution of the public safety policy. Once it is proven that technologies incorporate the bias of its creators, a society built on the basis of oppression and marginalization ends up reinforcing discriminations through the algorithms themselves.

1. INTRODUÇÃO

O videomonitoramento e o reconhecimento facial ganharam um lugar fixo nas notícias em 2019 nos protestos de Hong Kong, quando o governo local passou a utilizar a tecnologia para identificar e prender manifestantes. Apesar de distante da realidade de Hong Kong, no Brasil a tecnologia também está sendo utilizada para fins punitivistas em Estados como São Paulo, Rio de Janeiro e Bahia, sendo o último o objeto de análise do presente trabalho, que se propõe analisar a implementação da tecnologia em Salvador, Bahia, pela Secretaria de Segurança Pública local (SSP/BA).

O reconhecimento facial como parte da política pública de videomonitoramento implementada na Bahia ainda não ganhou um espaço relevante o suficiente na mídia para a conscientização da população acerca do que essa tecnologia realmente significa e como ela é utilizada. Apesar da aparência moderna, os projetos mencionados implicam em graves riscos para liberdades individuais, além de um problema sério de legalidade, transparência e publicidade. Mesmo presente no projeto o interesse público em sentido estrito - uma vez que foram realizadas prisões -, a invocação da existência de um princípio de segurança pública foi elevada a uma máxima maquiavélica de modo que não há mensuração sobre os potenciais vieses e retrocessos no plano civil que acompanham a tecnologia, como a sua predisposição a conclusões de cunho racista.

O mais grave dos problemas - e também o principal componente de análise no estudo - diz respeito à presença de vieses raciais na tecnologia. Como fruto de uma sociedade estruturalmente racista, o reconhecimento facial, quando implementado de modo inconsequente, traz consigo o problema dos falsos positivos na identificação dos indivíduos, que passam de presumidamente inocentes a alvos predeterminados do sistema.

2. O USO DE RECONHECIMENTO FACIAL EM SALVADOR

> *“ Aí foi que ele constatou que meu filho não era quem ele estava procurando, pediu desculpas ali no momento, falaram que tavam procurando duas pessoas por assalto e que meu filho foi reconhecido nas câmeras.*
> *Eu disse: ‘Como assim reconhecido? Foi reconhecido ou foi confundido, o que é muito diferente’.”* [1]

Múltiplos são os exemplos disponíveis a serem estudados em profundidade, no Brasil e no mundo, referentes ao emprego da tecnologia de reconhecimento facial como meio de promoção da segurança pública. No Brasil, o Estado da Bahia foi pioneiro na utilização da tecnologia de reconhecimento facial para fins de segurança pública através do “Projeto Vídeo-Polícia”, o que garantiu seu lugar nas manchetes. O Projeto teve dois momentos: em 2018 com o (I) Projeto Vídeo-Polícia - Mais Inteligência na Segurança; e em 2019, com o (II) Projeto Vídeo-Polícia Expansão[2].

2.1. HISTÓRICO

O projeto de videomonitoramento e reconhecimento facial na Bahia, o Projeto Vídeo-Polícia, começou oficialmente em 2018, e foi expandido entre 2020-2021. Apesar disso, seu histórico remonta ao início da década de 2010 com a preparação do Brasil para a Copa das Confederações e a Copa do Mundo FIFA Brasil, eventos internacionais em 2013 e 2014, quando foram construídas e idealizadas as principais estruturas que seriam responsáveis por seu funcionamento.

No âmbito do Ministério da Justiça, em 2011, foi criada a Secretaria Extraordinária de Segurança para Grandes Eventos (SESGE), que ficou responsável pela coordenação das atividades relacionadas à segurança pública durante os eventos. As ações da SESGE se desenvolveram na esfera nacional através do Sistema Integrado de Comando e Controle, que compreendia um conjunto de Centros

1 PALMA, Amanda; Clarissa, PACHECO. ‘O policial já foi com a arma na cabeça dele’, diz mãe de rapaz confundido por reconhecimento facial: Jovem de 25 anos estava a caminho de consulta médica e foi abordado dentro de padaria. Correio 24 horas. 05 jan. 2020. Disponível em: <https://www.correio24horas.com.br/noticia/nid/o-policial-ja-foi-com-a-arma-na-cabeca-dele-diz-mae-de-rapaz-confundido-por-reconhecimento-facial/>. Acesso em 31/05/2021.

2 Apesar do Projeto de Expansão ter começado em 2019 com a publicação do Termo de Referência, ainda não há disponível o resultado da Concorrência - aspectos que serão melhor abordados no decorrer do trabalho.

Integrados de Comando e Controle (CICCs) e Plataformas de Observação Elevado (POE), reunindo, fundamentalmente, pessoal com alto desempenho e ferramentas de inteligência e tecnologia. Na Bahia, por sua vez, a coordenação e gestão dos CICCs ficaram a cargo do Centro Integrado de Gestão de Emergências (CIGE)[3].

Criado em 2013, o CIGE foi o articulador do Parque Tecnológico na Bahia e também da construção e manutenção de nove Centros Integrados de Comunicação (CICOMs), responsáveis pela gestão e atendimento de ocorrências alertadas pelos sistemas de comunicação e videomonitoramento[4]. Com a chegada da Copa das Confederações em 2013, o CIGE passou também a fazer a cobertura e controle através do CICC, com sede provisória no próprio Parque Tecnológico. A inauguração do CICC naquele ano integrou um projeto nacional para cidades que sediaram a Copa e foi resultado de um investimento de 95 milhões de reais, dos governos federal e estadual[5], para atender a demanda de grandes eventos internacionais. Como parte do projeto, foram instaladas câmeras e computadores de bordo em mais de 80 viaturas da Polícia Militar para a transmissão em tempo real das ações policiais e facilitação da consulta do cadastro de veículos roubados, situação de condutores e mandados de prisão em aberto[6].

À época dos eventos de 2013 e 2014, as estruturas mencionadas foram essenciais ao então projeto-piloto "Vídeo-Policiamento - Mais Inteligência na Segurança", pois viabilizaram a implantação de tecnologias de videomonitoramento, incluindo a de reconhecimento facial.

Os maiores avanços para a configuração do Projeto Vídeo-Polícia se dão a partir de 2016, com a edição do Decreto nº 16.852/2016 e a instituição do Centro de Operações e Inteligência (COI) dentro da Secretaria de Segurança Pública da Bahia. Visando o fortalecimento de uma atuação mais integrada entre os órgãos, assim como a coordenação de ações táticas e operacionais dentro da SSP/BA, ele passa a se ligar aos CICOMs e, a partir daí, utilizar os sistemas de comunicação e videomonitoramento para proteção da vida e do patrimônio.

3 SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. Histórico CIGE. Disponível em: <http://www.ssp.ba.gov.br/modules/conteudo/conteudo.php?conteudo=25>. Acesso em 31/05/2021.

4 SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. Cicom. Disponível em: <http://www.ssp.ba.gov.br/modules/conteudo/conteudo.php?conteudo=65>. Acesso em 08/06/2021.

5 Inaugurado centro que vai controlar ações de segurança da Copa na BA. G1-BA, 13 jun. 2013. Disponível em: <http://g1.globo.com/bahia/noticia/2013/06/inaugurado-centro-que-vai-controlar-acoes-de-seguranca-da-copa-na-ba.html>. Acesso em 08/06/2021.

6 Viaturas da PM são equipadas com câmeras e computador de bordo. R7, 31 jul. 2014. Disponível em: <https://noticias.r7.com/bahia/viaturas-da-pm-sao-equipadas-com-cameras-e-computador-de-bordo-28082015>. Acesso em 08/06/2021.

2.2. O PROJETO "VÍDEO-POLICIAMENTO - MAIS INTELIGÊNCIA NA SEGURANÇA"

Em dezembro de 2018, o Governo do Estado da Bahia investiu 18 milhões de reais no projeto-piloto "Vídeo-Policiamento - Mais Inteligência na Segurança"[7], com objetivo de integrar um sistema de reconhecimento facial e monitoramento no Estado para fins de segurança pública[8]. Para a consolidação do projeto-piloto, a SSP/BA realizou uma prova de conceito para averiguar quais soluções estavam disponíveis e foi celebrado um aditivo no âmbito do contrato previamente estabelecido entre a SSP/BA e a empresa espanhola Informática El Corte Ingles Brasil Ltda., à época dos eventos esportivos, responsável pela tecnologia de videomonitoramento utilizada[9]. Deste modo, ao invés de realizar uma licitação apartada, uma justificativa para a assinatura do aditivo foi enviada à Secretaria-Geral do Estado permitindo que a empresa Informática El Corte Ingles Brasil trouxesse para a Bahia os equipamentos e a tecnologia da Huawei - conforme informações obtidas através de entrevista com a Secretaria de Segurança Pública da Bahia[10].

Assim, a escolhida para ser responsável pelo fornecimento da tecnologia foi a Huawei Enterprise no Brasil. Integrante da China National Biotech Group (CNBG), a empresa criada em 1987 é originária de Shenzhen, na China, e atua no ramo de tecnologia, informação e comunicação (ICT) e no desenvolvimento de infraestrutura e aparelhos de inteligência. Sua tecnologia relacionada ao reconhecimento facial é utilizada em diversos lugares do mundo, e no Brasil, além da Bahia, outra região que ganha destaque é a cidade de Campinas, no Estado de São Paulo.

Em entrevista dada pela empresa através de Rômulo Horta, diretor de Marketing da Huawei, em outubro de 2018 ao Portal Convergência Digital (CDTV)[11], explica-se que a tecnologia fornecida recebe o nome de "*VideoCloud*", e seria um "*sistema de vídeo analítico que tem capacidade de fazer reconhecimento facial, contagem de pessoas, leitura de placa de veículos*". A função primordial da tecnologia,

7 GOVERNO DO ESTADO, CASA CIVIL. Lançado sistema de videomonitoramento inteligente de segurança, 18 dez. 2018. Disponível em: <http://www.casacivil.ba.gov.br/2018/12/1271/Lancado-sistema-de-videomonitoramento-inteligente-de-seguranca.html>. Acesso em 08/06/2021.

8 HOSANA, Kelly. Vídeo Policiamento vai facilitar identificação de procurados. SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. 18 dez. 2018. Disponível em: <http://www.ssp.ba.gov.br/2018/12/4908/Video-Policiamento-vai-facilitar-identificacao-de-procurados.html>. Acesso em 31/05/2021.

9 FERREIRA, Wanise. Smart cities: Salvador e Búzios fazem pilotos de videomonitoramento inteligente. tele.síntese (terra), 17 out. 2018. Disponível em: <https://www.telesintese.com.br/smart-cities-salvador-e-buzios-fazem-pilotos-de-videomonitoramento-inteligente/>. Acesso em 31/05/2021.

10 Entrevista semi-estruturada realizada em 26 de abril de 2021. Questionário utilizado disponível em: <https://docs.google.com/document/d/1SHn5ybgVReVLfXjsgDvh3lV05QK1QU5T7NzePLIXoZs/edit?usp=sharing>.

11 PRESCOTT, Roberta; MARIANO, Rafael. Salvador integra 1900 câmeras em sistema único de segurança. Convergência Digital, 25 out. 2018. Disponível em: <https://www.google.com/url?q=https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate%3Dsite%26UserActiveTemplate%3Dmobile%26infoid%3D49299%26sid%3D18&sa=D&source=editors&ust=1623707058117000&usg=AOvVaw3lMadKyrxgrrxEFtXRyZbS>. Acesso em 31/05/2021.

conforme colocado por Rômulo Horta, seria realizar a integração entre as 1900 câmeras da SSP/BA instaladas na Rodoviária de Salvador, estações de metrô, *ferry-boat*, aeroporto de Salvador, Elevador Lacerda e nas entradas do estádio Arena Fonte Nova, e garantir que o gerenciamento possa ser feito pela SSP/BA. Comparando o caso da Bahia com o de Shenzhen (cidade que possui aproximadamente 1 milhão e 200 mil câmeras), em entrevista feita ao CDTV, Rômulo Horta explicou que o projeto integrativo do *VideoCloud* é idealizado para realizar a ponte entre câmeras do setor público e privado.

Na época de implementação, o software de integração continha dados de veículos roubados e de 65 mil pessoas com mandado de prisão expedido[12]. O sistema *VideoCloud*, por sua vez, contava com 60 terabytes disponíveis para processamento e armazenamento dos dados, e permitia a pesquisa nos bancos de dados utilizados[13] e a delimitação da trajetória de pessoas e automóveis[14].

No primeiro ano de funcionamento, o projeto-piloto ganhou o Prêmio de Sucesso na 12ª edição do 4CIO Bahia (Chief Information Officer), promovido pela Internet Technology Four[15] (IT4CIO). Assim, percebido como um sucesso pela SSP/BA, logo após seu lançamento, surgiu a demanda por uma ampliação do piloto, até então concentrado majoritariamente em Salvador. Conforme a fala do Governador Rui Costa durante o lançamento do Projeto Vídeo-Policiamento, a ideia era de que a tecnologia fosse implantada em todas as unidades de serviço público do Estado, nas escolas, SACs e unidades de saúde, com posterior disponibilização da solução para as prefeituras e iniciativa privada[16], além de ser ampliada para outras 55 cidades na Bahia além de Salvador e Feira de Santana.

12 GOVERNO DO ESTADO, CASA CIVIL. Lançado sistema de videomonitoramento inteligente de segurança, 18 dez. 2018. Disponível em: <http://www.casacivil.ba.gov.br/2018/12/1271/Lancado-sistema-de-videomonitoramento-inteligente-de-seguranca.html>. Acesso em 08/06/2021.

13 Não se sabe se o banco de dados utilizado nesta iniciativa seria o mesmo de seu projeto de expansão - pelo Banco Nacional de Mandados de Prisão, do Conselho Nacional de Justiça -, que será explicado posteriormente.

14 SSP usa reconhecimento facial para identificar criminosos em Salvador. A TARDE (UOL), 18 dez. 2018. Disponível em: <https://atarde.uol.com.br/bahia/salvador/noticias/2020477-ssp-usa-reconhecimento-facial-para-identificar-criminosos-em-salvador>. Acesso em 13/06/2021.

15 ASCOM; ANDRADE, Mariana. SSP recebe Prêmio Case de Sucesso com Reconhecimento Facial. SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. 17 set. 2019. Disponível em: <http://www.ssp.ba.gov.br/2019/09/6446/SSP-recebe-Premio-Case-de-Sucesso-com-Reconhecimento-Facial.html>. Acesso em 31/05/2021.

16 SANTOS, Gil. Bandidos serão identificados por câmeras de reconhecimento facial em Salvador: Rodoviária, metrô, ferry-boat, Fonte Nova e aeroporto começaram a usar recurso. Correio 24 horas, 18 dez. 2018. Disponível em: <https://www.correio24horas.com.br/noticia/nid/bandidos-serao-identificados-por-cameras-de-reconhecimento-facial-em-salvador/>. Acesso em 31/05/2021.

2.3. O PROJETO "VÍDEO-POLÍCIA EXPANSÃO"

Em 2019, foi emitida pela SSP/BA a primeira versão do Termo de Referência para o que foi nomeado "Projeto Vídeo-Polícia Expansão"[17]. Simplificadamente, o que se buscava era a contratação conjunta de três serviços distintos: o serviço de Monitoramento e Sustentação da infraestrutura de operações; o serviço de Ponto de Imagem; e o Serviço de Comunicação Nível Crítico com Banda Larga.

O adendo I da primeira versão do Termo de Referência, publicado em 2019, contém os diversos requisitos a serem disponibilizados pela solução, que tem como objetivo, conforme dispositivo 3.4.1.1.5, auxiliar a Superintendência de Gestão Tecnológica e Organizacional e a Superintendência de Telecomunicações no cumprimento das ações delineadas no Plano Estratégico de TI, e estender o serviço previamente implementado pelo Projeto Vídeo-Policiamento (dispositivo 3.4.1.2.2.). O documento coloca a contratante, ou seja, a SSP/BA, como a responsável pela gestão do contrato e pela aferição dos resultados esperados e níveis de qualidade exigidos (dispositivo 4.1.), e descreve o objeto da contratação no dispositivo 1.1 como:

> **" [...]** a contratação de pessoa jurídica especializada no fornecimento de serviços integrados, sob demanda, voltados a segurança eletrônica de locais de interesse com operação de primeiro nível, monitoramento, sustentação e atualização de infraestrutura de operações e provimento de comunicação móvel crítica com operação de primeiro nível, para o Centro de Operações e Inteligência (COI), para os 22 (vinte e dois) Centros Integrados de Comunicação (CICOM), todos da Secretaria de Segurança Pública, distribuídos na Capital e 58 (cinquenta e oito) municípios do Interior do Estado da Bahia. **"**

No documento, também são descritos requisitos técnicos a serem disponibilizados pelo sistema (dispositivo 6.2.1.2.8.1.3.2.), como a possibilidade de controle mínimo da contratante de alguns itens de configuração como o *hardware*, *software* e banco de dados. Um dos requisitos mais relevantes é o contido no dispositivo 6.2.1.2.8.1.8.4, que prevê que as informações sensíveis devem ter cópias de segurança atualizadas, assim como serem armazenadas em mídias criptografadas. Ainda no ponto

17 COMPRASNET-BA. Termo de Referência - Projeto Vídeo-Polícia Expansão. Disponível em: <https://comprasnet.ba.gov.br/sites/default/files/termo_de_referencia_v1.pdf>. Acesso em 24/05/2021.

6, há a referência a uma "plataforma integradora" (dispositivo 6.2.2.2), responsável por aglutinar os sistemas de TI, comunicação e o videomonitoramento, e também para servir como base de dados ao COI e aos CICOM.

Em 2020, o Município de Salvador recebeu um financiamento do Banco Interamericano de Desenvolvimento (BID) para financiar o custo do Programa Nacional de Desenvolvimento Turístico em Salvador (PRODETUR SALVADOR) no âmbito da Secretaria de Cultura da Bahia (SECULT). Assim, para o fornecimento e instalação da solução de conectividade e monitoramento, foi calculado um orçamento de mais de 14 milhões de reais, financiado por meio do Contrato de Empréstimo n. 3682/OC-BR com o BID[18]. A formalização da demanda se deu em fevereiro de 2020 com a publicação do edital da Concorrência Pública nº 02/2020, visando à contratação anteriormente especificada no Termo de Referência, e seguiu com a reabertura da Licitação Pública Nacional nº 005/2020[19] para a aquisição de solução de monitoramento para melhoria da segurança turística pelo programa PRODETUR SALVADOR através do financiamento pelo BID.

Em 2021, com o início da pandemia e a obrigatoriedade do uso de máscaras, a SSP/BA, que faz um acompanhamento das prisões efetuadas com o auxílio da tecnologia, publicou nota informando que o sistema permaneceria em uso e apenas adaptado à nova situação. Conforme a nota, houve uma adequação "[das] fórmulas matemáticas utilizadas na captação dos pontos focais de cada rosto", de forma que as câmeras focalizassem o trecho facial do nariz à testa[20].

Com isso, em pouco mais de 2 anos de funcionamento, até o início de maio de 2021, 207 cidadãos haviam sido presos com o auxílio da tecnologia de reconhecimento facial, todos procurados por crimes contra a vida ou crimes contra o patrimônio, segundo a SSP/BA[21]. Sobre as prisões, tendo em vista que a Expansão aqui examinada ainda se encontra em andamento, ou seja, com a seleção dos futuros parceiros do Estado da Bahia no fornecimento da tecnologia de reconhecimento facial, importa especificar que todas ocorreram dentro do desenvolvimento do Projeto Vídeo-Policiamento em sua versão piloto.

18 Documento disponível para consulta em PDF no site da PRODETUR: <http://www.prodeturssa.salvador.ba.gov.br/images/prodeturssa/licitacoes/LPN_0052020_-_edital.pdf>. Acesso em 08/06/2021.

19 Em agosto de 2021, foi indicado no Diário Oficial do Município que a Licitação Pública Nacional nº 005/2020 foi revogada. Tal revogação foi feita com base no art. 49 da Lei Federal n. 8.666/93 (nulidade por ilegalidade, de ofício ou por provocação de terceiros) e na Súmula n. 473 do STF (que permite a nulidade dos atos da administração quando estes tiverem vícios que os tornam ilegais).

20 ASCOM; RODRIGUES, Rafael. Reconhecimento facial completa dois anos e se adapta à pandemia. SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. 18 dez. 2020. Disponível em: <http://www.ssp.ba.gov.br/2020/12/8875/Reconhecimento-facial-completa-dois-anos-e-se-adapta-a-pandemia.html>. Acesso em 31/05/2021.

21 ASCOM; SANTANA, Marcia. Reconhecimento Facial flagra dois foragidos por tráfico de drogas. SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. 04 mai. 2021. Disponível em: <http://www.ssp.ba.gov.br/2021/05/9497/Reconhecimento-Facial-flagra-dois-foragidos-por-trafico-de-drogas.html>. Acesso em 31/05/2021.

2.4. COMO FUNCIONA A TECNOLOGIA DE VIDEOMONITORAMENTO NO PROJETO VÍDEO-POLÍCIA

Antes da contratação da Huawei, haviam mais de 1.900 câmeras em funcionamento em quatro ambientes distintos, porém não integralizados e com programas diferentes (por exemplo, CFTV e reconhecimento de placas). Por isso, foi contratado pela SSP/BA o serviço de *VideoCloud* da Huawei, uma plataforma que centraliza o gerenciamento das diferentes informações dentro da SSP/BA[22] e oferece diversos serviços - sendo provavelmente os mais importantes para a SSP/BA o processamento, coleta e armazenamento na nuvem de vídeos ao vivo[23]. Posteriormente, entre 2019 e 2020, ou seja, a partir do Termo de Referência do Projeto Vídeo-Polícia Expansão da SSP/BA e do aditivo contratual celebrado pela SSP/BA, quando ocorreu a entrada da empresa Huawei, foram compradas mais 300 câmeras e licenças para a tecnologia de reconhecimento facial.

Para o período do Carnaval de Salvador, Micareta de Feira de Santana e Festival da Virada de Salvador de 2020, foi publicada uma Solicitação de Proposta Comercial pela SSP/BA[24] para a instalação de circuito fechado de TV, CFTV e para operações de reconhecimento facial em ambientes não controlados. Nesta proposta estavam presentes requisitos para a contratação, sendo os mais importantes concernentes ao (i) tipo de câmera e aos (ii) pontos de recebimento de imagem. Sobre o (i) tipo de câmera, foi escolhida a PTZ ("*Pan*, *Tilt*, *Zoom*"), com movimentações verticais, horizontais e capacidade de aproximação da imagem, sendo ideal para o monitoramento de grandes ambientes por conta de sua versatilidade[25]. A respeito dos (ii) pontos de recebimento de imagem, foi estabelecido que estes seriam o COI, CICCM e POE.

Segundo dados do site da SSP/BA[26], a tecnologia de videomonitoramento da Huawei captaria as imagens e as transmitiria aos pontos de recebimento de imagem citados. O Centro Integrado de Comunicações do COE seria o responsável por gerar alertas e acionar equipes nas ruas para verificação da sua veracidade. Para que os alertas fossem gerados, o sistema compararia traços dos rostos das pessoas com as imagens do banco de dados selecionado, no caso, o Banco Nacional de Mandados

22 PRESCOTT, Roberta; MARIANO, Rafael. Salvador integra 1900 câmeras em sistema único de segurança. Convergência Digital, 25 out. 2018. Disponível em: <https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&UserActiveTemplate=mobile&infoid=49299&sid=18>. Acesso em 31/05/2021.

23 HUAWEI CLOUD. Video Cloud infrastructure. Disponível em: <https://www.huaweicloud.com/en-us/solution/onlinevideo/>. Acesso em 25/05/2021.

24 SSP/BA. Solicitação de proposta comercial - serviço de conectividade e ponto de imagem para eventos. Disponível em: <http://www.ssp.ba.gov.br/arquivos/File/TR_MODELO.pdf>. Acesso em 24/05/2021.

25 O que são câmeras PTZ? Merlin, 26 mar. 2019. Disponível em: <https://www.merlin.com.br/o-que-sao-cameras-ptz/>. Acesso em 25/05/2021.

26 SSP/BA. Reconhecimento facial completa um ano e é destaque nacional. Disponível em: <http://www.ssp.ba.gov.br/2019/12/6981/Reconhecimento-Facial-completa-um-ano-e-e-destaque-nacional.html>. Acesso em 24/05/2021.

de Prisão, do Conselho Nacional de Justiça (CNJ)[27]. Nos documentos disponíveis ao público, não há especificação do método empregado para tal comparação[28].

Na prática, as imagens captadas são enviadas a uma central de monitoramento da COI, onde são cruzadas com os dados de pessoas com mandado de prisão em aberto no Banco Nacional de Monitoramento de Prisões ou BNMP 2.0, desenvolvido pelo CNJ e com a Base de Registro Civil da Bahia. Segundo informações obtidas em entrevista com a SSP/BA, este segundo banco de dados é utilizado visando à concretização de uma das diretrizes do Projeto: a valorização de resultados acertados em detrimento de um alto número de alertas. Assim, há a preferência por uma base de dados menor, mas mais completa e na qual a imagem disponível seja de melhor qualidade.

Ademais, segundo a Huawei, os dados coletados são criptografados e ficam com a SSP/BA, sendo a empresa apenas responsável pela disponibilização da plataforma tecnológica (comprada pelo cliente) e instalação do equipamento.

No Adendo II do Termo de Referência do Projeto Vídeo-Polícia Expansão da SSP/BA[29], que versa sobre Condições Gerais e Técnicas do Serviço de Ponto Imagem, é feita uma distinção sobre os Pontos de Imagem (PI) das câmeras. Segundo o dispositivo 1.3., são estes: Tipo 1 - Passeio Público em rua ou avenida com suporte a análise comportamental/situacional; Tipo 2 - Pátios e praças de convivências externos com suporte a análise comportamental/situacional; Tipo 3 - Vias de circulação urbana de veículos e vias de transporte interurbano com suporte a reconhecimento de placa de veículo; Tipo 4 - Ambientes internos e externos de fluxo controlado, com suporte a reconhecimento facial; Tipo 5 - Ambientes internos e externos de fluxo livre, com suporte a reconhecimento facial; Tipo 6 - Áreas de Orla com suporte de reconhecimento de placas de veículos e análise situacional; Tipo 7 - Panorama tático urbano. Para cada um desses PIs, são descritos diferentes tipos de câmera – variando entre *speed dome*, tipo *bullet* profissional, tipo *box*, ou PTZ, dependendo do ambiente – e suas especificações (ex: zoom óptico e campo de visão mínimos), além da manutenção a ser feita.

Sobre os Tipos 1, 2 e 3 de PI, há requisitos mínimos analíticos comportamentais presentes no dispositivo 2.18., que não devem ser confundidos com o método pelo qual é feito o reconhecimento facial. São requisitos para os tipos mencionados: o Cruzamento de Linha Vertical (CLV), que gera um alerta quando uma linha desenhada na imagem é cruzada em determinado sentido; o Controle de Fluxo

27 PALMA, Amanda; PACHECO, Clarissa. Entenda como funciona o reconhecimento facial que ajudou a prender mais de 100 na BA: Câmeras estão espalhadas em várias partes de Salvador e imagens são enviadas à central da SSP. Correio 24 horas, 05 jan. 2020. Disponível em: https://www.correio24horas.com.br/noticia/nid/entenda-como-funciona-o-reconhecimento-facial-que-ajudou-a-prender-mais-de-100-na-ba/. Acesso em 31/05/2021.

28 Os métodos mais comumente utilizados para o reconhecimento facial serão aprofundados no tópico 4.1 do trabalho.

29 COMPRASNET-BA. Termo de Referência - Projeto Vídeo-Polícia Expansão, pg. 106. Disponível em: https://comprasnet.ba.gov.br/sites/default/files/termo_de_referencia_v1.pdf. Acesso em 24/05/2021.

Poligonal (CFP), que gera um alerta quando uma pré-condição de fluxo é atingida em um dos lados de um quadrilátero desenhado em tela; a Permanência em Área Designada (PAD), que gera um alerta quando um tempo pré-determinado é excedido por uma pessoa ou objeto que permanece em certa área delimitada; a Detecção de Ausência de Movimento (DAM), que gera um alerta quando não há movimento na área designada por um quadrilátero na tela por um tempo pré-determinado; os Objetos Deixados/Retirados (ODR), que gera um alerta quando um objeto é removido ou aparece em tela; a Contagem de Objeto/Pessoa (COP) que, além de fazer o que o nome indica, também identifica a saída ou entrada do objeto; a Classificação de Pessoa ou Veículo (CLS); e a Detecção de Aglomeração de Pessoas (DAP), que gera um alarme quando uma quantidade pré-determinada de pessoas for excedida em determinada área designada.

Ainda sobre os requisitos, de acordo com dados do site da SSP/BA, a similaridade das imagens capturadas pelo vídeo, em comparação com as prisões realizadas na época, variou de 81% a 98%, sendo afirmado que a polícia apenas faria abordagens quando o sistema apresentasse uma similaridade acima de 90%, dado este corroborado em entrevista do grupo com membros da SSP/BA. No entanto, vale ressaltar que há uma disparidade quando tais afirmações são comparadas com dispositivos presentes no próprio Termo de Referência do Projeto Vídeo-Polícia Expansão da SSP/BA. Isso se dá pela leitura dos requisitos mínimos comuns entre os Tipos 4 e 5 de PI para o Reconhecimento de Faces (RDF).

Segundo o dispositivo 2.19.1.1.1. do mesmo documento, o serviço de RDF deve "*Detectar, capturar e reconhecer rostos das pessoas em tempo real, considerando o respectivo cenário de captura de faces, com precisão de acerto maior que 90%, em ambientes controlados e 50% para ambientes diversos*". Ambientes controlados são aqueles onde os indivíduos que entram e saem já são registrados ou reconhecidos pelo sistema, enquanto ambientes diversos (ou seja, não regulados ou semi regulados) seriam os espaços públicos onde a maioria das pessoas não são reconhecidas pelo sistema, ou seja, por sua base de dados[30]. Quando perguntada pelo grupo acerca de tal percentual, a SSP/BA afirmou que, apesar do mínimo ser 50%, os policiais apenas abordariam as pessoas quando a similaridade fosse maior que 90%. No entanto, não há evidências que possam confirmar isso uma vez que não são registradas as abordagens policiais feitas com o uso da tecnologia, apenas as prisões de fato.

Em entrevista com representante da Huawei, foi mencionada a necessidade da utilização do fator humano - o elemento subjetivo - para suprir quaisquer erros de apontamento da tecnologia. Nesse cenário, a tecnologia diria a probabilidade de precisão e o policial realizaria uma apuração que, supostamente, seria mais precisa.

30 ADEBAYO, Olawale; DANIEL, Akpagher; GANIYU, Shefiu; OLANIYI, Olayemi. *Systematic Review of Facial Recognition Algorithms and Approaches for Crime Investigations*, In: *International Journal of Information Processing and Communication* (IJIPC), Vol. 8, No. 1. pg. 69.

2.5. FALSOS POSITIVOS

Um outro aspecto do uso da tecnologia de reconhecimento facial no decorrer do Projeto Vídeo-Policiamento é o número de falsos positivos. Tendo em vista a sensibilidade dos dados tratados com a tecnologia e o alto potencial lesivo aos direitos e à liberdade derivado do reconhecimento facial, a verificação dos falsos positivos se mostra fundamental para que possa ser feita uma análise da qualidade do Projeto.

Falsos-positivos são casos em que o reconhecimento facial falha. Nestes, o reconhecimento da imagem capturada e cruzada com o banco de dados, apesar de ser lida como uma correspondência (no presente caso, como alguém com mandado de prisão em aberto), é errôneo, ou seja, as identidades do perfil e da pessoa reconhecida são diferentes das que se buscava. No presente caso, o maior problema é a ausência dos dados relativos aos falsos positivos.

Sabe-se que o número de prisões efetuadas com o auxílio da tecnologia de reconhecimento facial é 207. Entretanto, a transparência da SSP/BA quanto aos números relativos aos Projetos acaba aí. Dados como quantas prisões erradas foram efetuadas com o auxílio da tecnologia; quantas abordagens foram motivadas pelo reconhecimento e quantos cruzamentos com similitude acima de 90% não resultaram em abordagem ou prisão não são apresentados à sociedade. E isso apenas quanto aos dados referentes aos falsos-positivos, tendo em vista que uma série de informações adicionais seriam fundamentais para o completo entendimento da execução do Projeto Vídeo-Polícia e da tecnologia de reconhecimento, como por exemplo, se o cruzamento com o banco de dados de mandados de prisão em aberto se refere somente a crimes contra a vida e o patrimônio, dentre outras.

Entretanto, a ausência de dados concretos sobre a porcentagem de falsos-positivos não impede o diagnóstico de que a tecnologia de reconhecimento facial não é infalível e pode levar a graves violações dos direitos da população baiana[31]. Exemplo disso é o caso que ocorreu em setembro de 2019 na Bahia, quando uma mãe e seu filho foram seguidos pela polícia, do metrô até uma padaria, e abordados de forma violenta após o filho, um homem de 25 anos com deficiência, ter sido reconhecido pela tecnologia como um cidadão procurado por assalto. Após apresentação dos documentos aos

31 Sobre tal afirmação importa salientar que as informações obtidas sobre falsos-positivos no âmbito do projeto Vídeo-Polícia são bastante conflitantes. Exemplo disso é a matéria que noticia o caso de falso positivo aqui detalhado, mas que também veicula uma fala do coronel Marcos Oliveira sobre a inexistência de dados referentes à falsos-positivos. Ou ainda, matéria que noticia ampliação do projeto de reconhecimento para o Pelourinho em que a SSP/BA, apesar da existência de notícias narrando falsos-positivos, afirma que não existe nenhuma ocorrência. Matérias disponíveis em: PALMA, Amanda; PACHECO, Clarissa. Entenda como funciona o reconhecimento facial que ajudou a prender mais de 100 na BA: Câmeras estão espalhadas em várias partes de Salvador e imagens são enviadas à central da SSP. Correio 24 horas, 05 jan. 2020. Disponível em: <https://www.correio24horas.com.br/noticia/nid/entenda-como-funciona-o-reconhecimento-facial-que-ajudou-a-prender-mais-de-100-na-ba/>. Acesso em 31/05/2021; e ALVES, Sarah. O Pelourinho vai ganhar câmeras de reconhecimento facial; isso é bom ou ruim? Tilt (UOL), 01 mar. 2021. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/03/01/pelourinho-vai-ganhar-cameras-de-reconhecimento-facial-isso-e-bom-ou-ruim.htm#:~:text=A%20Secretaria%20de%20Seguran%C3%A7a%20P%C3%BAblica,n%C3%A3o%20se%20trata%20da%20pessoa>. Acesso em 30/05/2021.

policiais que realizaram a abordagem e a comprovação de que o reconhecimento havia sido equivocado, mãe e filho foram liberados pela polícia, apenas com um pedido de desculpas[32].

Ainda dentro da dinâmica de números relativos à utilização da tecnologia, vale ressaltar a ocorrência de dois eventos de grande porte na Bahia, no âmbito do projeto Vídeo-Policiamento, nos quais o reconhecimento facial foi utilizado, mas onde sua eficiência e proporcionalidade podem ser amplamente questionados. O primeiro, nos quatro dias de duração da Micareta de Feira de Santana em abril de 2019, quando foram capturados mais de 1,3 milhões de rostos e houve a geração de 903 alertas pela ferramenta de reconhecimento que levaram à prisão de 15 pessoas e ao cumprimento de 18 mandados de prisão[33]. O segundo, no carnaval de Salvador, em março de 2019, quando aproximadamente 15.880 rostos precisaram ser capturados para que 361 alertas fossem gerados e apenas uma prisão fosse efetuada[34].

Quando se considera que todos os reconhecimentos realizados que não se converteram em prisão são falsos-positivos, ou seja, que apesar de terem sido reconhecidas (um alerta foi gerado) esse grande número de cidadãos não correspondia às pessoas com as quais haviam sido identificadas, é impositivo o questionamento acerca da eficiência do sistema.

Em sentido diverso, considerando a imposição feita pela SSP/BA de que a semelhança no reconhecimento seja superior à 90%, por mais que os alertas sejam gerados à partir de 50% de semelhança[35] - tendo em vista as previsões do Termo de Referência do Projeto Vídeo-Polícia Extensão -, o fato de que grande parte dos alertas não tenham resultado em prisão pode ser entendido como positivo, muito embora incapaz de indicar, por exemplo, o número de abordagens policiais realizadas.

Sobre a ausência de dados concretos sobre o número de falsos-positivos cabe uma última consideração: ainda que o fator humano não esteja presente no reconhecimento, ele permanece

32 PALMA, Amanda; Clarissa, PACHECO. 'O policial já foi com a arma na cabeça dele', diz mãe de rapaz confundido por reconhecimento facial: Jovem de 25 anos estava a caminho de consulta médica e foi abordado dentro de padaria. Correio 24 horas. 05 jan. 2020. Disponível em: <https://www.correio24horas.com.br/noticia/nid/o-policial-ja-foi-com-a-arma-na-cabeca-dele-diz-mae-de-rapaz-confundido-por-reconhecimento-facial/>. Acesso em 31/05/2021.

33 Retratos da Violência: cinco meses de monitoramento, análises e descobertas. Cinco meses de monitoramento, análises e descobertas. Rede de observatórios de segurança, 2019. Disponível em: <http://observatorioseguranca.com.br/wp-content/uploads/2019/11/1relatorio-riorede.pdf>. Acesso em 21/05/2021.

34 *Digital Transformation Process, Bahia Safe & Intelligent - Results* - Apresentação realizada pelo Governador da Bahia. Disponível p. 46-55 Inicial do MS (Processo nº 8000691-28.2021.8.05.0000).

35 Não existem dados concretos acerca das porcentagens utilizadas no Projeto Vídeo-Policiamento. Ainda que em entrevista com a SSP/BA tenha sido afirmado que as abordagens e prisões só sejam realizadas após um reconhecimento com pelo menos 90% de semelhança, não há documentação oficial (a que o grupo tenha tido acesso) com tais diretrizes. Nesse sentido, tendo em vista a discrepância entre os números obtidos nos eventos citados (Carnaval de Salvador e Micareta de Feira de Santana), pode-se entender que, ainda que sem previsão documental, já haja uma porcentagem mínima de reconhecimento realizada pelo software (no Termo de Referência do Projeto Vídeo-Polícia Expansão este valor corresponde à 50%), mas que as abordagens só sejam realizadas caso o reconhecimento atinja o valor informado pela SSP/BA.

integrando a operação como um todo. Na entrevista realizada com a SSP/BA, foi informado que - ainda que não definido na estruturação da política - o Projeto Vídeo-Policiamento é guiado por dois critérios: um objetivo, outro subjetivo. O primeiro, objetivo, se refere à tecnologia de reconhecimento facial, à configuração de alerta das câmeras, aos protocolos operacionais definidos e à base de dados utilizada. O segundo, subjetivo, compreende a interação policial. Foi explicado que após receber a informação de que o alerta foi gerado, ou seja, que foi reconhecido rosto com 90% de similitude a um perfil presente no banco de dados, a realização da abordagem pela polícia não é automática e obrigatória e depende de intervenção do próprio policial alertado.

2.6. CONTESTAÇÃO NO USO DA TECNOLOGIA

Como se pôde perceber - e será melhor enfatizado no decorrer do presente trabalho - a aplicação da tecnologia de reconhecimento facial para fins de segurança pública no âmbito dos Projetos "Vídeo-Policiamento" e "Vídeo-Polícia Expansão" levanta uma série de problemas.

Era de se esperar que fossem chamados para o debate muitos outros agentes, como o Legislativo, sociedade civil, coletivos imersos em estudos relativos à direito e tecnologia, para além dos que foram chamados, o Judiciário e Ministério Público. Dentre os chamados, nenhum contestou o design dos projetos. Segundo a SSP/BA, a ausência de oposição decorreu do fato de que tanto o Ministério Público quanto o Tribunal de Justiça foram trazidos para a prova de conceito realizada anteriormente à celebração do aditivo que viabilizou a implementação do reconhecimento facial, de forma que as instituições entendessem a importância para a segurança pública da utilização da tecnologia.

O AqualtuneLab, coletivo formado por juristas, engenheiros, cientistas políticos e sociais voltado ao estudo e litigância no âmbito de tecnologias racistas[36], tem atuado na Bahia, contestando prisões efetuadas a partir do uso desta tecnologia. Alain Amorim, advogado da organização e residente de Salvador, na Bahia, reportou a propositura de duas ações de sua autoria no âmbito do Projeto Vídeo-Polícia e seu desenvolvimento: um habeas corpus e, posteriormente, um mandado de segurança.

O *habeas corpus*[37] foi impetrado no Superior Tribunal de Justiça (STJ) em 2020, em face do Secretário de Segurança Pública do Estado da Bahia, Comandante da Polícia Militar da Bahia e Governador do Estado da Bahia. Alain Amorim se coloca como autor e paciente da ação, alegando que, por conta da ineficiência, imprecisão, inobservância de princípios e falta de reserva legal para a tecnologia, encontra-se na iminência de sofrer violência ou coação em sua liberdade de locomoção. Assim, requereu à Corte que fosse concedido liminarmente um salvo-conduto a ele até que seja editada legislação específica que garanta os princípios gerais e direitos dos titulares de dados, conforme dispõe a LGPD. Em entrevista concedida ao grupo, o autor disse que a ação foi apresentada também com a finalidade de compreender o cenário jurídico-institucional para propositura de ações mais robustas.

Indeferido liminarmente, o Ministro Joel Ilan Paciornik alegou a inexistência de flagrante ilegalidade ao direito de locomoção, assim como impossibilidade do uso do *habeas corpus* para a concessão

36 Entrevista semiestruturada realizada no dia 29 de abril de 2021 com o coletivo AqualtuneLab através de seus integrantes Arthur Almeida e Alain Amorim. Questionário utilizado disponível em: <https://docs.google.com/document/d/1Bs-PEo8n7e4i3S0zPi8gVaq4ele--GoGlhE630e0JxAY/edit?usp=sharing>.

37 BRASIL. STJ - Superior Tribunal de Justiça. Habeas Corpus nº 631298 / BA (2020/0325153-1). Impetrante: Alain Amorim. Impetrado: Governador do Estado da Bahia, Secretário de Segurança Pública do Estado da Bahia, Comandante da Polícia Militar do Estado da Bahia. Relator: Ministro Joel Ilan Paciornik. Autuado em 01 dez. 2020.

do salvo conduto, uma vez que, segundo o relator, isso feriria a finalidade do "remédio heroico"[38]. Na decisão, entendeu que a impetração do *writ* em razão da utilização da tecnologia de reconhecimento facial não implica em "constrangimento direto e concreto ao direito de ir e vir do paciente".

Em 2021, Alain Amorim impetrou um Mandado de Segurança, designando as mesmas autoridades coatoras do *habeas corpus*. O documento, especificamente em face do projeto Vídeo-Polícia Expansão, traz uma análise crítica acerca da política de vigilância, questionando a falta de legislação específica e transparência acerca da forma como se dá o tratamento dos dados sensíveis (segundo própria definição da Lei Geral de Proteção de Dados), além dos dados concernentes ao número de alertas por falsos positivos.

Um ponto interessante levantado pelo impetrante se refere à proporcionalidade entre o número de rostos capturados - e, portanto, tido como suspeitos e com direitos afetados - e o número de prisões efetuadas de fato pela tecnologia. Segundo dados retirados da propositura e já citados, dos 1,39 milhões de rostos capturados, somente 34 foram positivos. Questiona-se então a eficiência do equipamento e sua necessidade frente à interferência em direitos fundamentais e liberdades civis da população - majoritariamente negra - para a prisão de menos de 0,3% desse total.

Na ação, busca-se a suspensão do processo de reconhecimento facial e do tratamento dos dados por ele coletados, a exclusão do banco de dados formado através da tecnologia e a apresentação de relatórios de impacto[39] acerca da tecnologia em posse dos impetrados[40]. Adentrando em outras características do Projeto de reconhecimento facial, argumenta que, para além do *profiling* negro[41] que é realizado com a implantação de equipamento de reconhecimento em ambientes de grande circulação da população negra, a aplicação da tecnologia implica, ainda, numa série de ilegalidades, tendo em vista seu distanciamento de princípios da administração pública, como a legalidade, publicidade e eficiência.

38 BRASIL. Supremo Tribunal de Justiça. Decisão do habeas corpus n. 631298-BA (2020/0325153-1). Impetrante: Alain Amorim. Impetrados: Secretário de Segurança Pública do Estado da Bahia; Comandante da Polícia Militar da Bahia; e Governador do Estado da Bahia. Relator: Min. Joel Ilan Paciornik, 10 de dezembro de 2020. Disponível em: <https://processo.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=119176992&tipo_documento=documento&num_registro=202003251531&data=20201210&formato=PDF>. Acesso em 09/06/2021

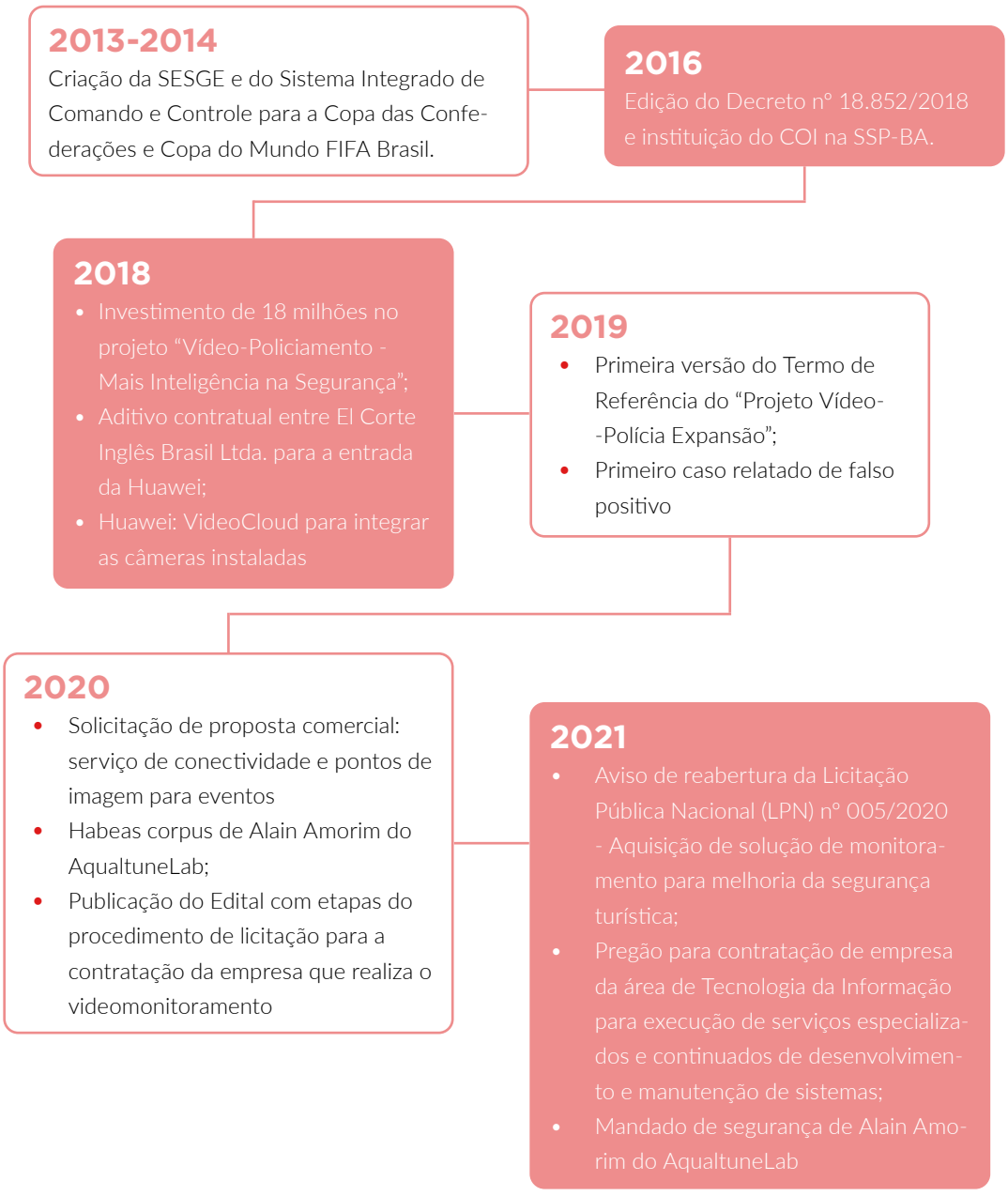
39 Em entrevista do grupo com a SSP/BA, quando questionados sobre a existência de Relatório de Impacto, foi informado que ele não é realizado. Entretanto, conforme trazido na conversa com o coletivo AqualtuneLab, os dados necessários para a consolidação de tal Relatório existem e estão em posse da SSP/BA.

40 BRASIL. Tribunal de Justiça da Bahia. Mandado de Segurança Cível. Processo nº 8000691-28.2021.8.05.0000. Impetrante: Alain Amorim. Impetrados: Secretário de Segurança Pública do Estado da Bahia, Comandante Geral da Polícia Militar do Estado da Bahia, Governador do Estado da Bahia. Relator: Des. Maurício Kertzman Szporer. Salvador (BA). 2021.

41 Em tradução livre da definição fornecida pela American Civil Liberties Union, a ideia de *profiling* negro ou *racial profiling*, se refere às práticas discriminatórias perpetradas por agentes da lei de considerarem um indivíduo criminalmente suspeito em razão da sua raça, etinicidade, religião ou nacionalidade. Maiores informações disponíveis em: <https://www.aclu.org/other/racial-profiling-definition>. Acesso em 31/05/2021.

Na decisão que indefere a liminar pleiteada, o Desembargador Maurício Kertzman adota fundamentação voltada ao fato de que não foram apresentadas provas de falha na identificação pelo sistema de reconhecimento facial adotado na Bahia. Em sentido diverso do que foi veiculado na inicial, o magistrado entende que o fato de 1,3 milhões de rostos - como no caso da Micareta de Feira de Santana de 2019 - terem sido capturados para que um procurado pela justiça fosse encontrado é indicativo da funcionalidade do sistema.

A sequência dos principais fatos narrada até este ponto pode ser observada no fluxograma (Figura 1) a seguir:



3. O RECONHECIMENTO FACIAL EM SALVADOR, BAHIA: ENTRE CONSTITUIÇÃO, LGPD E DIREITOS

> *“ Everyday people should support lawmakers, activists, and public-interest technologists in demanding transparency, equity, and accountability in the use of artificial intelligence that governs our lives. Facial recognition is increasingly penetrating our lives, but there is still time to prevent it from worsening social inequalities. To do that, we must face the coded gaze.”* [42]
>
> **JOY BUOLAMWINI**[43]

Os Projetos de reconhecimento facial expostos apresentam diversos problemas quando colocados frente-a-frente com a legislação brasileira e, uma vez que implicam tratamento de dados pessoais, é preciso avaliar sua adequação aos parâmetros legais e constitucionais. Assim, serão analisados aqui os principais: a (i) legalidade, a (ii) publicidade e transparência, a (iii) eficiência, (iv) finalidade, (v) segurança da informação e por fim a (vi) prevenção, não discriminação e responsabilização.

O art. 37, *caput*, da Constituição Federal de 1988 (CF/88) estabelece como um dos princípios basilares a (i) legalidade, ou seja, a vinculação da administração pública à normas. A tecnologia de reconhecimento facial para uso na segurança pública não possui quaisquer bases legais ou regulações e nem decorre de princípios bem delimitados, não havendo sequer justificativas acerca da necessidade da política.

Toda vinculação do Projeto à lei reside apenas nas previsões trazidas pelo Decreto nº 10.186/2006, que institui o Regimento da SSP/BA e positiva como suas competências: a programação da segurança pública do Estado, a execução de ações policiais ostensivas, preventivas, repressivas, de investigação e o policiamento do Estado, e, por fim, o mantimento de sistemas de informações estratégicas. Assim, há a determinação da competência da SSP/BA para atuar no âmbito de projetos que envolvam reconhecimento facial - sem maior estabelecimento de uma conduta específica -, porém,

42 Tradução livre: “Todas as pessoas devem apoiar legisladores, ativistas e tecnólogos de interesse público na exigência de transparência, equidade e responsabilidade no uso da inteligência artificial que governa nossas vidas. O reconhecimento facial está penetrando cada vez mais em nossas vidas, mas ainda dá tempo de prevenir o agravamento das desigualdades sociais. Para fazer isso, devemos enfrentar o olhar codificado.”.

43 BUOLAMWINI, Joy. *When the robot doesn't see dark skin*, In: Aperture, Vision & Justice, pg. 51.

há de se questionar, em que medida, essa atribuição de competência é uma autorização genérica para que a SSP/BA proceda sem qualquer gênero de guia disponibilizado ao público na condução do Projeto Vídeo-Polícia.

Conforme traz o art. 4º, inciso III, alínea 'a' da Lei Geral de Proteção de Dados (LGPD), as disposições sobre tratamento de dados pessoais impostas pela lei não se aplicam às matérias de segurança pública. Entretanto, a ausência de qualquer legislação que imponha limites e diretrizes à utilização da tecnologia e à organização do Projeto configura violação direta ao parágrafo primeiro do supracitado artigo, que postula a necessidade de legislação específica para emprego de tecnologia que atue no tratamento de dados pessoais. Nesse sentido, a ausência de uma LGPD Penal[44] não deveria obstar a criação de legislação própria que previsse "*medidas proporcionais e estritamente necessárias ao atendimento do interesse público*" quando da utilização de reconhecimento facial.

Vale ressaltar que aqui não se argumenta que a criação de tal legislação resultaria no fim de todas as problemáticas levantadas até então. No entanto, é necessário apontar, no sentido do que foi alegado na Inicial do Mandado de Segurança anteriormente apresentado, que a ausência de embasamento legal criou, o que o autor chama, de "*um Estado de exceção, sem legislação que regulamentasse o uso do equipamento tem-se um campo livre para o encarceramento em massa da população negra e seu extermínio como foco do Estado da Bahia*"[45].

Outrossim, deve-se também analisar os deveres de (ii) publicidade - positivado pelo art. 37, caput, da CF/88 - e transparência, que ditam a obrigação de publicização dos atos da administração pública. Se a SSP/BA tem grande preocupação em mostrar à sociedade em sua página institucional o número de prisões bem-sucedidas e prêmios conferidos à tecnologia, neste e nos outros portais de transparência do governo baiano, não há informações mais profundas sobre a política. Não são viabilizados, para consulta da população, dados sobre o funcionamento da tecnologia, seus riscos, benefícios e prejuízos, indicações sobre os direitos dos indivíduos que têm suas imagens capturadas ou o que fazer se forem vítimas de uma abordagem por falso-positivo, tampouco as licitações feitas e contratos celebrados. Há um problema sério de transparência e publicidade.

44 De modo geral, a LGPD Penal é um anteprojeto - portanto, ainda sujeito a emendas – que discute o tratamento de dados pessoais para fins de segurança pública e investigação criminal - contextos não contemplados pelo texto da LGPD - a fim de compatibilizar as políticas públicas com as garantias processuais, assim como os direitos fundamentais dos titulares de dados, conforme a própria exposição de motivos da lei.

45 BRASIL. Tribunal de Justiça da Bahia. Mandado de Segurança Cível. Processo nº 8000691-28.2021.8.05.0000. Impetrante: Alain Amorim. Impetrados: Secretário de Segurança Pública do Estado da Bahia, Comandante Geral da Polícia Militar do Estado da Bahia, Governador do Estado da Bahia. Relator: Des. Maurício Kertzman Szporer. Salvador (BA). 2021. p. 17 da Inicial.

Pode-se questionar a aplicabilidade de tais deveres à administração com relação às matérias de segurança pública uma vez que resta em dúvida se a vigilância massiva poderia se enquadrar no critério definido pela LGPD. Não obstante, mediante a observação do texto do Anteprojeto da LGPD Penal[46], percebe-se que o princípio recebe bastante atenção, como exposto pelo seu art. 6º, inciso VIII. Conforme trazido na Exposição de Motivos, "qualquer operação que pretenda gerar confiança acerca de sua legitimidade e integridade, acompanhada de mecanismos de supervisão e controle institucional, passa pela garantia de publicidade aos tipos, escopo e finalidades específicas de usos de dados".

Desse modo, é sabido que até o mês de maio de 2021, 207 prisões de cidadãos baianos procurados pela polícia foram realizadas com a utilização da tecnologia de reconhecimento facial pela SSP. Entretanto, não se sabe quantas mais prisões foram feitas para só então ser descoberto que o algoritmo havia errado, quantas abordagens equivocadas foram autorizadas e efetivadas mediante um reconhecimento com menos de 100% de semelhança, o que faz com que não se possa analisar a real eficácia da política.

Com a ampliação do uso da tecnologia de reconhecimento facial pela SSP para o Pelourinho, ponto turístico do centro histórico de Salvador, em reportagem feita pela Tilt UOL em comunicação com a Secretaria de Turismo e de Segurança Pública[47], foi afirmado pela pasta que as informações relativas ao Projeto são disponibilizadas no site da SSP/BA. Entretanto, seja em pesquisa no site oficial da SSP/BA, seja no Portal de Contratações e Licitações do Estado, informações primordiais ao público como qual a tecnologia utilizada, a sua origem e propriedade, os números de falsos-positivos, quais informações são recebidas pelos policiais quando há uma correspondência com o banco de dados, se há treinamento nas abordagens policiais, como os dados são processados, quais informações pessoais recebem tratamento, quão protegidas são tais informações e muitas outras, não recebem qualquer atenção.

Outro problema grave que decorre dessas informações é que não é possível encontrar dados sobre o perfil dos mandados de prisão do CNJ, e nem sobre o tamanho de tal lista. A falta de transparência faz com que não se saiba ao certo se, na base de dados, são incluídas pessoas com mandados de prisão em aberto por crimes como o pagamento da pensão alimentícia pendente ou até mesmo crianças. Ainda sobre a base de dados, não há informações sobre as imagens armazenadas, ou seja, se elas são

46 Compreende-se que o texto do Anteprojeto pode - e deve - sofrer diversas mudanças até sua aprovação e entrada em vigor, mas aqui parte-se do ponto em que algumas tendências da legislação de proteção de dados já podem ser compreendidas. Salienta-se que esse entendimento é, inclusive, o que é adotado pela SSP/BA, que, durante a entrevista realizada, se posicionaram contra o texto atual do Anteprojeto, entendendo que haveria um engessamento das políticas de segurança pública, argumentando pela necessidade de sensibilização dos legisladores quanto à inviabilidade de aplicação do esboço de lei. Mais informações em: Exposição de Motivos - Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Disponível em: <https://static.poder360.com.br/2020/11/DADOS--Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf>. Acesso em 11/06/2021.

47 ALVES, Sarah. O Pelourinho vai ganhar câmeras de reconhecimento facial; isso é bom ou ruim? Tilt (UOL), 01 mar. 2021. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/03/01/pelourinho-vai-ganhar-cameras-de-reconhecimento-facial-isso-e-bom--ou-ruim.htm#:~:text=A%20Secretaria%20de%20Seguran%C3%A7a%20P%C3%BAblica,n%C3%A3o%20se%20trata%20da%20pessoa>. Acesso em 30/05/2021.

ideais para serem usadas na tecnologia por conta de sua qualidade, por quanto tempo são guardadas, em que sistema são armazenadas, como são processadas e exatamente quem tem acesso a elas.

Ainda quanto à necessidade de transparência como meio de garantir a legitimidade e integridade da política, na mesma reportagem, quando questionada acerca dos casos de falsos positivos, a Secretaria informou que não havia nenhum. O confronto de tais alegações com a notícia anteriormente apresentada, que relata ocorrência de falso-positivo, leva ao questionamento da veracidade das informações prestadas pela SSP/BA. Se em situações de normalidade esses tipos de incongruência não seriam aceitáveis do ponto de vista administrativo, quando se pensa no desenvolvimento de uma política pública de alto impacto nos direitos individuais, sem qualquer tipo de oposição institucional, percebe-se a obstrução de todo e qualquer controle que a sociedade - em especial os grupos marginalizados mais afetados pelo Projeto - poderia exercer sob a política de reconhecimento facial do governo da Bahia.

Sobre a (iii) eficiência, além dos elementos já demonstrados[48], vale examinar o custo-efetividade da tecnologia. Apesar de não haver documentos suficientes para que possa ser averiguado com profundidade os gastos feitos com a contratação e os resultados obtidos, pode-se listar, de modo geral, as condições necessárias para a implementação da política e como afetam o seu custo final. No desenvolvimento de uma tecnologia de reconhecimento facial, há diversas variáveis a serem consideradas a fim de que esta atinja os resultados almejados e não fira direitos fundamentais, como, por exemplo: alta precisão de acerto (acima de 90%); pessoal especializado para analisar a empresa contratada, observar como se dá o processo de reconhecimento facial para constatar se ele é o mais adequado dado o contexto sócio-cultural do local e realizar relatórios de impacto; treinamento específico dos policiais para que estes aprendam a manusear o equipamento e realizar abordagens corretas; entre outros. O que podemos observar é que, para a implementação correta e ética da tecnologia, há diversos custos extras a serem considerados, que podem não compensar se comparados aos resultados atingidos.

Ademais, para além de um olhar macro voltado à Constituição, é interessante enfatizar alguns aspectos que entendemos essenciais quando se fala do tratamento de dados pessoais. Comparando a Lei Geral de Proteção de Dados com o Anteprojeto da LGPD Penal, há elementos comuns que demonstram uma preocupação geral, dos legisladores e juristas, dentro da matéria: a finalidade, segurança da informação e colaboração com entes privados, prevenção e outros diversos - desconsiderando aqueles que, de algum modo, ratificam os déficits já positivados, como a licitude, livre acesso e transparência.

O primeiro, a (iv) finalidade, elenca a necessidade de que o tratamento dos dados seja feito visando propósitos legítimos e específicos. Em conversa com a SSP/BA, foi colocado de modo bastante claro pelos entrevistados que o objetivo final da utilização da tecnologia é a preservação da ordem

48 Como, por exemplo, funciona a tecnologia, e qual o percentual de falsos positivos.

pública e a incolumidade das pessoas e do patrimônio. Entretanto, é inviável considerar o objetivo e metas traçadas desvinculadas da realidade e dos efeitos perversos que a persecução da finalidade exposta pode trazer - em específico sobre grupos marginalizados, conforme vai se argumentar. A finalidade e a proporcionalidade não podem ser apartadas na análise do caso de Salvador, Bahia.

O segundo elemento, referente à (v) segurança da informação, é particularmente interessante no Projeto Vídeo-Policiamento quando relembrado que se trata do manejo de dados sensíveis, envolvendo o sistema de justiça criminal, realizado por empresa e tecnologia estrangeira. O *VideoCloud*, conforme apresentado, é uma nuvem de origem internacional. Ainda que, em entrevista realizada com a Huawei[49], a informação obtida seja de que as imagens derivadas do reconhecimento facial não podem ser "abertas", sendo criptografadas, e de que todos os dados utilizados no Projeto ficam com a SSP/BA, a ausência de transparência quanto à parceria levanta questões sobre a efetiva segurança dessas informações. Sabe-se apenas que os dados biométricos são criptografados, mas, não há informações sobre como tal encriptação é feita, nem sobre como e por quem ela pode ser lida.

49 Entrevista semiestruturada realizada no dia 26 de abril de 2021 com a Huawei Brasil através de Ricardo Mansano. Questionário utilizado disponível em: <https://docs.google.com/document/d/1lDrlfhlk4ATN4BMj7WfOnBdtgMv5GUVYlZ8Dye2a4pc/edit?usp=sharing>.

Um ponto interessante sobre o assunto está presente na justificativa de contratação (dispositivo 3) do Termo de Referência para o "Projeto Vídeo-Polícia Expansão" previamente citado. Neste, lê-se:

> **"** 3.3.5. Portanto, optou-se por uma **contratação integrada de infraestrutura**, onde, uma única empresa ou empresas consorciadas especializadas na gestão de atividade de apoio, comunicação e infraestrutura, comprovadamente capacitada para tal serviço integrará em um único contrato todos os seguimentos de manutenção de forma a cumprir os níveis de qualidade exigidos, através de Níveis de Acordo de Serviços, ou SLA (Service Level Agreement), hoje muito utilizado por empresas em contrato de gestão, cuja característica principal se dá justamente pela **desvinculação da contratação de mão de obra, uma vez que na qualidade de CONTRATANTE a Administração Pública, limita-se apenas a fiscalizar a qualidade, eficiência e prestabilidade do referido serviço.**
> **[...]**
> 3.3.8. Ou seja, **a CONTRATANTE** com o monitoramento em tempo real dos serviços realizados, chamadas atendidas, correção dos defeitos, presteza e conformidade exigida, **não precisa se preocupar com a "forma" que a CONTRATADA prestou**, uma vez mesma[50] tem interesse em mensurar adequadamente o trabalho prestado e equipamento necessário ao cumprimento do mesmo.**"** (grifo nosso).

Tal cláusula se mostra problemática ao nos depararmos com a afirmação de que a contratante (ora SSP/BA) não seria responsável pela forma pela qual o serviço é prestado pela contratada por se tratar de uma contratação integrada. A falta de clareza em tal dispositivo no que tange não apenas a gramática, como também a falta de especificidade sobre o que seria a tal "forma"[51], faz com que o mesmo seja perigoso quando se fala da proteção de direitos fundamentais, uma vez que o que a

50 A cláusula foi copiada exatamente do jeito que foi escrita no Termo de Referência. Infere-se que a frase originalmente pretendida seja "(...) que a CONTRATADA prestou, uma vez que a mesma tem interesse (...)".

51 Por exemplo: a "forma" se refere à contratação de empresas pela contratada para quais fases da implementação do projeto? Todas elas?; a "forma" se refere apenas no que tange a contratação das empresas?

tecnologia capta - e portanto, a tecnologia em si lida - são dados sensíveis da população segundo a LGPD, e devem ser tratados com cuidado.

Por fim, quanto à (vi) prevenção, não discriminação e responsabilização, respectivamente incisos X, XI e XII do art. 6º do Anteprojeto da LGPD Penal, residem neles o enfoque do presente projeto. Ocorre que, quando se usa um algoritmo essencialmente racista para o tratamento de dados pessoais, em específico na utilização de uma tecnologia de reconhecimento facial, o resultado será a automatização da discriminação. Apesar da grande problemática, não foram achados pareceres, consultas ou documentos que mostram ter havido preocupação da Secretaria com essas questões.

Positivados os principais aspectos e eventos acerca da implementação da tecnologia de reconhecimento facial na Bahia, as controvérsias e fragilidades presentes nos Projetos, resta um aprofundamento em dois aspectos do tema proposto. Desse modo, seguem à esse tópico, uma análise mais detalhada de tecnologias de videomonitoramento e reconhecimento facial para que, então, possamos verificar a tese de que essas tecnologias, em razão dos vieses que carregam, fundamentalmente através de seus algoritmos, auxiliam na perpetuação do racismo.

4. A TECNOLOGIA DE VIDEOMONITORAMENTO E O RECONHECIMENTO FACIAL É RACISTA?

> *“ If you’re thinking about data and artificial intelligence, in many ways data is destiny. Data is what we’re using to teach machines how to learn different kinds of patterns. So if you have largely skewed data sets that are being used to train these systems, you can also have skewed results. So this is when you think of AI, it’s forward looking, but AI is based on data and data is a reflection of our history. The past dwells within our algorithms.”* [52]
>
> **JOY BUOLAMWINI**[53]

Na visão de Joy Buolamwini, uma das principais ativistas na conscientização acerca de tecnologias de reconhecimento facial, essas podem ser definidas como o conjunto de ferramentas digitais usadas para realizar tarefas em imagens ou vídeos de rostos humanos[54]. Para além da detecção de um rosto humano na imagem, os *softwares* de reconhecimento facial podem realizar a classificação de atributos do rosto, como a distinção entre as diferentes categorias de gênero, raça ou etnia. Podem estimar números, como no caso da idade de um indivíduo, utilizando-se de atributos faciais e realizar a detecção de atributos nos rostos identificados que servem à diferenciação entre eles, como a localização de acessórios, cicatrizes, barbas e bigodes.

4.1. COMO FUNCIONA O RECONHECIMENTO FACIAL NAS TECNOLOGIAS DE VIDEOMONITORAMENTO

O rosto, assim como nossas impressões digitais, compõe o que a ciência chama de biometria; dados específicos e únicos que variam de indivíduo para indivíduo. Assim, do mesmo jeito que as pessoas podem ser identificadas por meio de suas impressões digitais, elas também podem ser iden-

52 Tradução livre: “Se você está pensando em dados e inteligência artificial, de várias maneiras os dados são o destino. Dados são o que estamos usando para ensinar as máquinas a aprender diferentes tipos de padrões. Portanto, se você distorce amplamente os conjuntos de dados que estão sendo usados para treinar esses sistemas, você também pode ter distorcido seus resultados. Então, quando você pensa em inteligência artificial, olha-se para o futuro, mas a inteligência artificial é baseada em dados, e os dados são um reflexo da nossa história. O passado reside em nossos algoritmos.”.

53 BUOLAMWINI, Joy. *Facial Recognition Technologies: A Primer*, In: Algorithmic Justice League, pg. 2.

54 KANTAYYA, Shalini. *Educational Discussion Guide*, In: Coded Bias, pg. 10.

tificadas pelo registro certo de seus rostos. É com base nessa premissa que surgem os *softwares* de reconhecimento facial[55].

Antes que o reconhecimento facial ocorra de fato, o *software* (i) recebe imagens de criminosos de diferentes fontes, para depois (ii) detectar, extrair e armazenar tais fotos em uma base de dados a fim de que (iii) o algoritmo seja treinado. Uma vez que isso é feito, (iv) o *software* recebe imagens das câmeras de videomonitoramento e as comparam com a base de dados citada para que sejam reconhecidas correspondências[56]. Para que sejam feitas estas correspondências, há duas etapas após o recebimento das imagens das câmeras de videomonitoramento: a (v) aquisição e o (vi) processamento das imagens. A aquisição é responsável por transformar as imagens em formatos digitais, e é nela também que são detectados em que parte da imagem estão presentes os rostos para que possam ser posteriormente processados. Assim, por sua vez, o processamento das imagens consiste nas atividades feitas pelo *software* utilizado para eliminar defeitos de imagem, tais quais a iluminação e foco indevido. Em seguida, dos rostos coletados e devidamente processados, são retiradas suas partes mais importantes para o reconhecimento e tal escolha é feita com base no algoritmo utilizado[57].

Após esse processo preliminar, o software passa de fato a tentar (vii) identificar o rosto apresentado. De modo geral, as técnicas para o reconhecimento facial consistem na comparação dos rostos coletados com os já existentes em uma base de dados vinculada ao programa. Para tal, existem diversos métodos, sendo os mais famosos: o *Principal Component Analysis* (PCA), que se utiliza de medidas chamadas de *Eigenvectors e Eigenfaces*; os *Local Binary Patterns Histograms* (LBPH), que convertem a imagem em uma escala de cinzentos; a *Convolutional Neural Network* (CNN), que reconhece rostos por meio da aplicação de zooms em partes específicas das imagens, usando redes de pixels cada vez menores, chamadas de *kernels*; e, por fim, o método Viola Jones, que se utiliza de *Haar Figures*, formas retangulares que identificam padrões em comum nas fotos comparadas, caído em desuso atualmente[58].

Uma vez que todas as etapas são perpassadas, (viii) as autoridades são notificadas para que possa ser feita a prisão do indivíduo.

55 O presente tópico será explicado com base no seguinte artigo acadêmico: ADEBAYO, Olawale; DANIEL, Akpagher; GANIYU, Shefiu; OLANIYI, Olayemi. *Systematic Review of Facial Recognition Algorithms and Approaches for Crime Investigations*, In: *International Journal of Information Processing and Communication* (IJIPC), Vol. 8, No. 1.

56 Ibidem, p. 64.

57 Ibidem, p. 69.

58 Os dois últimos métodos foram retirados da obra: LESLIE, David. *Understanding bias in facial recognition technologies*, In: *The Alan Turing Institute, Public Policy Programme*, pgs. 9-11.

4.2. HISTÓRICO DO VIDEOMONITORAMENTO: A FOTOGRAFIA E SEUS VIESES INCONSCIENTES

A fotografia é, como sua tradução no grego (*phōtographia*) implica, a escrita por meio da luz[59]. É por ela que os fotógrafos regulam tons e os registros são feitos. Para tal, as câmeras possuem dois modos gerais de utilização, o manual e o automático. No manual, o fotógrafo tem liberdade para balancear configurações como a quantidade de luz que entra no instrumento, a velocidade com que isso ocorre e a sensibilidade da lente. No entanto, este modo é normalmente usado apenas por fotógrafos profissionais, uma vez que pede por técnicas específicas, como a fotometria, que permite medir a luz e calcular todas as variações presentes no cenário a fim de que a foto capture a imagem que o fotógrafo pretende, ou seja, o que na visão dele, seria o ideal. O modo automático, entretanto, atua de forma diferente. Este calcula sozinho as configurações que devem ser usadas a fim de que a imagem fique "ideal" e a tendência de acordo com a qual ele toma essa decisão afeta gravemente as pessoas com a coloração de pele escura, uma vez que o padrão para as fotos é o tom de pele claro, um legado histórico da fotografia.

Inventada em meados do século XIX na França, a fotografia consistia numa série de processos químicos relacionados a aspectos como cor, nitidez e contraste da foto para que, enfim, essa fosse revelada. No entanto, as fotos eram apenas tiradas para registrar membros da elite, uma vez que este era o mercado almejado, o que fez com que a invenção se tornasse um retrato de apenas uma pequena fração da sociedade da época. Os fotógrafos priorizavam a captura de fotos de pessoas brancas, tornando este o padrão mesmo com o desenvolvimento da tecnologia, o que fez com que as configurações da câmera não fossem, por muito tempo, sensíveis a pessoas negras, por exemplo. Tal fenômeno, é chamado por estudiosos da área de "*flesh tone imperialism*" e consiste no inconsciente da tecnologia em reconhecer tons de pele que não sejam o branco como não-padrões. Sobre essa questão, cita-se:

59 Etimologia de fotografia. Etimologia, 2019. Disponível em: <https://etimologia.com.br/fotografia/>. Acesso em 15/06/2021.

> *“ Problems for the African-American community, for example, have included reproduction of facial images without details, lighting challenges, and ashen-looking facial skin colours contrasted strikingly with the whites of eyes and teeth. From a more technical perspective, evidence has been accumulating that the reason for these deficiencies is that film chemistry, photo lab procedures, video screen colour balancing practices, and digital cameras in general were originally developed with a global assumption of “Whiteness” embedded within their architectures and expected ensemble of practices.”* [60]

Nessa linha, pode-se afirmar que há um viés inconsciente construído na fotografia uma vez que o padrão é visto como o tom de pele claro, enquanto outros tipos de pele precisam de correções manuais[61]. Um exemplo dado na obra acerca do porquê desse viés é o *Shirley Card*. Criado pela Kodak no século XX, o *Shirley Card* era uma foto de uma mulher branca que locais de revelação de fotos usavam como medida para a calibração das cores, luz, sombras etc. Como se vê, tal calibração, por ser feita a partir da foto de uma mulher branca, não era ideal para pessoas com outros tons de pele, que tinham suas fotografias menos nítidas.O *Shirley Card* original foi abandonado em detrimento de outros modelos que permitiam que houvesse maior diversidade[62]. No entanto, apesar do *Shirley Card* não ser mais utilizado, o viés racial continua priorizando configurações de luz para pessoas com pele mais clara.

Assim, a história da fotografia apresenta-se como mais um elemento que revela o racismo estrutural institucionalizado em diversas esferas de nossas vidas, tema a ser aprofundado adiante em nosso trabalho. Algoritmos são “opiniões incorporadas no código”[63] e, nesse sentido, vale pontuar a passagem:

60 ROTH, Lorna. *Looking at Shirley, the Ultimate Norm: Colour Balance, Image Technologies, and Cognitive Equity*, In: *Canadian Journal of Communication*, Vol. 34, pg. 117.

61 LEWIS, Sarah. *Racial Bias and the Lens*, In: *Aperture, Vision & Justice*, pg. 54.

62 Vale ressaltar que tal mudança foi feita em decorrência de protestos de lojas que queriam vender produtos de cores além das claras, e não por conta de um cuidado ou atenção com pessoas com outros tons de pele.

63 O’NEIL, Cathy. *Weapons of Mass Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Broadway Books, 2016.

> “ Como vemos o mundo e escolhemos representá-lo se reflete nos modelos algorítmicos do mundo que construímos. As ferramentas que construímos necessariamente incorporam, refletem e perpetuam estereótipos sociais e culturais e suposições inquestionáveis.” [64]

A partir do exposto, é inegável que a apresentação dessas tecnologias e o público ao qual são destinadas tornam-se parte de um panorama maior que envolve uma sociedade preconceituosa e excludente. Assim, demonstrada a natureza discriminatória inerente ao instrumento elementar através do qual se realiza o reconhecimento facial, faz-se necessário entender como se dá a manutenção e legitimação da exclusão na sociedade. A subjetividade dos programadores, socializados numa realidade racista, une-se aos problemas objetivos encontrados já nas câmeras de monitoramento utilizadas na criação de uma vigilância enviesada, na qual os alvos do sistema são predeterminados.

64 SILVA, Tarcízio. Comunidades, Algoritmos e Ativismos Digitais: Olhares Afro Diaspóricos, pg. 176.

5. POPULAÇÕES MARGINALIZADAS E TECNOLOGIAS DE REPRESSÃO

> *“ O exercício da disciplina supõe um dispositivo que obrigue pelo jogo do olhar; um aparelho onde as técnicas que permitem ver induzam a efeitos de poder, e onde, em troca, os meios de coerção tornem claramente visíveis aqueles sobre quem se aplicam. ”*
>
> **MICHEL FOUCAULT**[65]

Tendo em mente os tópicos acima abordados, tanto com relação às finalidades para as quais as câmeras de videomonitoramento e reconhecimento facial são utilizadas, quanto aos meios utilizados para a construção das máquinas fotográficas, aproxima-se uma reflexão acerca de como o uso dessas tecnologias reverbera para aqueles que se encontram às margens da sociedade. Quando trazemos o recorte brasileiro ao estudo dessa tecnologia, é possível analisar falhas que podem surgir a partir de como se estrutura a população brasileira, já que 54% se autodeclara como preta ou parda[66], formando assim uma maioria negra.

A partir desse dado, se contamos com um software que não foi desenvolvido para reconhecer o rosto negro e suas nuances, podemos identificar problemas como (i) a imprecisão no reconhecimento de pessoas negras, (ii) falsos-positivos que apontariam pessoas com características físicas semelhantes àquelas da pessoa procurada, (iii) situações de grande constrangimento para aqueles abordados por conta do apontamento do software, ainda que sejam completamente inocentes e a (iv) prisão infundada daqueles que, por quaisquer motivos, não possam se identificar como não sendo a pessoa procurada.

Ademais, a localização dessas câmeras é capaz de traduzir qual parcela da população está sendo primordialmente fiscalizada. Se a maioria da população é negra e pobre[67], em uma linha de raciocínio lógica, é possível inferir que essa população é a que mais se locomove de transporte público e habita as

65 FOUCAULT, Michel. Vigiar e punir: história da violência nas prisões. 27. ed. Petrópolis: Vozes, 1987. Terceira parte, Cap. II: os recursos para o bom adestramento. p. 143 - 161.

66 Desigualdades sociais por cor ou raça no Brasil. IBGE - Instituto Brasileiro de Geografia e Estatística. Rio de Janeiro, 2019. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101681_informativo.pdf>. Acesso em 20/05/2021.

67 Desigualdades sociais por cor ou raça no Brasil. IBGE - Instituto Brasileiro de Geografia e Estatística Rio de Janeiro, 2019. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101681_informativo.pdf>. Acesso 20/05.2021.

áreas periféricas da cidade. Dessa maneira, ao posicionar essa tecnologia nos locais de maior circulação de pessoas marginalizadas, não só negros e pobres, mas também, por exemplo, pessoas em situação de rua, é nítido um juízo de valor anterior à abordagem policial em si.

O tema de populações marginalizadas e do desenvolvimento de tecnologias utilizadas para a sua vigilância não é novo para a academia e, com a quantidade de novos *softwares* e equipamentos sendo utilizados para essa finalidade, vem sendo cada vez mais discutido. Os modos como essas tecnologias são aplicadas como instrumentos de repressão social de grupos marginalizados serão demonstrados a seguir.

5.1. ALVOS PREDETERMINADOS: RAÇA E TERRITORIALIDADE

A vigilância é uma engrenagem específica da disciplina de poder. Essa é a tese elementar proposta por Foucault, vastamente utilizada para abordar o racional que ampara o progressivo desenvolvimento de mecanismos que monitoram o comportamento individual com precisão cada vez maior. Nesse cenário, os sistemas de reconhecimento facial são mais um passo no sentido do que o autor enunciou como o aparelho disciplinar perfeito, aquele que capacitaria a um único olhar para tudo ver permanentemente, especificando a vigilância e tornando-a funcional[68].

A implementação de um sistema de reconhecimento facial no Estado da Bahia requer atenção a duas problemáticas centrais, que apesar da profunda intersecção, devem ser analisadas em separado. A primeira diz respeito à questão racial, já que no Brasil, as abordagens e prisões, que incidiram sobre pessoas negras mais de 90% das vezes[69], foram motivadas pelo mesmo sistema que, no carnaval de 2019, na Micareta de Feira de Santana, emitiu 903 alertas, dos quais, 870 eram falsos-positivos, mais de 96% do total[70]. Outro problema concerne a territorialidade da vigilância, isto é, os lugares onde estão instaladas as câmeras com inteligência para realizar o reconhecimento. Como demonstra o caso brasileiro, a tecnologia é estrategicamente posicionada no transporte público, centros comerciais e nos locais com maior circulação de pessoas. A questão a ser enfrentada é qual o perfil da população que frequenta cotidianamente esses espaços.

Em 2019, o Brasil já contava com 37 iniciativas de cidades adotando tecnologias de reconhecimento facial, concentradas majoritariamente na área de transportes. A principal justificativa para a implementação do sistema no transporte coletivo é a fiscalização do uso de cartões de gratuidade e meia-passagem[71]. No dia 18 de maio de 2021, o governador da Bahia, Rui Costa, anunciou a instalação de câmeras dotadas do sistema de reconhecimento facial em ônibus de 70 cidades do Estado. A preocupação do governador não prima evitar prejuízo à arrecadação do valor das passagens, mas sim combater assaltos nos coletivos, motivo pelo qual, segundo ele, as cidades contempladas pela tecnologia "serão escolhidas levando em conta o mapa da violência, priorizando os lugares de maior incidência de violência"[72].

68 FOUCAULT, Michel. Vigiar e punir: história da violência nas prisões. 27. ed. Petrópolis: Vozes, 1987. Terceira parte, Cap. II: os recursos para o bom adestramento. p. 143 - 161.

69 O algoritmo e racismo nosso de cada dia. Revista Piauí, 02 jan. 2021. Disponível em: <https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia/>. Acesso 24/05/2021.

70 Retratos da Violência: cinco meses de monitoramento, análises e descobertas. Cinco meses de monitoramento, análises e descobertas. Rede de observatórios de segurança, 2019. Disponível em: <http://observatorioseguranca.com.br/wp-content/uploads/2019/11/1relatoriorede.pdf>. Acesso 24/05.2021.

71 Biometria facial começa a ser implantada nos ônibus de Belém a partir desta segunda, 14. G1-PA, 14 out. 2019. Disponível em: <https://g1.globo.com/pa/para/noticia/2019/10/14/biometria-facial-comeca-a-ser-implantada-nos-onibus-de-belem-a-partir-desta-segunda-14.ghtml>. Acesso 24/05/2021.

72 Governo da Bahia vai instalar câmeras com reconhecimento facial em ônibus de 70 cidades para combater assaltos. Diário do Trans-

O mais recente estudo de Origem e Destino[73] do metrô da capital de São Paulo embasa os apontamentos de pesquisadores da mobilidade urbana, como o professor do Instituto das Cidades da Unifesp, Kazuo Nakano. Segundo ele, são os trabalhadores periféricos e de baixa renda os que dependem do uso de ônibus, trem e metrô para a sua locomoção[74]. Nesse cenário, levando em consideração as condições precárias do transporte público brasileiro que fazem com que as classes mais altas recorram, via de regra, ao transporte particular, é possível enxergar com clareza o delineamento de um perfil específico da população alvejado pela implementação do reconhecimento facial no transporte coletivo. Assim, a população periférica e de baixa renda, composta majoritariamente por pessoas negras[75], é colocada desde logo como aquela a qual se interessa vigiar.

Simultaneamente, centros comerciais e pontos turísticos das grandes metrópoles são progressivamente alimentados pela tecnologia. Em fevereiro deste ano, a prefeitura de Salvador anunciou a instalação de câmeras de reconhecimento facial no Pelourinho, centro histórico e um dos principais pontos turísticos da capital baiana. Nas palavras do secretário Municipal de Cultura e Turismo, Fábio Mota, o objetivo é "criar um verdadeiro *Big Brother* do bem para auxiliar a gestão e dar segurança"[76].

Apesar da falsa impressão de democratização da vigilância, um olhar mais atento descobre a diferença nas motivações para a implementação do sistema nos espaços ocupados pelas classes mais baixas e naqueles dominados pelas elites. A antropóloga Teresa Caldeiras centraliza a sua tese no reconhecimento de padrões de diferenciação social e de separação nas regras que organizam o espaço urbano. Para a autora, as formas de relacionamento urbano teriam sofrido transformações ao longo da década de 90, marcadas pela proximidade entre grupos heterogêneos que, no entanto, estão cada vez mais separados socialmente. Nessa nova proximidade espacial, as desigualdades tornam-se mais explícitas e violentas, aumentando a tensão e levando aqueles que se sentem ameaçados pelo medo do crime e da violência a abandonarem os espaços públicos e recolherem-se a espaços privatizados, fechados e monitorados, o que a autora denomina "enclaves fortificados"[77].

porte, 19 mai. 2021. Disponível em: <https://diariodotransporte.com.br/2021/05/19/governo-da-bahia-vai-instalar-cameras-com-reconhecimento-facial-em-onibus-de-70-cidades-para-combater-assaltos/>. Acesso 24/05/2021.

73 Pesquisa origem e destino: 50 ANOS. Metrô de São Paulo, 2017. Disponível em: <http://www.metro.sp.gov.br/pesquisa-od/pesquisa-od-50-anos.aspx>. Acesso 24/05/2021.

74 Covid mata mais entre trabalhadores que dependem do transporte coletivo. Brasil de fato, 18 ago. 2020. Disponível em: <https://www.brasildefato.com.br/2020/08/18/covid-mata-mais-entre-trabalhadores-que-dependem-do-transporte-coletivo>. Acesso 24/05/2021.

75 IBGE: negros são 17% dos mais ricos e três quartos da população mais pobre. Agência Brasil, 02 dez. 2016. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2016-12/ibge-negros-sao-17-dos-mais-ricos-e-tres-quartos-da-populacao-mais-pobre>. Acesso 24/05/2021.

76 'BBB no Pelô': Prefeitura vai implantar reconhecimento facial no Centro Histórico. Correio 24 horas, 02 fev. 2021. Disponível em: https://www.correio24horas.com.br/noticia/nid/bbb-no-pelo-prefeitura-vai-implantar-reconhecimento-facial-no-centro-historico. Acesso 24/05/2021.

77 AUGUSTO, Maria Helena Oliva. Segregação social e violência urbana. *Revista brasileira de ciências sociais*. Vol. 17, N. 48. 2002.

Nesse cenário, a implementação de sistemas de monitoramento nos locais de circulação de turistas e da parcela privilegiada da população presta-se justamente a incrementar a sensação de segurança entre a elite que, temerosa pelo compartilhamento dos espaços públicos com as classes marginalizadas, fecha-se em espaços privados e demanda por mais segurança nas ruas.

O que se observa, portanto, é que enquanto no transporte público e bairros periféricos o reconhecimento facial atua como um cão farejador que intenciona localizar procurados pela polícia, o que se depreende pelo uso do banco nacional de dados do CNJ como base de dados para o funcionamento do *software*, nas regiões abastadas das cidades, ele é usado como um guardião do bem estar dos seus habitantes, objetivando evitar os inconvenientes causados pelos "invasores". Nesse sentido, prevalece o que Teresa Caldeira chamou de "criminalização simbólica", traduzida na naturalização da periculosidade de certos grupos[78].

78 AUGUSTO, Maria Helena Oliva. Segregação social e violência urbana. *Revista brasileira de ciências sociais*. Vol. 17, N. 48. 2002.

5.2. DOMINAÇÃO PELA ESTIGMATIZAÇÃO

O uso da tecnologia na esfera social frequentemente concentra-se em práticas punitivas, seja para prever quem cometerá um crime ou para encontrar alguém que já o cometeu. Conforme demonstrado, os elementos racial e de classe estão, por vezes, sobrepostos na construção da parcela populacional que se pretende vigiar com os sistemas de monitoramento extensivo. A discriminação racial herdada de um passado colonial conjuga-se à estratificação social na composição da camada mais vulnerável da população, relegada às periferias, dependente do transporte público e principal alvo das abordagens policiais. Assim, o imaginário sociocultural que atribui à cor da pele e à classe um determinado comportamento resulta numa condenação prévia; antes mesmo de serem abordados, pretos e pobres já foram condenados e relegados às margens.

Ainda, apesar de coincidirem grande parte do tempo, os critérios para a seleção dos "delinquentes em potencial" também atuam separadamente. Nesse sentido, a cor da pele opera uma diferenciação automática, que recai na estigmatização fabricada sobre os corpos negros, enquanto a baixa renda de pessoas brancas pode incluí-las no rol de vigiados. Assim, desenvolvimentos tecnológicos aplicados com o objetivo de resguardar a segurança pública, inevitavelmente, são acompanhados de julgamentos sociais que culminam em práticas cruéis e discriminatórias para alguns indivíduos[79].

No que tange a estigmatização da população não branca, nos serve a concepção foucaultiana das estruturas de poder como estratégias globais que utilizam táticas locais de dominação a partir de uma multiplicidade de sujeições. Apesar de difundidos em diversos países ao redor do mundo, os sistemas de reconhecimento facial nunca passaram isentos de questionamento. Essa desconfiança é pautada na ideia de que a tecnologia, capaz de rastrear os passos de um indivíduo na sua convivência social cotidiana, não é imparcial na qualificação das condutas dos referidos conforme os padrões do que se considera melhor ou pior, certo ou errado, inocente ou culpado. Aparte a sua atuação enquanto condicionante do comportamento dos indivíduos monitorados, os aparelhos disciplinares possuem a capacidade de hierarquizar, numa relação mútua, os "bons" e os "maus" indivíduos. Nesse sentido, "Através dessa microeconomia de uma penalidade perpétua, opera-se uma diferenciação que não é a dos atos, mas dos próprios indivíduos, de sua natureza, de suas virtualidades, de seu nível ou valor"[80].

Essa diferenciação é especialmente problemática quando reforça problemas estruturais enraizados na sociedade. Como demonstrado, a eficácia dos sistemas de reconhecimento facial é significativamente reduzida quando usada na identificação de pessoas negras, quando comparada ao seu

79 BANNAN, Christine; BLASE, Margarite. *Automated Intrusion, Systemic Discrimination: How Untethered Algorithms Harm Privacy and Civil Rights*. October, 2019.

80 FOUCAULT, Michel. *Vigiar e punir*: história da violência nas prisões. 27. ed. Petrópolis: Vozes, 1987, p. 151.

desempenho em pessoas brancas, justificando a centralidade da abordagem racial sobre o debate. Partindo da teoria, importa a concepção do racismo como a criação de um "ser-outro", que se diferencia na medida em que não corresponde ao ser humano universal. Isso é dizer que a definição do negro se dá a partir de um lugar de ausência, do negativo, do que não é - e isso só é possível a partir do estabelecimento de padrões para aquele que é[81]. Historicamente, a centralização do hemisfério ocidental operou a neutralização da branquitude, tornando-a uma referência cultural e com isso, uma régua para medir o encaixe do indivíduo na sociedade. Disso decorre que, incapaz de alcançar fenotipicamente os padrões que permitem a humanização do ser, o negro só pode ocupar um "não-lugar", enquanto ser branco é um lugar de transparência total[82].

Não existindo enquanto tal, o Negro é constantemente produzido. Para Achille Mbembe, produzir o Negro é produzir um vínculo social de submissão e um corpo de exploração, com a raça constituída pelo ato de atribuição. Na obra *Crítica da razão negra*, o pensamento do autor permite endereçar as tecnologias de monitoramento utilizadas na esfera da segurança pública, na medida em que:

> **"** A reactivação da lógica da raça é indestrinçável da escalada em força da ideologia securitária e da instalação de mecanismos com vistas a calcular e minimizar os riscos, e a fazer da proteção a moeda de troca da cidadania.
>
> **[...]** Toda a securitização requer obrigatoriamente a disseminação de dispositivos globais de controle das pessoas e a tomada de poder sobre um corpo biológico múltiplo e em movimento.**"** [83]

Nesse sentido, a autora estadunidense Cheryl Harris atribui à branquitude um sentido de propriedade[84], sendo um conjunto de características - principalmente o tom da pele - que blindam o sujeito branco, protegendo-o de situações e constrangimentos exclusivamente destinados aos negros. Assim, nesse caso, percebemos essa hierarquia social sendo reforçada pela tecnologia; possuir um rosto

81 MBEMBE. Achille. *Crítica da razão negra*. 1. ed. Lisboa: Antígona, 2014. p. 25 - 74.

82 MOREIRA, Adilson José. Direito, poder, ideologia: discurso jurídico como narrativa cultural. *Rev. Direito e Práx.*, Rio de Janeiro, Vol. 8, N. 2, 2017, p. 830-868.

83 MBEMBE. Achille. *Crítica da razão negra*. 1. ed. Lisboa: Antígona, 2014, p. 47.

84 HARRIS, Cheryl I. *Whiteness as Property. Harvard Law Review*, Vol. 106, No. 8, p. 1707, 1993, *UCLA School of Law Research Paper No. 06-35*. Disponível em: <https://ssrn.com/abstract=927850>. Acesso em 09/06/2021.

negro, inocente ou não, apresenta-se como um fator determinante para ser injustamente abordado e/ou condenado por conta da tecnologia de reconhecimento facial. Ainda nessa linha, o conceito de microagressão, proposto pelo psiquiatra Chester Pierce, explica que os mecanismos ofensivos são mais frequentemente sutis e paralisantes do que brutos ou violentos fisicamente, constituindo uma "forma de racismo sistêmico e cotidiano usado para manter aqueles à margem racial em seus lugares"[85]. Dentre as microagressões bem conhecidas pela população negra, a suposição de criminalidade, sob a qual uma pessoa racializada tem mais chance de ser "perigosa, criminosa ou desviante baseado em sua raça"[86].

As potenciais consequências da implementação das tecnologias de reconhecimento facial a contextos de estratificação social já foram previstas e denunciadas por estudos acadêmicos e produções cinematográficas, como bem sintetizado por Silva e Silva[87]:

> **" [...]** a seletividade do sistema penal, demonstrada previamente, comprova que a população negra já sofre diuturnamente com o estereótipo de criminoso, desde microagressões que envolvem uma excessiva vigilância em estabelecimento comercial, cuja intencionalidade é facilmente negada, até casos de prisões indevidas e injustas. Com uma tecnologia em que o próprio algoritmo cumprirá este papel de indicar pessoas negras, equivocadamente, como potenciais suspeitas de um crime, novamente elas estarão "sujeitas à automatização de constrangimentos e violências, como abordagens policiais indevidas e atribuição inverídica de antecedentes criminais
>
> **[...]** A criação de uma base de treinamento com exemplos de faces em que não há diversidade nas amostras pode fazer com que o algoritmo trabalhe e reforce estereótipos de exclusão da população negra." [88]

85 SILVA, Tarcízio. *Racismo algorítmico em plataformas digitais: microagressões e discriminação em código*. VI Simpósio Internacional LAVITS, 2019.

86 Ibidem.

87 SILVA, Rosane L. & SILVA, Fernanda S. R. Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. 5° Congresso Internacional de Direito e Contemporaneidade, 2019.

88 Ibidem.

5.3. CONDIÇÃO PARA MATAR E A TECNOLOGIA

Nas suas considerações sobre o exercício do poder Estatal, Michel Foucault afirma que o funcionamento do Estado inevitavelmente passaria pelo racismo. Segundo ele, o racismo "é a condição de aceitabilidade da condenação à morte numa sociedade de normalização"[89]. Assim, a raça autoriza, entre as categorias abstratas, eleger aqueles passíveis de estigmatização, desqualificação moral e segregação. Nesse contexto, o processo de racialização fixa os limites nos quais grupos de populações podem circular, sob a defesa de prevenir contra os riscos que possam significar para a segurança geral[90].

Na concepção foucaultiana, amplamente explorada por Mbembe, o biopoder parece funcionar mediante a divisão entre as pessoas que devem viver e as que devem morrer. Nesse sentido, pode ser entendido como "racismo" a subdivisão da espécie humana e o estabelecimento da censura entre uns e outros, um poder definido em relação a um campo biológico que permite o controle[91]. Isso funciona, segundo Mbembe, a um dos muitos imaginários da soberania, que percebe "a existência do outro como um atentado contra a minha vida, como uma ameaça mortal ou perigo absoluto, cuja eliminação biofísica reforçaria o potencial para minhas vida e segurança"[92]. Dessa forma, "a função assassina do Estado só pode ser garantida, funcionando o Estado no modo do biopoder, através do racismo"[93], que é a condição para a aceitabilidade do fazer morrer[94].

O mundo da informação, atendendo às necessidades dos regimes democráticos liberais em guerra permanente contra inimigos em constante movimento, torna-se uma ferramenta do Estado. Nesse cenário, ocorre uma transformação na economia da violência que culmina no aumento da força do Estado securitário, acompanhada da necessidade de instalação de dispositivos panópticos que possibilitem o controle das pessoas[95]. Tecnologias surgem para garantir a reunião de dados necessários à vigilância em massa, atuando pela transcrição de características biológicas, genéticas e comportamentais em impressões numéricas, enquanto o cidadão é redefinido como seu sujeito e beneficiário, como se vê abaixo[96].

89 MBEMBE. Achille. *Crítica da razão negra*. 1. ed. Lisboa: Antígona, 2014, p. 67.

90 Ibidem.

91 MBEMBE, Achille. *Necropolítica*. Arte & Ensaios, PPGAV, EBA, UFRJ, n.32, dez. 2016.

92 Ibidem, p. 129.

93 FOUCAULT, Michel. apud MBEMBE. Achille. *Crítica da razão negra*. 1. ed. Lisboa: Antígona, 2014, p. 67.

94 MBEMBE, Achille. *Necropolítica*. Arte & Ensaios, PPGAV, EBA, UFRJ, n.32, dez. 2016.

95 Ibidem.

96 Ibidem

> “ Neste novo regime tecnotrónico, caracterizado pela miniaturização, a desmaterialização e a fluidez na administração da violência de Estado, as impressões (digitais, da íris, da retina, da voz e, até, da forma do rosto) permitem medir e arquivar a unicidade dos indivíduos. **As partes imutáveis do corpo humano tomam-se a pedra de toque de inéditos sistemas de identificação, vigilância e repressão.”** [97] (grifo nosso)

O rosto humano é uma característica biométrica única que varia consideravelmente de aparência de uma pessoas para outra, o que o torna proveitoso aos sistemas de vigilância na distinção entre os indivíduos[98]. Nesse contexto, o racismo, que não deve ser entendido como um comportamento excepcional, mas um sistema sociopolítico global, exerce influência sobre a formatação dos campos produtivos da tecnologia que favorecem o treinamento enviesado de sistemas que intensificam discriminações e opressões[99]. Isso significa que os vieses inconscientes de programadores e treinadores desses sistemas são inevitavelmente incorporados aos algoritmos, como possível verificar:

> “ Ocorre que, apesar da aparente isenção, os algoritmos não estão blindados de reproduzir relações de poder e opressão já existentes na sociedade. [...] Destarte, em que pese a superficial imparcialidade, a sua operacionalização pode permitir a reprodução de discursos sociais preconceituosos.” [100]

97 MBEMBE. Achille. *Crítica da razão negra*. 1. ed. Lisboa: Antígona, 2014, p. 50.

98 ADEBAYO, Olawale; DANIEL, Akpagher; GANIYU, Shefiu; OLANIYI, Olayemi. *Systematic Review of Facial Recognition Algorithms and Approaches for Crime Investigations*, In: *International Journal of Information Processing and Communication* (IJIPC), Vol. 8, No. 1.

99 SILVA, Tarcízio. *Racismo algorítmico em plataformas digitais: microagressões e discriminação em código*. VI Simpósio Internacional LAVITS, 2019.

100 SILVA, Rosane L. & SILVA, Fernanda S. R. Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. *5º Congresso Internacional de Direito e Contemporaneidade*, 2019.

Reproduz-se o discurso de que a Inteligência Artificial é objetiva, neutra e sem valores, como se eliminasse as subjetividades do viés humano; no entanto, mesmo quando não intencionado pelos desenvolvedores, ferramentas algorítmicas reforçam padrões de discriminação histórica enraizados no imaginário sociocultural. Por falta de transparência acerca de como essas tecnologias são desenvolvidas, torna-se um desafio julgar a precisão dos resultados obtidos e, assim, tendemos a atribuir uma objetividade a eles, supondo que resultados carregados de vieses discriminatórios sejam imparciais e infalíveis. Diante dessa suposição, decisões feitas por máquinas carecem da mesma verificação atribuída às decisões realizadas por humanos, aumentando a probabilidade de violações e injustiças passarem despercebidas.

6. CONCLUSÃO

São evidentes as consequências negativas contidas na implementação dos Projetos Vídeo-Policiamento e Vídeo-Polícia Expansão, que invocam a promoção da segurança pública como escudo para camuflar interferências gravíssimas em direitos individuais fundamentais. A expansão do uso da tecnologia a todo o Estado da Bahia configura ação precipitada e perigosa uma vez que não há transparência e clareza acerca do projeto-piloto, o que dificulta a análise de sua conformidade legal e efetividade, e faz com que seja descartada a possibilidade de aperfeiçoamento do projeto antes que este seja expandido ao restante do Estado.

Em primeiro lugar, tem-se uma política que possui um custo externo extremamente delicado, pois requer o monitoramento inconsentido de toda uma população. Nesse sentido, importa a vigilância em massa de um grande número de pessoas para que poucas sejam de fato abordadas - como apresentado anteriormente, na Micareta da Feira de Santana, mais de 1,3 milhões de rostos foram registrados para que apenas 18 mandados de prisão fossem cumpridos. Restam dúvidas acerca do manejo dos dados de todos os outros rostos que supostamente foram inutilizados pela polícia: seriam excluídos ou recuperáveis? Um projeto que ancora-se na vigilância da população por meio da coleta de dados sensíveis e biométricos de milhares de rostos diariamente requer maiores esclarecimentos acerca do manejo de tais informações.

Ainda, as disparidades presentes entre as informações contidas no Termo de Referência e as apresentadas pela SSP/BA em entrevista nos revelam uma falta de transparência, que compromete a análise adequada da política, uma vez que não há informações claras e publicizadas acerca de elementos como: a composição do banco de dados, a porcentagem mínima de precisão da tecnologia requerida para que seja realizada uma abordagem, os crimes realizados pelos agentes procurados, a quantidade de falsos positivos, o número total de abordagens, entre outras informações cruciais para o entendimento da efetividade da política.

A dificuldade de acesso a documentos importantes da implementação e funcionamento do caso analisado revelam problemáticas de um Estado que atua por trás das cortinas, alegando sua competência para implementar mecanismos que resguardem a segurança pública a qualquer custo, sem atentar às responsabilidades que devem ser assumidas neste processo. Ainda, a falta de conhecimento e informações sólidas e transparentes acerca do caso dificulta qualquer reivindicação e questionamento por parte da sociedade civil, principalmente por parte das populações mais vulnerabilizadas pela implementação da política pública. Portanto, conclui-se que a implementação de tecnologias que utilizam dados sensíveis visando a segurança pública e a condenação de criminosos requer transparência total acerca do uso e tratamento desses dados, além de relatórios de impacto que tracem sua efetividade, porcentagens de acerto e metas de aprimoramento.

Ademais, diante da tecnologia empregada nos projetos, percebe-se que a sutileza com a qual mecanismos tecnológicos discriminam dificulta o entendimento popular acerca de seus perigos, já que estão respaldados pela suposição de uma neutralidade algorítmica que supostamente eliminaria a subjetividade contida em procedimentos realizados por humanos. Como levantado, todo o processo da construção da tecnologia fotográfica reproduziu o olhar de uma sociedade racista, inevitavelmente codificado e reproduzido nos algoritmos. Assim, a implementação do reconhecimento facial atua para perpetuar a discriminação estrutural de uma sociedade exclusivista e uma polícia movida pela necessidade de condenar, atuando de maneira discriminatória e violenta; enquanto a tecnologia visa proteger alguns, outros muitos tornam-se alvos predeterminados: pretos e pobres.

De todo o exposto, resta demonstrada a eficiência do uso de tecnologias excludentes e discriminatórias à manutenção do status quo que aparta os sujeitos marginalizados de seus direitos. A teoria é assertiva ao identificar a eliminação de corpos considerados indesejáveis pelo sistema como uma prerrogativa do Estado moderno e denuncia a instrumentalização do desenvolvimento tecnológico a esse fim. Não bastasse a continuidade da violência contra indivíduos historicamente subjugados, resta claro o veemente ataque aos preceitos democráticos simbolizados pela implementação dos sistemas de reconhecimento facial. O Estado, que deveria ser responsável pela promoção da igualdade e do acesso a direitos fundamentais, impulsionando as transformações necessárias para possibilitar sua concretização e privando-se de qualquer atuação na direção contrária, acaba fazendo uso de uma ferramenta responsável pela perpetuação de desigualdades. Os alvos predeterminados do imaginário social são os alvos predeterminados do algoritmo e do Estado.

7. REFERÊNCIAS BIBLIOGRÁFICAS

- ADEBAYO, Olawale; DANIEL, Akpagher; GANIYU, Shefiu; OLANIYI, Olayemi. *Systematic Review of Facial Recognition Algorithms and Approaches for Crime Investigations*, In: *International Journal of Information Processing and Communication* (IJIPC), Vol. 8, No. 1.
- ALVES, Sarah. O Pelourinho vai ganhar câmeras de reconhecimento facial; isso é bom ou ruim? Tilt (UOL), 01 mar. 2021. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/03/01/pelourinho-vai-ganhar-cameras-de-reconhecimento-facial-isso-e-bom-ou-ruim.htm#:~:text=A%20Secretaria%20de%20Seguran%C3%A7a%20P%C3%BAblica,n%C3%A3o%20se%20trata%20da%20pessoa>. Acesso em 30/05/2021.
- ASCOM; ANDRADE, Mariana. SSP recebe Prêmio Case de Sucesso com Reconhecimento Facial. SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. 17 set. 2019. Disponível em: <http://www.ssp.ba.gov.br/2019/09/6446/SSP-recebe-Premio-Case-de-Sucesso-com-Reconhecimento-Facial.html>. Acesso em 31/05/2021.
- ASCOM; RODRIGUES, Rafael. Reconhecimento facial completa dois anos e se adapta à pandemia. SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. 18 dez. 2020. Disponível em: <http://www.ssp.ba.gov.br/2020/12/8875/Reconhecimento-facial-completa-dois-anos-e-se-adapta-a-pandemia.html>. Acesso em 31/05/2021.
- ASCOM; SANTANA, Marcia. Reconhecimento Facial flagra dois foragidos por tráfico de drogas. SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. 04 mai. 2021. Disponível em: <http://www.ssp.ba.gov.br/2021/05/9497/Reconhecimento-Facial-flagra-dois-foragidos-por-trafico-de-drogas.html>. Acesso em 31/05/2021.
- AUGUSTO, Maria Helena Oliva. Segregação social e violência urbana. *Revista brasileira de ciências sociais*. Vol. 17, N. 48. 2002.
- BANNAN, Christine; BLASE, Margarite. *Automated Intrusion, Systemic Discrimination: How Untethered Algorithms Harm Privacy and Civil Rights*. October, 2019.
- 'BBB no Pelô': Prefeitura vai implantar reconhecimento facial no Centro Histórico. Correio 24 horas, 02 fev. 2021. Disponível em: <https://www.correio24horas.com.br/noticia/nid/bbb-no-pelo-prefeitura-vai-implantar-reconhecimento-facial-no-centro-historico>. Acesso 24/05/2021.
- Biometria facial começa a ser implantada nos ônibus de Belém a partir desta segunda, 14. G1-PA, 14 out. 2019. Disponível em: <https://g1.globo.com/pa/para/noticia/2019/10/14/biometria-facial-comeca-a-ser-implantada-nos-onibus-de-belem-a-partir-desta-segunda-14.ghtml>. Acesso 24/05/2021.
- BRASIL. STJ - Superior Tribunal de Justiça. *Habeas Corpus* nº 631298 / BA (2020/0325153-1). Impetrante: Alain Amorim. Impetrado: Governador do Estado da Bahia, Secretário de Segurança Pública do Estado da Bahia, Comandante da Polícia Militar do Estado da Bahia. Relator: Ministro Joel Ilan Paciornik. Autuado em 01 dez. 2020.
- BRASIL. Tribunal de Justiça da Bahia. Mandado de Segurança Cível. Processo nº 8000691-28.2021.8.05.0000. Impetrante: Alain Amorim. Impetrados: Secretário de Segurança Pública do Estado da Bahia, Comandante Geral da Polícia Militar do Estado da Bahia, Governador do Estado da Bahia. Relator: Des. Maurício Kertzman Szporer. Salvador (BA). 2021.
- BUOLAMWINI, Joy. *Facial Recognition Technologies: A Primer*, In: *Algorithmic Justice League*.
- BUOLAMWINI, Joy. *When the robot doesn't see dark skin*, In: *Aperture, Vision & Justice*, pg. 51.
- COMPRASNET-BA. Termo de Referência - Projeto Vídeo-Polícia Expansão. Disponível em: <https://comprasnet.ba.gov.br/sites/default/files/termo_de_referencia_v1.pdf>. Acesso em 24/05/2021.
- Covid mata mais entre trabalhadores que dependem do transporte coletivo. Brasil de fato, 18 ago. 2020. Disponível em: <https://www.brasildefato.com.br/2020/08/18/covid-mata-mais-entre-trabalhadores-que-dependem-do-transporte-coletivo>. Acesso 24/05/2021.

- Desigualdades sociais por cor ou raça no Brasil. IBGE - Instituto Brasileiro de Geografia e Estatística. Rio de Janeiro, 2019. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101681_informativo.pdf>. Acesso em 20/05/2021.
- *Digital Transformation Process*, *Bahia Safe & Intelligent - Results* - Apresentação realizada pelo Governador da Bahia. Disponível p. 46-55 Inicial do MS (Processo nº 8000691-28.2021.8.05.0000).
- Etimologia de fotografia. Etimologia, 2019. Disponível em: <https://etimologia.com.br/fotografia>. Acesso em 15/06/2021.
- Exposição de Motivos do Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Disponível em: <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf>. Acesso em 25/05/2021.
- FERREIRA, Wanise. *Smart cities*: Salvador e Búzios fazem pilotos de videomonitoramento inteligente. tele.síntese (terra), 17 out. 2018. Disponível em: <https://www.telesintese.com.br/smart-cities-salvador-e-buzios-fazem-pilotos-de-videomonitoramento-inteligente>. Acesso em 31/05/2021.
- FOUCAULT, Michel. *Em defesa da sociedade*. 4. ed. São Paulo: Martins Fontes, 2005. Aula de 21 de janeiro de 1976. p. 49 - 74.
- FOUCAULT, Michel. *Vigiar e punir*: história da violência nas prisões. 27. ed. Petrópolis: Vozes, 1987. Terceira parte, Cap. II: os recursos para o bom adestramento. p. 143 - 161.
- Governo da Bahia vai instalar câmeras com reconhecimento facial em ônibus de 70 cidades para combater assaltos. Diário do Transporte, 19 mai. 2021. Disponível em: <https://diariodotransporte.com.br/2021/05/19/governo-da-bahia-vai-instalar-cameras-com-reconhecimento-facial-em-onibus-de-70-cidades-para-combater-assaltos>. Acesso 24/05/2021.
- GOVERNO DO ESTADO, CASA CIVIL. Lançado sistema de videomonitoramento inteligente de segurança, 18 dez. 2018. Disponível em: <http://www.casacivil.ba.gov.br/2018/12/1271/Lancado-sistema-de-videomonitoramento-inteligente-de-seguranca.html>. Acesso em 08/06/2021.
- HARRIS, Cheryl I. *Whiteness as Property. Harvard Law Review*, Vol. 106, No. 8, p. 1707, 1993, *UCLA School of Law Research Paper* No. 06-35. Disponível em: <https://ssrn.com/abstract=927850>. Acesso em 09/06/2021.
- HOSANA, Kelly. Vídeo Policiamento vai facilitar identificação de procurados. SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. 18 dez. 2018. Disponível em: <http://www.ssp.ba.gov.br/2018/12/4908/Video-Policiamento-vai-facilitar-identificacao-de-procurados.html>. Acesso em 31/05/2021.
- HUAWEI CLOUD. *Video Cloud infrastructure*. Disponível em: <https://www.huaweicloud.com/en-us/solution/onlinevideo/>. Acesso em 25/05/2021.
- IBGE: negros são 17% dos mais ricos e três quartos da população mais pobre. Agência Brasil, 02 dez. 2016. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2016-12/ibge-negros-sao-17-dos-mais-ricos-e-tres-quartos-da-populacao-mais-pobre>. Acesso 24/05/2021.
- Inaugurado centro que vai controlar ações de segurança da Copa na BA. G1-BA, 13 jun. 2013. Disponível em: <http://g1.globo.com/bahia/noticia/2013/06/inaugurado-centro-que-vai-controlar-acoes-de-seguranca-da-copa-na-ba.html>. Acesso em: 08/06/2021.
- KANTAYYA, Shalini. *Educational Discussion Guide*, In: *Coded Bias*, pg. 10.
- LESLIE, David. *Understanding bias in facial recognition technologies*, In: *The Alan Turing Institute, Public Policy Programme*, pgs. 9-11.
- LEWIS, Sarah. *Racial Bias and the Lens*, In: *Aperture, Vision & Justice*, pg. 54.
- MBEMBE. Achille. *Crítica da razão negra*. 1. ed. Lisboa: Antígona, 2014.
- MBEMBE, Achille. *Necropolítica*. Arte & Ensaios, PPGAV, EBA, UFRJ, n.32, dez. 2016.
- MOREIRA, Adilson José. Direito, poder, ideologia: discurso jurídico como narrativa cultural. *Rev. Direito e Práx.*, Rio de Janeiro, Vol .08, N. 2, 2017, p. 830-868.
- O algoritmo e racismo nosso de cada dia. Revista Piauí, 02 jan. 2021. Disponível em: <https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-

-cada-dia/>. Acesso 24/05/2021.

- O que são câmeras PTZ? Merlin, 26 mar. 2019. Disponível em: <https://www.merlin.com.br/o-que-sao-cameras-ptz/>. Acesso em 25/05/2021.
- O'NEIL, Cathy. *Weapons of Mass Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Broadway Books, 2016.
- PALMA, Amanda; PACHECO, Clarissa. Entenda como funciona o reconhecimento facial que ajudou a prender mais de 100 na BA: Câmeras estão espalhadas em várias partes de Salvador e imagens são enviadas à central da SSP. Correio 24 horas, 05 jan. 2020. Disponível em: <https://www.correio24horas.com.br/noticia/nid/entenda-como-funciona-o-reconhecimento-facial-que-ajudou-a-prender-mais-de-100-na-ba/>. Acesso em 31/05/2021.
- PALMA, Amanda; Clarissa, PACHECO. 'O policial já foi com a arma na cabeça dele', diz mãe de rapaz confundido por reconhecimento facial: Jovem de 25 anos estava a caminho de consulta médica e foi abordado dentro de padaria. Correio 24 horas, 05 jan. 2020. Disponível em: <https://www.correio24horas.com.br/noticia/nid/o-policial-ja-foi-com-a-arma-na-cabeca-dele-diz-mae-de-rapaz-confundido-por-reconhecimento-facial/>. Acesso em 31/05/2021.
- Periferia, Racismo e Violência. Instituto Locomotiva. Unesco Portuguese, 08 jul. 2020. Youtube. Disponível em: <https://www.youtube.com/watch?v=Ad1q3Qj2XWs>. Acesso em 30/05/2021.
- Pesquisa origem e destino: 50 ANOS. Metrô de São Paulo, 2017. Disponível em: <http://www.metro.sp.gov.br/pesquisa-od/pesquisa-od-50-anos.aspx>. Acesso 24/05/2021.
- PRESCOTT, Roberta; MARIANO, Rafael. Salvador integra 1900 câmeras em sistema único de segurança. Convergência Digital, 25 out. 2018. Disponível em: <https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&UserActiveTemplate=mobile&infoid=49299&sid=18>. Acesso em 31/05/2021.
- *Racial profiling: definition*. ACLU. Disponível em <https://www.aclu.org/other/racial-profiling-definition>. Acesso em 31/05/2021.
- Retratos da Violência: cinco meses de monitoramento, análises e descobertas. Cinco meses de monitoramento, análises e descobertas. Rede de observatórios de segurança, 2019. Disponível em: <http://observatorioseguranca.com.br/wp-content/uploads/2019/11/1relatoriorede.pdf>. Acesso 21/05/2021.
- RODRIGUES, Artur.; PAGNAN, Rogério. & VALENTE, Rubens. Falhas em reconhecimento alimentam máquina de prisões injustas de negros e pobres no Brasil. Folha de São Paulo, 25 mai. 2021. Disponível em: <https://www1.folha.uol.com.br/paywall/login.shtml?http://temas.folha.uol.com.br/inocentes/erros-de-reconhecimento/falhas-em-reconhecimento-alimentam-maquina-de-prisoes-injustas-de-negros-e-pobres-no-brasil.shtml>. Acesso em: 31/05/2021.
- ROTH, Lorna. *Looking at Shirley, the Ultimate Norm: Colour Balance, Image Technologies, and Cognitive Equity*, In: *Canadian Journal of Communication*, Vol. 34, pg. 117.
- SALVADOR (BA). Licitação pública nacional nº 005/2020. [Aquisição de solução de monitoramento para melhoria da segurança turística]. Secretaria de Cultura e Turismo, Salvador, novembro 2020. Disponível em: <http://www.prodeturssa.salvador.ba.gov.br/images/prodeturssa/licitacoes/LPN_0052020_-_edital.pdf>. Acesso em 08/06/2021.
- SANTOS, Gil. Bandidos serão identificados por câmeras de reconhecimento facial em Salvador: Rodoviária, metrô, ferry-boat, Fonte Nova e aeroporto começaram a usar recurso. Correio 24 horas, 18 dez. 2018. Disponível em: <https://www.correio24horas.com.br/noticia/nid/bandidos-serao-identificados-por-cameras-de-reconhecimento-facial-em-salvador/>. Acesso em 31/05/2021.
- SILVA, Rosane L. & SILVA, Fernanda S. R. *Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro*. 5º Congresso Internacional de Direito e Contemporaneidade, 2019.
- SILVA, Tarcízio. *Racismo algorítmico em plataformas digitais: microagressões e discriminação em código*. VI Simpósio Internacional LAVITS, 2019.

- SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. Cicom. Disponível em: <http://www.ssp.ba.gov.br/modules/conteudo/conteudo.php?conteudo=65>. Acesso em 08/06/2021.
- SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. Histórico CIGE. Disponível em: <http://www.ssp.ba.gov.br/modules/conteudo/conteudo.php?conteudo=25>. Acesso em 31/05/2021.
- SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. Reconhecimento facial completa um ano e é destaque nacional. Disponível em: <http://www.ssp.ba.gov.br/2019/12/6981/Reconhecimento-Facial--completa-um-ano-e-e-destaque-nacional.html>. Acesso em 24/05/2021.
- SSP/BA - Secretaria da Segurança Pública da Bahia. Site da SSP/BA; Site do Governo da Bahia. Solicitação de proposta comercial - serviço de conectividade e ponto de imagem para eventos. Disponível em: <http://www.ssp.ba.gov.br/arquivos/File/TR_MODELO.pdf>. Acesso em 24/05/2021.
- Viaturas da PM são equipadas com câmeras e computador de bordo. R7, 31 jul. 2014. Disponível em: <https://noticias.r7.com/bahia/viaturas-da-pm-sao-equipadas-com-cameras-e-computador-de-bordo-28082015>. Acesso em 08/06/2021.

II

COVID-19:

ANÁLISE DOS *APPS* DE COMBATE À PANDEMIA E SEUS IMPACTOS À PROTEÇÃO DE DADOS E À PRIVACIDADE NO PÓS-PANDEMIA

COVID-19: ANÁLISE DOS *APPS* DE COMBATE À PANDEMIA E SEUS IMPACTOS À PROTEÇÃO DE DADOS E À PRIVACIDADE NO PÓS-PANDEMIA

Isabella Matusita
Juliana Reimberg
Maria Julia Gonçalves
Nicole Pudo Gomes

RESUMO

O contexto da pandemia da COVID-19 exigiu que inúmeras medidas fossem adotadas para o combate à doença. Neste artigo, buscou-se analisar as ferramentas de *contact-tracing* e geolocalização presentes em aplicativos para *smartphones* que foram criados para atingir tal objetivo, estudando também o contexto internacional de países que adotaram esse tipo de tecnologia, quais foram os impactos e diante de qual tipo de justificativa fática e apoio jurídico tais ações foram empregadas. Nessa perspectiva, foram apresentados os desafios de ponderar o poder do Estado e os direitos dos cidadãos e, principalmente, avaliar o contexto pós pandemia, analisando questões como: finalidade, necessidade, consentimento, transparência e término do uso de dados, de modo a propor recomendações a serem seguidas para proteger os cidadãos e seus direitos individuais[101].

PALAVRAS CHAVES

Proteção de dados. Pandemia. Aplicativos. *Contact-tracing*. COVID-19.

101 O grupo agradece ao Data Privacy Brasil e às professoras Heloisa Estellita e Eloísa Machado de Almeida pelas contribuições ao desenvolvimento desse artigo.

1. INTRODUÇÃO

Pouco após o início da disseminação do novo coronavírus, o escritor e historiador israelense Yuval Harari (2020) apontou preocupação com a possibilidade do surgimento de novos regimes totalitários em função da crise sanitária vivida mundialmente e das medidas propostas para combatê-la. Harari (2020) sustenta que, na busca por controlar a doença, inúmeros governos estão desenvolvendo novas tecnologias de vigilância em massa, abrindo margem para a legitimação de ferramentas mais invasivas. O risco ainda pode ser majorado pensando em países que costumam rejeitar tais tecnologias, mas que, diante do cenário atual, passaram a utilizar massivamente dados pessoais como algo aceitável, mantendo esse uso após o fim do estado emergencial. Harari (2020) apontou preocupação com a possibilidade do surgimento de novos regimes totalitários em função da crise sanitária vivida mundialmente e das medidas propostas para combatê-la. O autor sustenta que, na busca por controlar a doença, inúmeros governos estão desenvolvendo novas tecnologias de vigilância em massa, abrindo margem para a legitimação de ferramentas mais invasivas (HARARI, 2020).

Mais de um ano depois, a apreensão de Harari (2020) se mostrou fundamentada. Diversos países aderiram ao uso de tecnologia para controlar a pandemia, sobretudo aquelas relacionadas aos dados de *contact-tracing* por meio de aplicativos para celular. No cenário brasileiro, segundo dados coletados pelo *InternetLab* (2021), muitos desses *apps* surgiram sem que houvesse qualquer tipo de política de privacidade e proteção de dados. Como evidência desse comportamento, diversos aplicativos lançados no início da crise sanitária não contavam com termos de uso próprios, estando condicionados aos termos da plataforma em que o *download* ocorria, como *Play Store* e *Apple Store*, ou ainda optavam por dizer que o consentimento para o uso de dados era cedido apenas pelo fato do usuário ter baixado a ferramenta.

O cenário de avanço do uso de tecnologia no monitoramento e controle das atividades sociais lembra a sociedade ficcional e totalitária, constantemente vigiada pelo "Grande Irmão", descrita por Orwell em *1984*, na qual a vigilância massiva era justificada por razões de segurança. No mesmo sentido, atualmente, ferramentas de coleta e tratamento de dados, que podem desencadear vigilância massiva, estão sendo utilizadas sob a justificativa de controlar o avanço da pandemia em diversos países.

Assim, há um risco de que o contexto da pandemia seja utilizado para violações de direitos, sobretudo aqueles relacionados à privacidade e à proteção de dados, para além deste cenário excepcional. No Brasil, desde março de 2020, houve um crescimento dos aplicativos de coleta e tratamento de dados para fins de controle sanitário, ao mesmo tempo em que aumentou o uso de ferramentas digitais e cadastros para realizar atividades durante as medidas de distanciamento social. A coleta e tratamento de dados possuem limites legais para serem realizadas e as principais preocupações que emergem neste contexto são: (i) se as finalidades de coleta e tratamento desses dados estão restritas

ao contexto da pandemia; (ii) se os titulares dos dados possuem clareza sobre tais finalidades.

Diante dessas inquietações, o presente trabalho pretende responder à seguinte questão: quais são as possíveis alternativas para cessar a vigilância massiva pós pandemia no caso brasileiro? O objetivo geral é analisar a vigilância massiva no contexto de tratamento de dados para o combate à pandemia. Entre os objetivos específicos, busca-se (i) analisar os instrumentos jurídicos que regulam o uso de dados pessoais; (ii) identificar os desafios e impactos relacionados à vigilância massiva pós pandemia no Brasil e no mundo; (iii) apresentar possíveis recomendações para assegurar a proteção dos dados e o direito à privacidade no contexto pós pandemia.

Para isso, o texto foi organizado da seguinte forma: na próxima seção será apresentada uma breve revisão de literatura, apontando os problemas da vigilância massiva e o direito à privacidade (item 2); a isso se segue um panorama dos principais casos de uso de dados no controle à pandemia no cenário internacional (item 3); com o que são introduzidos os principais casos no cenário brasileiro, bem como o ordenamento jurídico que regulamenta estas questões (item 4) e, finalmente, apresentadas recomendações para cessar a vigilância massiva no contexto pós-pandemia (item 5).

2. OS DESAFIOS DA VIGILÂNCIA MASSIVA PARA A PROTEÇÃO DE DADOS

Ainda no século 19, Warren e Brandeis (1890) apontavam o nascimento do "direito de ser deixado só"[102], invocado para proteger a privacidade do indivíduo diante dos avanços dos meios de comunicação. Hoje, dois séculos depois, há um debate crescente sobre a vigilância massiva sobretudo nas sociedades capitalistas. Zuboff (2019) nomeia esta era como o "capitalismo da vigilância", que denota um recente gênero do capitalismo que monetiza dados adquiridos por meio da vigilância digital. Para a autora, algumas das definições possíveis para este fenômeno são:

> Uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais ocultas de extração, previsão e vendas (...) 5. A estrutura fundamental de uma economia de vigilância (ZUBOFF, 2019, p. 9, tradução própria).

Esta modalidade incorpora um novo tipo de capitalismo, com base nos dados fornecidos gratuitamente por usuários às empresas de tecnologia, transformando-os em matéria-prima e produto altamente lucrativos. Os dados fornecidos são tantos que podem ser utilizados na previsão e antecipação de comportamentos dos usuários das redes, algo que, à primeira vista, poderia parecer inofensivo, mas que pode ser extremamente problemático, como ilustra o ocorrido nas eleições presidenciais dos Estados Unidos, em 2016, com as operações da *Cambridge Analytica*[103].

Tratamentos em massa de dados pessoais por meio de aplicativos vêm sendo utilizados como ferramentas necessárias para o combate à COVID-19, contudo, a falta de transparência, informação e segurança no tratamento e armazenamento dessas informações causa preocupação em inúmeros setores da sociedade civil. Rodotà (2008) afirma que, em relação aos dados de saúde, "a proteção especial atribuída a estes dados não se justifica somente por se referirem a fatos íntimos, mas também, e às vezes sobretudo, pelo risco que seu conhecimento possa provocar discriminações" (RODOTÀ, 2008, p. 106). No contexto pandêmico, questiona-se se o conhecimento dessas informações sensíveis por

102 Tradução própria. No original, em inglês, é "Right to be let alone".

103 Um exemplo de como os dados podem ter sido usados na campanha é que a *Cambridge Analytica* saberia dizer quais pessoas no Facebook teriam o perfil adequado para receber anúncios divulgando bandeiras e agendas específicas do candidato. Esses anúncios seriam "moldados", levando em conta os medos, necessidades e emoções das pessoas, colocando o até então candidato, Donald Trump, em maior evidência, assim como as pautas principais da sua campanha, podendo este ser um fator de maior angariação de votos.

parte de empregadores, companhias de seguro ou planos de saúde, possa dar causa a discriminações, além de prejudicar os titulares dos dados em contratações ou onerações excessivas para a garantia de serviços.

Existe uma enorme dificuldade em mensurar a extensão da intervenção nos direitos individuais à proteção de dados e o poder do governo de utilizá-los buscando medidas que ajudem no controle da doença. As relações entre o poder do Estado e os direitos dos cidadãos neste setor envolve uma ponderação entre o direito à saúde coletiva e o direito à privacidade. Essa ponderação, porém, deve ser realizada dentro do marco constitucional e do marco legal da Lei Geral de Proteção de Dados (Lei nº 13.709/2018, adiante, LGPD), que já é produto direto de uma ponderação feita pelo legislador, nunca se olvidando que a preservação dos direitos individuais também constitui porção do próprio interesse público, visto que a Administração Pública deve respeitar, proteger e realizar os direitos fundamentais individuais.

Como afirmam Palhares et al. (2020), o direito à privacidade está associado à dignidade da pessoa humana, sendo um direito fundamental, relacionado às liberdades individuais. Nos diplomas internacionais dos quais o Brasil é parte, o direito à privacidade está expressamente associado à vida privada familiar, às comunicações e à honra, como se vê tanto no artigo 12º da Declaração Universal dos Direitos Humanos, quanto no artigo 11, nº 2, da Convenção Americana de Direitos Humanos (Pacto de San José da Costa Rica). Na Constituição Federal de 1988, a proteção à privacidade também se encontra garantida no artigo 5º, inc. X, que prevê a possibilidade de indenização por dano material ou moral em caso de violação da intimidade, da vida privada, da honra e da imagem.

Já o direito à proteção de dados ultrapassa a tutela individual de direitos e relaciona-se a uma discussão mais ampla sobre o acesso a informações no auxílio para tomada de decisões tanto públicas quanto privadas (VENTURA; COELI, 2018). No caso brasileiro, no artigo 5º, inc. XII da Constituição, está assegurada a inviolabilidade de dados. Além dele, é fundamental reconhecer o direito constitucional ao habeas-data, previsto no inc. LXXII, do mesmo artigo, um remédio constitucional que pode ser utilizado tanto para conhecer informações próprias que estão em registros ou bancos de dados de entidades públicas, como também, para solicitar a retificação de tais dados.

Além destas normas constitucionais, está em vigor no Brasil, desde 2018, a LGPD, que dispõe sobre o tratamento de dados pessoais por pessoa natural ou jurídica, de direito público ou privado (art. 1º). Dentre os princípios estabelecidos pela lei nas atividades de tratamento de dados pessoais destacam-se: (i) da finalidade legítima e informada; (ii) da adequação; (iii) da necessidade; (iv) do livre acesso; (v) da qualidade e transparência; (vi) da segurança e prevenção; e (vii) da não discriminação. A lei autoriza, no artigo 7º, inc. VIII, o tratamento de dados pessoais para tutela de saúde, exclusivamente, ou em procedimento realizado por autoridades sanitárias. Assim, reconhece-se a possibilidade de tra-

tamento de dados pessoais em situações que tenham como finalidade a tutela de saúde, lembrando-se de que os direitos dos titulares dos dados assim como os princípios presentes no art. 7°, §7°, da LGPD, devem ser preservados.

O Supremo Tribunal Federal (STF) reconheceu o direito à privacidade como um direito do indivíduo condicionado pelo estabelecimento de garantias, devendo-se observar um conjunto mínimo de salvaguardas para que eventuais ingerências sejam adequadas e possuam uma necessidade legítima. A Corte enfrentou esse tema na ADI 6.387/DF[104], dirigida contra a Medida Provisória nº 954 de abril de 2020. Nessa ADI, a Ministra Rosa Weber destaca a necessidade da observância das excepcionalidades feitas em razão de situações de crise, como a da pandemia do coronavírus. A Ministra argumenta que a coleta de dados de localização sobre a saúde dos indivíduos pode ser benéfica na perspectiva da saúde pública nesse momento de crise global. Contudo, uma vez que esses dados tenham sido coletados é difícil deles serem descartados, já que os governos tendem a não alterar políticas de vigilância, fazendo com que os dados coletados com o objetivo de combater o momento crítico tenham, depois deste, outras finalidades. Assim, Weber aponta que é necessário que haja esforços para se balancear a proteção de dados com um cenário de crise, evitando exceções que se tornem irreversíveis e se mostrem como diminuidoras de direitos adquiridos.

Com o cenário pandêmico enfrentado pelo Brasil e pelo mundo, a grande preocupação é com o que acontecerá com os dados coletados e tratados para fins de controle da pandemia quando a situação atípica se encerrar, principalmente, como tais dados serão usados no futuro sem que haja desvio de finalidade e utilização para vigilância massiva por parte do Estado.

104 Entendimento similar foi proferido pelo Supremo Tribunal Federal nas Ações Diretas de Inconstitucionalidades nº: 6347; 6351 e 6353.

3. CONTEXTO INTERNACIONAL SOBRE O USO DE APLICATIVO DE *CONTACT-TRACING*

É importante fazer um registro do debate internacional a respeito de tais práticas, apresentando o proceder de alguns países[105] quanto a aspectos ligados à proteção de direitos fundamentais e coleta de dados na pandemia. Em raríssimos momentos da história mundial os países foram submetidos aos mesmos desafios - controle e combate à pandemia - quase que de forma simultânea, o que torna esta uma oportunidade preciosa para compreender como trataram a questão objeto deste estudo.

3.1. PAÍSES ASIÁTICOS

3.1.1. COREIA DO SUL

Os primeiros países escolhidos para análise estão localizados no continente asiático, visto que eles foram não só pioneiros no uso deste tipo de tecnologia, como também, foram os primeiros a apresentarem casos de coronavírus (HAN, 2020) e hoje já apresentam índices favoráveis de controle da doença (HAN, 2020). A primeira nação a ser observada é a Coreia do Sul, que desenvolveu o aplicativo governamental chamado de *Self-Quarantine Safe Protection* para controlar a quarentena de pessoas infectadas com o vírus, por meio do monitoramento dos passos desses indivíduos, buscando garantir que não haja violação do isolamento social.

Seu uso é obrigatório para todos os cidadãos sul-coreanos contaminados, e também, para estrangeiros que acabam de chegar em território nacional, sendo que todos devem responder a uma série de perguntas que envolvem fornecimento de dados sobre a saúde individual. Além disso, todos os edifícios e locais públicos foram equipados com câmeras de vigilância e, a partir da coleta deste material em conjunto com os dados do telefone celular, é possível criar o perfil de movimentação de um infectado. Deste modo, valendo-se de uma base de dados do *Korean Center for Disease Control*, o aplicativo registra todos os lugares em que infectados estiveram e envia uma notificação para aqueles que passaram em um raio de 100 metros destas pessoas (JOO, 2020).

Esse cenário favorável não implica dizer que a Coreia do Sul só tomou decisões acertadas. Na verdade, o uso de dados de geolocalização para rastrear casos de COVID-19 trouxe à tona inúmeras questões relacionadas à privacidade e evidenciou erros na proteção de dados feita pelo aplicativo que,

105 A escolha destes países se deu pela relevância no contexto pandêmico, relacionados a eficiência no combate à pandemia, a exemplo da Coreia do Sul; a vigilância estatal, como é o caso da China; o Reino Unido pelo fato de não estar mais na União Europeia e seguir a GDPR, ao contrário do que ocorre na Alemanha; e os Estados Unidos da América por ser um país que defende fortemente as liberdades individuais.

posteriormente, foram corrigidos. Contudo, a tecnologia foi bem aceita pela sociedade civil. Segundo uma pesquisa feita pelo grupo *STEP I*, um *think tank* do país, os sul-coreanos são a favor de medidas contínuas de saúde pública para o controle de doenças infecciosas, mesmo que isso signifique uma vigilância massiva (JIYEON; RICHARDS, 2021). Embora houvesse consenso entre o público disposto a aceitar extenso *contact-tracing* às custas de alguns níveis de violação de privacidade, encontrar o equilíbrio ideal entre privacidade e objetivos de saúde pública não é fácil (KANG; KWON; KIM, 2020).

Cabe ainda pontuar que, recentemente, a lei de saúde pública local foi alterada para obrigar a divulgação eficiente de informações como movimentação individual, meios de transporte, instituições de tratamento médico e contatos de pacientes com doenças infecciosas, a partir do momento em que a crise de doenças infecciosas atinge um determinado nível (JIYEON; RICHARDS, 2021). A transparência desse tipo de dados carrega uma tensão inerente aos riscos de privacidade e a ênfase dada pela Coreia do Sul na transparência das informações é protegida pela Lei de Proteção de Informações Pessoais. Além disso, a lei sul-coreana de saúde pública inclui disposições que garantem proteção rigorosa de dados pessoais, garantindo que apenas sejam usados para ajudar a combater a pandemia, sendo vedada sua utilização para propósitos diversos.

3.1.2. CHINA

Na China, por outro lado, o aplicativo de controle de contágio pelo vírus se tornou apenas mais uma ferramenta integrada ao aparato de vigilância estatal. O país já faz uso do sistema de "crédito social", em que há uma avaliação exaustiva das pessoas e de seus comportamentos, atribuindo uma pontuação, que posteriormente servirá para formar um ranking entre os chineses (BBC, 2017). Além disso, há também um sistema de mais de 200 milhões de câmeras de vigilância e de drones para vigiar os espaços públicos e os provedores de serviços de internet e telefonia são obrigados a compartilhar dados dos seus usuários com o governo, ou seja, há uma vigilância ativa e constante de todos os movimentos das pessoas.

Dentro desse cenário extraordinário, o grupo empresarial Alibaba desenvolveu um aplicativo de uso mandatório a todos os cidadãos, o *Alipay Health Code*. O app é responsável por atribuir a cada usuário um *QR Code* colorido - com base em seu estado de saúde e em seus deslocamentos, e, para receber o código, é necessário ceder informações pessoais como: nome, número da identidade nacional ou passaporte, e telefone (DAVIDSON, 2020). Dada a atual conjuntura do sistema sociopolítico e cultural da China, os usuários da ferramenta apresentam uma forte convicção de que devem confiar e obedecer às ordens do governo durante as circunstâncias anômalas da pandemia, em outras palavras, os usuários tendem a não pensar em erros nas operações com seus dados e são céticos ao imaginar a possibilidade do governo se utilizar desses dados de maneira ilícita (JOO; SHIN, 2020).

Especialista em privacidade e professor da Universidade Batista de Hong Kong, Jason Lau, aponta que as autoridades do governo chinês devem garantir que o aplicativo atenda aos princípios típicos de privacidade de dados, ou seja, deve-se levar em consideração o princípio da proporcionalidade, determinando-se qual objetivo busca-se ser alcançado por meio de tal política pública (GAN; CULVER, 2020). Lau também questiona o destino das informações coletadas após o fim da crise sanitária, serão elas armazenadas para sempre? Liu Yuewen, especialista em Big Data que trabalha para a polícia de uma província chinesa, disse em entrevista coletiva que todos os dados coletados seriam destruídos quando os esforços para conter a pandemia já não fossem mais necessários (GAN; CULVER, 2020).

Apesar da resposta negativa por parte de uma autoridade pública, sabe-se que o país é regido por um governo unitário e autoritário, sendo pouco crível que os dados estão de fato seguros e resguardados e não serão utilizados para outros fins com a melhora do quadro pandêmico.

3.2. PAÍSES EUROPEUS

3.2.1. INGLATERRA

De acordo com as informações fornecidas pelo site oficial do aplicativo *NHS COVID-19*, sua criação envolveu o auxílio de médicos, estudiosos de privacidade e participantes de grupos considerados de risco, como minorias sociais, buscando conciliar o interesse de todos os envolvidos. Afirma-se ali que o *app* foi desenhado de maneira que ninguém é capaz de descobrir quem é o usuário e onde ele esteve, sendo possível inclusive deletar os dados a qualquer momento (KENT, 2021).

Após o *download* da ferramenta, o indivíduo recebe um alerta caso seja detectado que esteve em contato próximo com outros usuários do aplicativo com teste positivo para coronavírus. Isso permite que medidas como o autoisolamento voluntário sejam prontamente tomadas buscando evitar a transmissão da doença. O aplicativo não coleta nenhum dado pessoal e qualquer informação que o usuário decidir enviar é protegida em todos os momentos e excluída quando não mais necessária, conforme a política de retenção de dados da plataforma, segundo o *National Cyber Security Centre* (2020).

O *NHS COVID-19* conta com as seguintes funcionalidades: alertas de pontuação de risco regional, informando o nível de risco presente em determinada área; *check-in* de localização, ou seja, o usuário escaneia um *QR Code* nos locais participantes que ficam registrados durante duas semanas. Caso o local seja considerado de alto risco uma notificação é enviada avisando sobre as possíveis ameaças à saúde; registrador de sintomas e, quando necessário, um convite ao usuário para agendar um teste; serviço de teste, podendo ser agendados por meio do aplicativo e contagem regressiva de auto isolamento, informando quanto tempo ainda é necessário permanecer isolado.

Um diferencial dessa plataforma reside no fato de que, a partir do momento que instalada, a única informação que precisa ser fornecida são os primeiros números do código postal, buscando descobrir o nível de risco em sua localidade. Nenhuma outra informação é solicitada, como nome ou e-mail, isso quer dizer que nenhuma informação pessoal é coletada, apenas dados relativos aos locais em que o usuário faz *check-in* e os sintomas voluntariamente indicados por ele. O aplicativo também registra uma série de análises anônimas, como a marca e o modelo do telefone e a versão do aplicativo que está sendo utilizada. Essas métricas são analisadas para identificar quais melhorias futuras podem ser feitas na ferramenta.

O governo inglês com empresas de tecnologia passou a utilizar os dados de pacientes para criar um repertório sobre a COVID-19. Tais empresas foram contratadas pelo Sistema de Saúde Britânico, a *National Health Service* (*NHS*) para criar uma coletânea de dados e auxiliar na elaboração de modelos preditivos utilizando inteligência artificial (ALMEIDA, 2020). Com relação aos dados confidenciais, anô-

nimos e armazenados em um banco de dados do governo e do *NHS*, os agentes responsáveis informam que permanecerão sob seu controle e sujeitos a severas restrições ligadas à legislação de proteção de dados.

A iniciativa, porém, tem gerado desconfiança quanto a aspectos éticos, de privacidade e de proteção de dados dos cidadãos. Esse sentimento se baseia em questões e desafios relacionados à confiança depositada nas organizações responsáveis pelo processamento e armazenamento dos dados que contêm informações pessoais, independentemente de serem privadas ou governamentais. Contudo, é importante pontuar que essa desconfiança por parte da população não gera um comportamento que busca impedir o uso de dados para criar respostas à pandemia, mas sim auxiliar na garantia de equilíbrio entre os interesses individuais e os coletivos, buscando sopesar o combate à pandemia e a proteção de direitos individuais (ALMEIDA, 2020).

3.2.2. ALEMANHA

Neste outro país europeu, o aplicativo utilizado para auxiliar no combate à pandemia recebeu o nome de *Corona-Warn-App* que, via rastreamento por *bluetooth*, determina se o usuário teve contato com pessoa infectada, o que poderia resultar em risco de contrair e disseminar o vírus; sendo possível interromper as cadeias de infecção mais rapidamente. Segundo informações apresentadas no site oficial do Governo Federal alemão, o aplicativo é um serviço público federal em cooperação com o Instituto Robert Koch, disponível para *download* gratuito na *App Store* e no *Google Play*, sendo o *download* e o uso totalmente voluntários.

No entanto, antes mesmo da disponibilidade da ferramenta, alguns estudos relataram possíveis problemas na aceitação do *app*, destacando questões de privacidade e efetividade (BECKER, 2020; WAGNER, 2020). Apesar dessa desconfiança, o aplicativo, que foi disponibilizado no dia 16 de junho de 2020, já tinha mais de 16 milhões de *downloads* no mês seguinte, e no final de abril de 2021 atingiu a marca de quase 28 milhões, segundo dados da própria plataforma.

O Instituto Robert Koch desempenha um papel duplo: faz uma contribuição profissional para o *design* do aplicativo como editor, mas também é o responsável por verificar cuidadosamente os requisitos de proteção e segurança de dados. De acordo com ele, as informações dos usuários estão sempre seguras e os indivíduos permanecem sob pseudônimos a todo instante, visto que não é necessário fornecer dados pessoais, como nome e e-mail, no momento do cadastro. O armazenamento dos dados que é feito de modo descentralizado e a pseudo-anonimização completa garantem um alto nível de proteção de dados.

Todas as informações sobre contato com outros usuários são criptografadas e armazenadas exclusivamente no *smartphone* individual. No caso de uma infecção, o usuário decide se seus próprios códigos aleatórios são carregados para o *Corona-Warn-App-Server*, o que permite que os usuários do aplicativo avaliem o risco e, em caso de um encontro relevante, enviem um relatório correspondente ao resultado positivo do risco. O aplicativo não tem acesso aos dados que tornam o usuário identificável, em outras palavras, uma pessoa com teste positivo para a doença não descobre quem está sendo informado e aqueles que são informados não sabem quem é a pessoa infectada. Medidas técnicas e organizacionais são tomadas para evitar o uso indevido do relatório de status de infecção por meio do aplicativo.

No geral, segundo o site *Boxcryptor* (2020), ferramenta de criptografia de arquivos e dados, o *Corona-Warn-App* é seguro para o uso do ponto de vista da proteção de dados.

3.3. AMÉRICA DO NORTE: ESTADOS UNIDOS DA AMÉRICA

Até meados de dezembro de 2020, o país contava com 18 aplicativos de *contact-tracing* disponíveis em 18 estados, o que em termos absolutos parece ser muito, mas, na prática, corresponde a menos da metade do território nacional. De acordo com dados disponibilizados pela *Associated Press*, grande parte dos norte-americanos não fizeram *download* da ferramenta, os números ainda sugerem que apenas uma a cada 14 pessoas utilizaram tal tecnologia (ANDERSON; O'BRIEN, 2020).

Na realidade, apesar dos esforços iniciais para implementar esses aplicativos, percebe-se que houve uma forte rejeição por parte da população e com isso, a ferramenta desempenhou um papel mínimo no controle e combate à doença. Um dos principais motivos que levaram a esta situação é que as pessoas não confiam nas empresas de tecnologia ou no governo para coletar, usar e armazenar seus dados pessoais (MADDEN, 2014), especialmente quando estes dados envolvem saúde e localização precisa. Embora a *Apple* e o *Google* tenham se comprometido a incluir medidas de privacidade no *design* dos *apps* - incluindo opções de aceitação, anonimato, limitações de uso e armazenamento de dados apenas no dispositivo próprio do usuário - a sociedade simplesmente não foi convencida das providências tomadas.

No entanto, a resposta dos norte-americanos evidencia o papel decisivo da privacidade na tomada de decisão. Esse cenário é explicado pelo fato de que, nos últimos anos, os cidadãos do país têm sido repetidamente vitimados por violações de dados e outros abusos de privacidade, inclusive por parte das grandes empresas tecnológicas, demonstrando que, em muitos casos, as normas de privacidade, quando existentes, falharam em proteger os indivíduos desses abusos, seja porque os excessos estavam fora do escopo limitado das leis, seja porque as penalidades impostas se mostraram insuficientes (RICH, 2021).

É preciso levar em consideração que os Estados Unidos não têm uma lei geral como a nossa LGPD que pudesse proteger os dados pessoais e confidenciais obtidos por meio desses aplicativos. Não se tem ciência de qualquer lei no país que exija claramente que todos as informações coletadas por meio de aplicativos de *contact-tracing* sejam armazenadas e transmitidas de forma segura, utilizando apenas para fins de rastreamento da COVID-19 e descartados com segurança quando já não forem mais necessários para atingir tal finalidade (RICH, 2021). Este conjunto de fatores demonstra a problemática por trás da ferramenta e aponta uma preocupação clara da sociedade norte-americana com relação à proteção de seus dados, quadro que não se repete em muitos outros locais.

4. O DEBATE NACIONAL: *APPS* CRIADOS PARA O COMBATE AO CORONA VÍRUS

No Brasil, o combate à pandemia tem forte atuação dos estados[106]. Assim, no que tange à vigilância epidemiológica, diferentes estados criaram distintas maneiras de coletar e tratar dados na tentativa de enfrentar a pandemia. Também foram utilizados aplicativos para que os cidadãos participassem de tele consultas e acessassem o auxílio emergencial, sendo o *app* a única via de acesso a esse benefício. As tecnologias nas quais se apostou podem oferecer à população acesso a informações relevantes; promover o rastreamento de contato com pessoas contaminadas; monitorar o deslocamento da população; e executar a fiscalização individualizada de isolamento compulsório. Todavia, a maior parte desses aplicativos foi criada antes da entrada em vigor da Lei Geral de Proteção de Dados, em setembro de 2020[107], sem que fosse realizado um amplo debate sobre os riscos associados a essa coleta e tratamento de dados.

Por esse motivo, a análise desses *apps* é crucial para entender se os critérios de consentimento, necessidade, transparência e segurança previstos na LGPD estão sendo respeitados por esses aplicativos, considerando sobretudo a entrada em vigor da LGPD.

Em abril de 2020, os aplicativos Coronavírus SUS, e-saúdeSP (nomeado de "Coronavírus SP" no início), Atende em Casa - PE, Saúde Osasco, Telemedicina Paraná, Cachoeirinha contra o Coronavírus, Caixa - Auxílio Emergencial já haviam sido criados. De acordo com o relatório publicado em abril de 2020 pela *InternetLab*, o *app* Coronavírus SUS não apresentava nenhum documento relacionado ao consentimento do usuário ou políticas de privacidade, explicitando as permissões solicitadas em sua página na *PlayStore*. Já no caso do Coronavírus SP, Atende em Casa - PE e Saúde Osasco, a política de privacidade era apresentada após um pré-cadastro que solicitava informações pessoais do usuário. Nas políticas de privacidade do Coronavírus SP e Atende em Casa – PE, admitia-se expressamente que poderiam ser feitas futuras alterações em tais políticas sem que usuário fosse comunicado. Contrariamente, os *apps* Saúde Osasco e Caixa - Auxílio Emergencial foram os únicos na época a colocarem

106 O Supremo Tribunal Federal na Ação Direta de Inconstitucionalidade (ADI) 6341, de autoria do PDT, em relação à Medida Provisória 926 de 2020, decidiu que União, Estados, Distrito Federal e Municípios têm competência concorrente na área da saúde pública para realizar ações de mitigação dos impactos do novo coronavírus. Assim, é responsabilidade de todos os entes da federação adotarem medidas em benefício da população brasileira no que se refere à pandemia. No frágil momento causado pela COVID-19, faz-se necessária a existência de harmonia e de coordenação entre as ações públicas dos diversos entes federativos, referido no inciso I do art. 30 da Constituição Federal. O Ministro Relator Marco Aurélio, no presente caso, que versava sobre a constitucionalidade da Medida Provisória 926 de 2020, manifestou que "*as providências [do Governo Federal] não afastam atos a serem praticados por Estados, Distrito Federal e Municípios, considerada a competência concorrente na forma do art. 23, II, da Lei Maior*".

107 O projeto da LGPD foi sancionado no ano de 2018, pelo então presidente Michel Temer, com início de sua vigência previsto para fevereiro de 2020. Entretanto, durante o processo legislativo de conversão da medida provisória em lei, foram feitas alterações em seu texto, havendo uma remarcação do início do período de vigência para agosto de 2020. A esse período entre a data da publicação de uma lei e o início de sua vigência é atribuído o nome *vacatio legis* (do Latim, vacância da lei), que tem por objetivo possibilitar que os destinatários da lei se adaptem às suas regras.

expressamente que os usuários seriam notificados se ocorresse uma alteração nas políticas de privacidade desses *apps*. Alguns desses aplicativos afirmavam que o consentimento ocorria após o *download* e utilização do mecanismo pelo usuário, como foi o caso de Atende em Casa - PE, Telemedicina Paraná e Cachoeirinha contra o coronavírus.

Todos os oito *apps* citados solicitaram permissões para diversas funcionalidades dos celulares daqueles que os utilizavam como, por exemplo, acesso a câmera, microfone, localização, contatos, armazenamento, galeria de fotos e vídeos, informações sobre a conexão *Wi-Fi*. A importância da LGPD fica clara nesse caso, já que, de acordo com a análise da *InternetLab* (2020), muitos dos programas analisados coletavam dados que não se demonstraram necessários para a finalidade do aplicativo.

Para identificar o panorama de aplicativos que são - ou foram[108] - utilizados no Brasil no monitoramento, controle e combate da pandemia da COVID-19, bem como de suas políticas de proteção de dados elaboramos a Tabela 1 que contém as informações disponíveis nos sites dos aplicativos ou em suas ferramentas de *download* e, quando existentes, os termos de uso e as políticas de privacidade[109].

TABELA 1 - MAPEAMENTO DOS APPS NO BRASIL[110]

APP	DADOS COLETADOS	FINALIDADE
Coronavírus SUS [111]	Dados salvos no smartphone (não especificado) e as conexões com o servidor de modo criptografado[112]	Alertar os usuários em relação ao contato com a COVID-19
Tem Política de Privacidade própria?		SIM
Prevê o término do uso de dados?		SIM
Compartilha dados com terceiros?		NÃO
O anonimato dos dados é garantido?		SIM

108 Alguns aplicativos foram extintos, entretanto, entendemos que os dados que foram coletados e tratados durante a existência do aplicativo ainda são relevantes para se discutir o contexto pós-pandemia, uma vez que não se tenha clareza do que foi feito com esses dados. Assim, tais aplicativos estão mantidos nessa análise.

109 A seleção dos *apps* ocorreu por meio de pesquisa na *Play Store* e na *Apple Store* de aplicativos que foram criados para combater ou auxiliar as ações na pandemia. Para isso pesquisamos nessas duas lojas de *apps* por termos como "coronavírus", "COVID-19" e "pandemia". Ademais, houve pesquisa prévia sobre artigos e notícias que já analisavam a criação de alguns aplicativos para combater o vírus.

110 Os espaços em branco na tabela apontam que a informação não foi encontrada.

111 https://apps-politica-privacidade.saude.gov.br.

112 O app não coleta dados do perfil como nome, sobrenome, data de nascimento, endereço, número de telefone e endereço de e-mail nem dados de geolocalização.

Monitora COVID-19 [113]	• Nome • E-mail • Endereço -localização • Protocolo de internet do computador - endereço de IP	
Tem Política de Privacidade própria?		NÃO
Prevê o término do uso de dados?		NÃO
Compartilha dados com terceiros?		SIM
O anonimato dos dados é garantido?		

Minha Saúde [114]	• Dados fornecidos pelo usuário • Dados coletados automaticamente pelo sistema [115]	Fins de controle e automação da gestão pública, bem como para o desenvolvimento de políticas públicas; ou pela licenciante com fins de pesquisa e desenvolvimento do sistema seguindo as normas de conformidade aplicáveis e a LGPD.
Tem Política de Privacidade própria?		SIM
Prevê o término do uso de dados?		NÃO
Compartilha dados com terceiros?		SIM
O anonimato dos dados é garantido?		SIM

Atende em Casa - PE [116]	• CPF • CEP	
Tem Política de Privacidade própria?		NÃO
Prevê o término do uso de dados?		NÃO
Compartilha dados com terceiros?		
O anonimato dos dados é garantido?		

113 https://esusatendsaude.com.br/docs/politica-de-privacidade.html.

114 https://esusatendsaude.com.br/docs/politica-de-privacidade.html.

115 São informações coletadas pelo sistema, independentemente do fornecimento pelo usuário. A cada acesso são obtidos alguns dados automaticamente, tais como, mas não se limitando a, características do dispositivo de acesso, número IP com informação de data e hora, origem do IP, funcionalidades acessadas, informações sobre cliques, entre outros.

116 https://docs.google.com/document/d/e/2PACX-1vSlvcsBRu9Ad6FDiIzf9pinSCrkL8Fxoy5iVHxYRMYP9wJW5CWMs5JOsKxQznG-Mgt5IqKp3JczZJuW-/pub.

Saúde Osasco		
Tem Política de Privacidade própria?		NÃO
Prevê o término do uso de dados?		NÃO
Compartilha dados com terceiros?		
O anonimato dos dados é garantido?		

Saúde Online Paraná [117]	• Nome completo • Data de Nascimento • Número e imagem do RG • Número CPF • Número da Carteira Nacional de Saúde • Fotografia 3x4, para biometria facial • Gênero • Endereço completo • Dados referentes à saúde • Números de telefone, WhatsApp e endereços de e-mail • Número de telefone celular • Nome de usuário e senha específicos para uso dos serviços do Controlador	Responda questionários de saúde para avaliação de pacientes com suspeitas de COVID- 19 e outras doenças; ter orientação de profissionais da área da saúde; Triagem prévia; e agendamento de teleconsultas.
Tem Política de Privacidade própria?		SIM
Prevê o término do uso de dados?		SIM
Compartilha dados com terceiros?		SIM
O anonimato dos dados é garantido?		SIM

Cachoeirinha contra o coronavírus - RS [118]		
Tem Política de Privacidade própria?		SIM
Prevê o término do uso de dados?		NÃO
Compartilha dados com terceiros?		SIM
O anonimato dos dados é garantido?		

117 https://saudeonlinepr.techtools.vc/termosdeuso.html.

118 https://cachoeirinha-rs.coronavirus.tmp.br/privacypolicy/

Coronavírus SP/e-saúde-SP [119]		Gestão da interação do profissional de saúde com o paciente e com outros profissionais
Tem Política de Privacidade própria?		SIM
Prevê o término do uso de dados?		NÃO
Compartilha dados com terceiros?		SIM
O anonimato dos dados é garantido?		

Caixa Auxilio Emergencial [120]	• Nome • CPF • Data de nascimento • Nome da mãe	
Tem Política de Privacidade própria?		NÃO
Prevê o término do uso de dados?		SIM
Compartilha dados com terceiros?		SIM
O anonimato dos dados é garantido?		

119 https://www.prefeitura.sp.gov.br/cidade/secretarias/saude/atencao_basica/index.php?p=302131

120 https://www.caixa.gov.br/auxilio/auxilio2021/Paginas/default.aspx

4.1. ANÁLISE DOS APLICATIVOS A LUZ DA LGPD

Dos oito aplicativos analisados no Brasil, apenas um não está mais em funcionamento: o Saúde Osasco.

Em relação à origem da iniciativa, a maioria dos aplicativos são de iniciativa pública, sendo o mais expressivo o *app* Coronavírus SUS, que é do Ministério da Saúde. Os demais pertencem a Municípios ou Estados da federação. A única exceção, sendo pertencente a iniciativa privada, é o aplicativo privado Minha Saúde, desenvolvido pela *HealthTech ProntLife*[121] e a *GovTech Lemobs*[122], em parceria com os grupos de pesquisa de universidades COPPE/UFRJ, LNCC, UNIFEI e CNM. No caso do Minha Saúde, os municípios podem aderir ao aplicativo para monitorar a disseminação do coronavírus.

O que se percebe é que a maior parte dos aplicativos são restritos a determinadas cidades ou estados, sendo o Coronavírus SUS o único aplicativo existente no âmbito nacional. Além dele, o aplicativo "Monitora COVID-19" resulta de uma parceria entre estados do Nordeste, abrangendo, consequentemente, toda essa região[123].

121 Uma empresa especializada em teleconsultas, prontuários eletrônicos e desenvolvimento de aplicativos para os pacientes.

122 GovTech incubada no Parque Tecnológico da UFRJ.

123 https://www.saude.ma.gov.br/destaques/governo-do-maranhao-e-consorcio-nordeste-lancam-aplicativo-para-monitorar-casos-da-covid-19/.

4.2. A COLETA DE DADOS SENSÍVEIS E SEUS IMPACTOS

4.2.1. OS CRITÉRIOS DE FINALIDADE E NECESSIDADE SÃO ATENDIDOS PELOS *APPS*?

O princípio da finalidade está positivado na LGPD, em seu artigo 6º, I, demonstrando a função da finalidade como a realização do tratamento para propósitos legítimos e explícitos. No mesmo artigo 6º se encontram os princípios de necessidade - definido como a limitação do tratamento ao mínimo necessário para a realização de suas finalidades - e da transparência - fixado como garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento -, nota-se que diversos *apps* apresentados não respeitam essas imposições da LGPD, não apresentando a descrição de sua finalidade e necessidade ou, então, não tendo uma descrição específica que realmente expresse as motivações e os limites do tratamento de todos os dados recolhidos.

Como demonstra a Tabela 1, o número de informações pessoais que devem ser fornecidas para a utilização de apenas três aplicativos dos dez analisados demonstra como a diversidade em número de *apps* para o combate do COVID-19 faz com que os usuários exponham - dependendo de sua região - seus dados diversas vezes para aplicativos que apresentam diversos níveis de segurança no tratamento desses dados.

À luz do princípio da necessidade, vê-se que alguns *apps* acabam por requisitar informações que poderiam ser entendidas como dispensáveis, como é o caso do Saúde Online do Paraná que apresenta a seguinte finalidade: possibilitar (i) que o usuário responda questionários de saúde para avaliação de pacientes com suspeitas de COVID- 19 e outras doenças; (ii) que o usuário, caso tenha COVID-19 ou outras doenças, possa contar com a orientação de profissionais da área da saúde, para fins de fornecer orientações e aconselhamentos relacionados à saúde; (iii) a triagem prévia para o atendimento através da autoavaliação feita pelo usuário e, por consequência, garantir maior agilidade no diagnóstico e solução do problema; (iv) o agendamento de teleconsultas. Apesar dessa finalidade, informações requisitadas, como fotografia 3x4 para biometria facial, podem ser entendidas como não sendo de fato necessárias para que a função do *app* seja exercida.

Acerca da finalidade, observou-se que uma parcela dos *apps* seguiram esse princípio previsto na LGPD, como é o caso do Coronavírus SUS. Os dados só serão utilizados para alertar os usuários em relação ao contato com a COVID-19, como exposto nas finalidades do *app*, além da forma agregada e anônima com o objetivo de saúde pública, profilaxia, estatística ou pesquisa científica. Já no caso do Monitora COVID-19, Cachoeirinha contra Coronavírus e o Saúde Osasco, não há nenhuma referência à finalidade em suas Políticas de Privacidade. No aplicativo Minha Saúde e do e-saúdeSP as descrições da finalidade são pouco específicas, o que pode apresentar riscos à proteção dos dados pessoais dos titulares.

Em relação ao aplicativo da Caixa - Auxílio Emergencial - *app* no qual os usuários utilizam para acompanhar a situação pessoal em relação ao seu auxílio emergencial - além dos dados coletados como demonstrado na Tabela 1, a política de privacidade informa que há dados coletados automaticamente quando houver navegação no site ou uso dos aplicativos, inclusive por meio do uso de *cookies*[124]. A justificativa é proporcionar comodidade, segurança na navegação e aprimorar os canais do banco. Algumas finalidades para o tratamento de dados pessoais descritas pela Caixa em sua política de privacidade são: (i) realizar as atividades necessárias à execução dos contratos de produtos ou serviços que o banco tem com o consumidor/usuário, inclusive em procedimentos preliminares às contratações; (ii) operar políticas públicas; (iii) responder as dúvidas, solicitações, reclamações ou elogios; (iv) verificar a identidade do usuário, visando evitar fraudes, atividades ilegais ou não autorizadas; (v) comunicar, administrar e oferecer conteúdo e benefícios direcionados e específicos ao seu perfil e que podem ser do interesse do usuário; (vi) enviar informações administrativas ao usuário, como termos, condições, políticas e contratos; (vii) desenvolver novos canais, serviços ou produtos e realizar melhorias naqueles que o usuário já utiliza; (vii) proteger a CAIXA, seus empregados, parceiros, clientes e mercado, incluindo as atividades relacionadas ao crédito; (viii) monitorar, analisar as tendências, medir audiências, corrigir problemas e evoluir o uso do site e aplicativos; (ix) atender a determinações legais ou regulatórias. Essas descrições compõem a política de privacidade da Caixa que é destinada a todos os serviços do banco que requerem dados e, por esse motivo acaba por ser pouco transparente, por não apresentar respostas claras aos princípios exigidos pela LGPD ao aplicativo. Ademais, política de privacidade não é apresentada diretamente no aplicativo e, portanto, para o usuário é necessário fazer uma busca no site da Caixa para encontrá-la.

Os princípios de finalidade e necessidade são importantes para fazer com que as empresas privadas e administração pública expressem de maneira clara qual é a motivação do recolhimento dos dados e qual é a necessidade de cada dado requisitado para atingir a finalidade do *app*. Assim, o usuário possui as informações necessárias para consentir de maneira consciente com a utilização dos seus dados. Além disso, quando a finalidade e necessidade estão expressas há maior facilidade para que uma fiscalização e cobrança possa ser feita. *Apps* como Monitora Covid-19, Atende em Casa e Saúde Osasco não apresentaram políticas de privacidade, sendo assim, esses apps não demonstram nenhum tipo de responsabilidade com os dados tratados, já que não manifestam por nenhuma via uma preocupação com a transparência do uso de algo tão significativo como os dados de diversos usuários. Diversos *apps* analisados nessa pesquisa, como é o caso do Caixa - Auxílio Emergencial, Minha Saúde, Atende em Casa, Saúde Online Paraná, e-Saúde SP, Cachoeirinha contra o Coronavírus - demonstram uma política de privacidade, contudo, não são específicos enquanto a descrição dos princípios de finalidade e necessidade, deixando lacunas como o entendimento de como cada dado coletado é estritamente necessário para atender aos critérios de finalidade.

124 *Cookies* são pequenos arquivos de texto que ficam gravados no computador do internauta e podem ser recuperados pelo site que o enviou durante a navegação. São utilizados pelos sites principalmente para identificar e armazenar informações sobre os visitantes.

4.2.2. O FUNCIONAMENTO DO CONTACT-TRACING E SUA UTILIZAÇÃO NO CONTEXTO BRASILEIRO

O *contact-tracing* é o rastreamento de contatos que busca: i) identificar as pessoas que estão com a doença; ii) estabelecer a rede de contatos com a qual a pessoa infectada interagiu; iii) identificar todos os indivíduos que tiveram contato com essa pessoa infectada pelo COVID-19, alertando-as e evitando que elas tenham contato com outros indivíduos. A execução dessa técnica facilita a identificação e monitoramento de infectados, podendo tratá-los com maior facilidade.

O *contact-tracing* é uma tecnologia que foi mais facilmente difundida devido à popularização dos smartphones, já que antigamente era executada muitas vezes de forma manual, dependendo da memória do paciente. A grande maioria dos aplicativos que se utilizam do *contact-tracing* consegue executar essa técnica com base em dados de geolocalização (GPS), *bluetooth* ou com a utilização dos dois somados a outros dados, como sinais de telefonia. Os sinais de telefonia foram empregados por alguns governantes, como a Prefeitura de Recife que iniciou o rastreio de 700 mil aparelhos celulares para monitorar o isolamento social em março de 2020. Já os sinais de GPS foram utilizados por empresas privadas que mediram índices de isolamento social, como foi o caso da *startup* brasileira *Inloco*. A utilização de *bluetooth* é a escolha do *app* Coronavírus SUS para rastrear os possíveis infectados após contato com algum indivíduo com COVID-19.

4.3. OS CRITÉRIOS DE SEGURANÇA E PREVENÇÃO SÃO ATENDIDOS PELOS *APPS*?

A LGPD, prevê, nos artigos do capítulo VII, seção I, que as atividades de tratamento de dados devem observar o princípio da segurança, utilizando de medidas técnicas e administrativas que visem à proteção dos dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas. Nos aplicativos analisados, a observância desse princípio cabe sempre ao controlador. No caso do Coronavírus SUS, o controlador é o próprio Ministério da Saúde, já nas demais aplicações essa figura é assumida pelo seu próprio desenvolvedor.

O controlador se responsabiliza pela manutenção das medidas de segurança, entretanto na maioria das políticas de privacidade não há informações explícitas a respeito dos métodos utilizados na proteção de dados pessoais, empregando cláusulas genéricas que dizem que serão utilizados todos os "esforços disponíveis no mercado"[125] para atingir tal objetivo. O e-Saúde SP e o Caixa - Auxílio Emergencial esclarecem que, visando à proteção dos dados a eles fornecidos, utilizam criptografia. Na política deste primeiro aplicativo, consta que há uma individualização e separação completa dos módulos de dados cadastrais, pessoais e pessoais sensíveis. O Auxílio Emergencial também usufrui de *firewall* e faz um monitoramento constante dos sistemas para garantia da proteção a acessos não autorizados.

Apesar da maioria dos aplicativos analisados serem de iniciativa pública, os desenvolvedores, consequentemente aqueles que armazenam os dados, são empresas de caráter privado. Assim, em conformidade com a LGPD, o controlador dos dados são os órgãos públicos e os encarregados de tratamento, as empresas de iniciativa privada ou, no caso do Monitora COVID-19, de iniciativa mista. Nas políticas de privacidade dos *apps*, consta que essas empresas privadas irão apenas coletar, usar e divulgar as informações na medida do necessário para permitir que realizem os serviços. A maneira com a qual os dados serão tratados por essas empresas é determinado na política de privacidade da própria empresa encarregada do tratamento dos dados. Existem duas exceções: o Coronavírus SUS e o Minha Saúde. O primeiro garante ao usuário o não compartilhamento de seus dados com nenhuma outra instituição, pública ou privada. Entretanto, diferente do que é exigido pela LGPD, a Política de Privacidade do *app* Coronavírus SUS não indicou o encarregado pelo tratamento dos dados. Já o *app* Minha Saúde, de iniciativa privada, coloca em sua política de proteção de dados que as informações dos usuários compõem os ativos da empresa e, desta forma, havendo integrações ou venda dessa, os dados serão transmitidos a terceiros.

125 Os aplicativos que possuem cláusulas como "são tomadas precauções razoáveis e seguidas as melhores práticas da indústria para que as informações não sejam perdidas inadequadamente, usurpadas, acessadas, divulgadas, alteradas ou destruídas." em suas políticas de privacidade, são: Monitora Covid-19, Minha Saúde e Coronavírus SUS.

4.4. OS CRITÉRIOS DE TRANSPARÊNCIA E CONSENTIMENTO SÃO ATENDIDOS PELOS *APPS*?

A análise feita sobre os termos de uso e políticas de privacidade dos apps que foram ou estão sendo utilizados no Brasil no enfrentamento da pandemia da COVID-19 ilustra como alguns *apps* não possuem termos de uso e as políticas de privacidade próprias. Também mostra que os que possuem esses documentos, apresentam termos de uso e políticas de privacidade muito diversos entre si.

Em relação à não apresentação de termos de uso próprios, o que se nota é que alguns aplicativos utilizam somente os termos de uso das próprias plataformas de *download*, como a *Play* e *Apple Store*, ou utilizam termos gerais das instituições às quais estão vinculados, como acontece com o aplicativo Caixa - Auxílio Emergencial, que usa os termos da própria Caixa Econômica Federal.

No que tange à diversidade dos termos de uso próprios e das políticas de privacidade existentes, o que se nota é que a LGPD estabelece, no art. 7º, que o titular dos dados deve fornecer o consentimento para coleta e tratamento dos dados, bem como para compartilhar esses dados com terceiros. Esse consentimento deve estar associado a uma finalidade específica, e essas informações normalmente são expressas nos termos de uso e nas políticas de privacidade, porém não há uma determinação na LGPD sobre como esses documentos devem ser elaborados, razão pela qual cada controlador adota a forma que lhe for mais conveniente.

O risco dessa liberdade dada aos controladores dos dados é que os termos de uso e de políticas de privacidade são muito amplos e, muitas vezes, pouco informativos sobre o que será feito com os dados. Outro ponto que merece destaque é os termos de uso e as políticas de privacidade poderem sofrer alterações a qualquer tempo. Os termos de uso e políticas de privacidade de muitos *apps* - Monitora COVID-19, Saúde Online Paraná e Coronavírus SP/e-saúde SP - apontam que os titulares não serão informados caso essas modificações ocorram, cabendo ao titular monitorar periodicamente esses documentos para verificar se eles foram alterados ou não. Entendemos que tal possibilidade configura-se como uma manipulação do conceito de "consentimento", sendo prejudicial aos titulares dos dados e colocando em risco a proteção desses dados.

O consentimento dos usuários é visto como a principal hipótese de autorização legal para o tratamento de dados pessoais através do Marco Civil da internet (art. 7º, VI, VII, VIII, IX). O entendimento é que esse consentimento deve ser "livre, expresso e informado" (Lei 12.965/2014, art. 7º, VII) para ter sua validade. Sendo assim, deve existir uma explicação transparente sobre o tratamento dos dados e, também, um maior grau de certeza do titular a respeito da autorização que está concedendo (INTERNETLAB, 2020), o que não acontece com alguns dos *apps* analisados, já que não informam os usuários quando fazem modificações nas políticas de privacidade ou, então, não criam algum modo de o titular aceitar expressamente o tratamento de seus dados.

4.5. O TÉRMINO DE USO DOS DADOS E A ANONIMIZAÇÃO SÃO ATENDIDOS PELOS *APPS*?

As políticas de privacidade dos aplicativos analisados apresentam disposições genéricas a respeito da anonimização dos dados e da cessação de uso desses. A LGPD, em diversos artigos, determina que, sempre que possível, deve haver a anonimização dos dados a partir da utilização de meios técnicos disponíveis no momento do tratamento, de forma que os dados percam a possibilidade de associação, direta ou indireta, a um indivíduo.

A anonimização dos dados é mencionada de forma não específica nas políticas de privacidade. Em nenhuma delas foi especificado quais seriam os dados anonimizados e nem a forma com a qual essa se daria, limitando-se apenas a garantir ao usuário que a política de privacidade encontra-se em conformidade ao determinado pela LGPD a respeito da anonimização dos dados. A LGPD apenas determina que a anonimização deve ser feita sempre que possível, não dispondo sobre a maneira com a qual deveria ocorrer.

No que tange ao término do uso dos dados, há posicionamento mais preciso da LGPD, dedicando a Seção IV do Capítulo II exclusivamente às determinações sobre a cessação. O artigo 15 dispõe acerca das hipóteses nas quais se dá o término do tratamento dos dados, no inc. I, há previsão de cessão dos dados com o atingimento da finalidade almejada. Tal disposição é replicada na política de proteção de dados do *app* Coronavírus SUS e Minha Saúde, que preveem que farão o tratamento dos dados enquanto servirem à finalidade. Ambos os aplicativos ainda versam a respeito do que ocorrerá uma vez que cessarem o tratamento dos dados. Seguindo as diretrizes legais, os dados anonimizados serão mantidos pelo controlador por tempo indeterminado. Os demais aplicativos não possuem disposições a respeito do destino dos dados por eles coletados.

5. RECOMENDAÇÕES

Diante de toda conjuntura apresentada anteriormente e buscando evitar que o contexto da pandemia seja utilizado de forma irresponsável para tornar o período atípico de crise sanitária um pretexto para a implementação de uma sociedade de vigilância massiva no Brasil, é imprescindível que recomendações quanto ao uso de dados pessoais sejam seguidas por parte do governo e, principalmente, pelos desenvolvedores dos aplicativos, garantindo proteção de direitos aos cidadãos.

Cabe à Organização Mundial da Saúde (OMS) anunciar o fim da pandemia da COVID-19, mas caberá de fato a cada um dos países determinar quando a emergência de saúde pública não é mais uma realidade e as restrições poderão ser suspensas. Essa indeterminação de quando terá início a "era pós-pandêmica" abre precedentes para que se mantenha esse estado de vigilância massiva de maneira prolongada, sob a justificativa de que o combate à COVID-19 ainda não acabou.

Ao contrário de outras normas de direitos fundamentais, não há um regime exclusivo quanto à proteção de dados em período de normalidade e outro regime diversificado para um período de emergência, tal qual a pandemia. A proteção de dados é, portanto, a regra e não exceção[126]. Por esse motivo, operações de tratamento de dados realizadas em período de emergência não devem ter uma resposta diferente da que seria dada à mesma questão se o estado fosse de normalidade (EGÍDIO, 2020). Através da experiência que o Brasil adquiriu com o coronavírus e a invenção desses apps, entende-se que a criação de uma lei temporária poderia fazer existir um fundamento legal para o tratamento de dados de saúde especificamente durante uma pandemia.

A LGPD surge a fim de exigir critérios e explicações quando dados forem requeridos, fazendo com que não seja possível que qualquer interesse público determine como será o processo de tratamento. A importância de garantir o direito à proteção de dados nessa pandemia está relacionada não só ao perigo da vigilância estatal, mas também, ao fato de diversos dados pessoais recolhidos serem aptos a gerar ou promover a estigmatização e a discriminação de seus titulares, como no caso do auxílio emergencial em junho de 2020. Os limites legais da LGPD existem não para inviabilizar iniciativas em prol do bem da sociedade brasileira, mas sim com a finalidade de evitar abusos provenientes dessas iniciativas. Assim, a administração pública e a iniciativa privada podem atuar, porém, respeitando os direitos fundamentais dos brasileiros.

Em junho de 2020, o caso de divulgação de dados dos respectivos beneficiários pelo auxílio emergencial demonstrou como é imprescindível a cautela na criação de sites e *apps* que requeiram infor-

126 Retoma-se, assim, a indagação trazida pela Ministra Rosa Weber na ADI 6.387/DF. No voto, a Ministra ressalta a importância de atentar-se às exceções feitas, uma vez que essas podem tornar-se irreversíveis, acarretando em uma diminuição do direito à proteção de dados já adquirido pelos cidadãos.

mações. Os dados pessoais de mais de 58,6 milhões de brasileiros beneficiários do auxílio emergencial foram publicados no Portal da Transparência do Governo Federal. Sob a justificativa de transparência em relação ao pagamento do auxílio emergencial, o ministro da Controladoria-Geral da União divulgou arquivos contendo dados pessoais daqueles que receberam o benefício, contendo informações como estado, cidade, número de identificação social, parte do CPF, nome completo e valor do auxílio emergencial recebido.

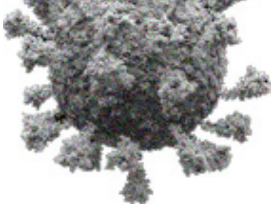
Diante do diagnóstico apresentado nas seções anteriores, nota-se que muitas vezes a finalidade, o compartilhamento dos dados, o término do tratamento, entre outros conceitos definidos na LGPD são utilizados de maneira ampla e genérica. Assim, para garantir de fato a proteção dos dados pessoais, e, assegurar que a vigilância massiva não continue após a pandemia da COVID-19, recomenda-se:

(i) Revisão dos termos de uso dos apps, de modo a apresentar clareza e especificidade sobre a finalidade de coleta e tratamento dos dados e sobre quando haverá o fim desse tratamento e o que será feito com os dados posteriormente. Nesse ponto, acredita-se que a Autoridade Nacional de Proteção de Dados (ANPD) pode ter um papel importante emitindo opiniões e recomendações técnicas que visem fornecer um framework de como devem ser elaborados os termos de uso e políticas de privacidade;

(ii) Coleta e tratamento de dados seja feita de forma proporcional à necessidade, como estabelece o art. 6º, inc. III da LGPD. A recomendação é que sejam coletados somente os dados estritamente necessários e que, nas hipóteses de coletas de dados sensíveis - como dados biométricos - as finalidades do seu uso sejam extremamente específicas, nos termos do art. 11 da LGPD;

(iii) Não condicionar o acesso a benefícios sociais somente aos que utilizam apps, de modo a dar liberdade ao cidadão utilizar ou não essas ferramentas digitais para ter acesso às políticas públicas;

(iv) Revisão dos termos de consentimento dos apps, a fim de que o consentimento livre, expresso e informado possa ser garantido.



6. CONCLUSÃO

Considerando os desafios impostos pelo contexto da pandemia, diversos países passaram a utilizar aplicativos, de iniciativa pública ou privada, para monitorar e controlar o avanço da doença. Nesse cenário, o presente artigo analisa se as finalidades que são apresentadas nesses *apps* são restritas ao momento da pandemia ou se essa vigilância massiva pode ter efeitos no pós-pandemia. Para responder a essa inquietação, foram realizadas uma análise dos instrumentos jurídicos que regulam a proteção de dados pessoais, uma pesquisa sobre como outros países estão enfrentando essa questão e um estudo sobre as políticas de privacidade dos *apps* utilizados no Brasil.

Entre os desafios de uma vigilância massiva no contexto pós-pandemia, destaca-se a colisão entre o direito à privacidade e direitos fundamentais à saúde e à vida, necessitando que o poder público faça o sopesamento entre eles. Assim, a tecnologia escolhida para auxiliar no combate à pandemia deve seguir critérios de proporcionalidade, adequação e necessidade, de modo a evitar uma sociedade de vigilância que pode ocorrer tanto no Brasil quanto em outros países. Uma sociedade de vigilância seria contrária às garantias e liberdades individuais, previstas na Constituição de 1988, como o direito à privacidade e proteção dos dados pessoais.

A análise internacional ilustra que o contexto do pós-pandemia também está presente nos debates e uso dos *apps* de monitoramento da população nesses países, havendo discussões sobre a utilização da tecnologia com base em dados pessoais para atingir um fim específico que por ora ainda é válido. Alguns países já apresentam estudos a respeito do tema, buscando inclusive entender quais os limites que devem ser impostos à utilização de dados em detrimento dos direitos individuais em situações de combate à pandemia.

No caso dos *apps* utilizados no Brasil, nota-se que as políticas de privacidade e os termos de uso dos *apps* são muito diversos entre si, o que impõe desafio à proteção dos usuários dessas ferramentas. Apesar de grande parte dos aplicativos apresentar menção legal à LGPD, nota-se que muitos carecem de informações essenciais como os dados que serão coletados, como e quando tais dados serão deletados e qual é o contato do encarregado em coletar e tratar esses dados. Ainda, em relação à finalidade, percebe-se que ela é muitas vezes apresentada de forma genérica e abrangente, não assegurando o cessamento da coleta e tratamento dos dados nos pós pandemia.

Diante desse panorama, o artigo apresenta as seguintes recomendações. Primeiro que a coleta e tratamento de dados apresente uma finalidade clara e específica nas políticas de privacidade. Segundo que a coleta e tratamento de dados seja feita de forma proporcional. Terceiro que o acesso à benefícios sociais, como foi feito no caso do Auxílio Emergencial, não seja condicionado à adesão a *apps*. Por fim, que os termos de consentimento sejam revistos de modo a garantir o consentimento livre, expresso e informado.

7. REFERÊNCIAS BIBLIOGRÁFICAS

- ALMEIDA, Bethania de Araujo et al. Personal data usage and privacy considerations in the COVID-19 global pandemic. *Ciência coletiva*, Rio de Janeiro, v. 25, supl. 1, p. 2487-2492, June. 2020. Available from <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702487&lng=en&nrm=iso>. Acesso em 10/05/2021. Epub Junho, 2020.
- ANDERSON, Bryan; O'BRIEN, Matt. COVID-19 exposure apps: Few states make coronavirus contact tracing smartphone tool available. *Usa Today, Providence*, 06 dez. 2020. Disponível em: <https://www.usatoday.com/story/tech/2020/12/06/coronavirus--contact-tracing-exposure-apps/3849099001/>. Acesso em 23/05/2021.
- APP, Corona Warn. KENNZAHLEN ZUR CORONA-WARN-APP. Disponível em: <https://www.coronawarn.app/assets/documents/2021-04-29-cwa--daten-fakten.pdf>. Acesso em 07/05/2021.
- BARBOSA, Alexandre; CARVALHO, Celina; STEIBEL, Fabro; COSTA, Janaina. Colombia's CoronApp. ITS, Rio de Janeiro, 26 maio 2020. Disponível em: <https://feed.itsrio.org/colombias-coronapp--5802ceb54b7>. Acesso em 23/05/2021.
- BECKER, Steffen. Akzeptanz von Corona-Apps in Deutschland vor der Einführung der Corona-Warn-App. Disponível em: <https://www.mobsec.ruhr-uni-bochum.de/media/mobsec/veroeffentlichungen/2020/06/29/corona_apps_de1_preprint_de.pdf>. Acesso em 07/05/2021.
- BBC. O plano chinês para monitorar – e premiar – o comportamento de seus cidadãos. BBC News. - 20 nov. 2017. Disponível em: <https://www.bbc.com/portuguese/internacional-42033007>. Acesso em 23/04/2021.
- BOXCRYPTOR. Data Protection in the German Corona-Warn-App: A Statement and our Approval. Disponível em: <https://www.boxcryptor.com/en/blog/post/corona-warn-app-data-protection/>. Acesso em 07/05/2021.
- BRASIL. Advocacia-Geral da União, Consultoria Geral da União. Parecer n. 00295/2020. EMENTA: CONSTITUCIONAL. ADMINISTRATIVO. CONTROLADORIA-GERAL DA UNIÃO (CGU). TRANSPARÊNCIA COMO REGRA. SIGILO COMO EXCEÇÃO. PUBLICIDADE NA ADMINISTRAÇÃO PÚBLICA. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). TRATAMENTO DE DADOS PELO PODER PÚBLICO. COMPARTILHAMENTO E DIVULGAÇÃO DE DADOS PESSOAIS. PARECER n. 00295/2020/CONJUR-CGU/CGU/AGU, Brasília, 16 out. 2020. Disponível em: <https://repositorio.cgu.gov.br/bitstream/1/63575/5/Parecer_295_2020_CONJUR_CGU_CGU_AGU.pdf>. Acesso em: 30 mar. 2021.
- BRASIL. Lei nº 13.709, de 14 de agosto de 2020. Lei Geral de Proteção de Dados Pessoais (LGPD). Lei Geral de Proteção de Dados, Brasília, 14 ago. 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 30 mar. 2021.
- BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.
- CAIXA ECONÔMICA FEDERAL, Aviso de Privacidade. Disponível em: <https://www.caixa.gov.br/privacidade/aviso-de-privacidade/Paginas/default.aspx>. Acesso em 15/06/2021.
- CETIC.BR. Celular é o dispositivo mais utilizado por usuários de Internet das classes DE para ensino remoto e teletrabalho, revela Painel TIC COVID-19. Novembro, 2020. Disponível em: <https://cetic.br/pt/noticia/celular-e-o-dispositivo-mais-utilizado-por-usuarios-de-internet-das-classes-de--para-ensino-remoto-e-teletrabalho-revela-painel-tic-covid-19/>. Acesso em 15/06/2021.
- COLÔMBIA, Governo da. *CoronApp*. Disponível em: <https://coronaviruscolombia.gov.co/Covid19/aislamiento-saludable/coronapp.html>. Acesso em 17/05/2021.
- CONECTA JÁ PROTESTE. Veja como são as leis de proteção de dados nos Estados Unidos. Disponível em: <https://conectaja.proteste.org.br/veja-como--sao-as-leis-de-protecao-de-dados-nos-estados--unidos/>. Acesso em 23/05/2021.

- DAVE, Paresh; NELLIS, Stephen. *Colombia's coronavirus app troubles show rocky path without tech from Apple, Google*. Reuters, São Francisco, 06 maio 2020. Disponível em: <https://www.reuters.com/article/us-health-coronavirus-colombia-apps/colombias-coronavirus-app-troubles-show-rocky-path-without-tech-from-apple-google idUSKBN22J03W?feedType=RSS&feedName=internetNews>. Acesso em 17/05/2021.
- DAVIDSON, Helen. China's coronavirus health code apps raise concerns over privacy. *The Guardian*. -01 abr. 2020. Disponível em: <https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy>. Acesso em 23/04/2021.
- EGÍDIO, Mariana. Protecção de dados em tempos de COVID-19-Breves reflexões. Revista Eletrônica de Direito Público, VOL. 7 Nº 1. Abril, 2020.
- FAPESP. 28% dos idosos em SP não têm celular e se isolam da tecnologia em plena pandemia. Abril, 2020. Disponível em: <http://jornaldoporto.inf.br/noticia/4615/28-dos-idosos-em-sp-nao-tem-celular-e-se-isolam-da-tecnologia-em-plena-pandemia.html>. Acesso em 15/06/2021.
- FERRAZ JÚNIOR, T. S.. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista Da Faculdade De Direito*, Universidade De São Paulo, 88, 439-459, 1993.
- G1. Recife rastreia 700 mil celulares para monitorar isolamento social e direcionar ações contra coronavírus. Disponível em: <https://g1.globo.com/pe/pernambuco/noticia/2020/03/24/recife-rastreia-700-mil-celulares-para-monitorar-isolamento-social-e-direcionar-acoes-contra-coronavirus.ghtml>. Acesso em 15/06/2021.
- GABRIEL, Anderson de Paiva. DAVID, Ivana. Tecnologias de 'contact tracing' e a proteção dos dados de localização: Quem é, contemporaneamente, o Leviatã de Hobbes?. JOTA. Junho, 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/juiz-hermes/tecnologias-de-contact-tracing-e-a-protecao-dos-dados-de-localizacao-22062020>. Acesso em 15/06/21.
- GAN, Nectar; CULVER, David. China usa QR code digital para combater o coronavírus. Saiba como funciona. CNN Brasil. *Hong Kong*, p. 1-1. 20 abr. 2020. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/2020/04/20/china-usa-qr-code-digital-para-combater-o-coronavirus-saiba-como-funciona>. Acesso em 23/04/2021.
- GOMES, Alessandra; LUCIANO, Maria; FRAGOSO, Nathalie; PAVARIN, Victor. COVID-19: Apps do governo e seus riscos à privacidade. 2020. Disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/covid-19-apps-do-governo-e-seus-riscos/>. Acesso em 17/05/2021.
- GOMES, Alessandra. LUCIANO, Maria. FRAGOSO, Nathalie. PAVARIN, Victor. COVID-19: Apps do governo e seus riscos à privacidade. InternetLab. Abril, 2020. Disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/covid-19-apps-do-governo-e-seus-riscos/>. Acesso em 15/06/2021.
- HAN, Byung-Chul. O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han. *El País*. 22 mar. 2020. Disponível em: <https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html>. Acesso em 21/04/2021.
- HAN, Byung-Chul. Por que a Ásia está melhor que a Europa na pandemia? O segredo está no civismo. *El País*. 30 out. 2020. Disponível em: <https://brasil.elpais.com/internacional/2020-10-30/por-que-a-asia-esta-melhor-que-a-europa-na-pandemia-o-segredo-esta-no-civismo.html>. Acesso em 21/04/2021.
- HARARI, Yuval Noah. The world after coronavirus. Financial Times. *London*. 20 mar. 2020. Disponível em: <https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75#comments-anchor>. Acesso em 21/04/2021.
- HINCH, Robert. Effective Configurations of a Digital Contact Tracing App: A report to NHSX. Disponível em: <https://www.semanticscholar.org/paper/Effective-Configurations-of-a-Digital-Contact-App%3A-Hinch-Probert/1c1adf321f56da38cab0826a29812b696471ed0b>. Acesso em 07/05/2021.
- JIYEON, Kim; RICHARDS, Neil. South Korea's COVID Success Stems From Earlier Lessons in Managing MERS. The Wire. 27 fev. 2021. Disponível

em: <https://science.thewire.in/health/south-koreas-covid-success-stems-from-earlier-lessons-in--managing-mers/>. Acesso em 23/04/2021.

- JOO, Jaehun; SHIN, Matthew Minsuk. Resolving the tension between full utilization of contact tracing app services and user stress as an effort to control the COVID-19 pandemic. -: Springer, 2020. Disponível em: <https://link.springer.com/content/pdf/10.1007/s11628-020-00424-7.pdf>. Acesso em 21/04/ 2021.
- KANG, Hyunjin; KWON, Soonman; KIM, Eunkyoung. COVID-19 Health System Response Monitor. -: Asia Pacific Observatory On Health Systems And Policies, 2020. Disponível em: <https://apps.who.int/iris/bitstream/handle/10665/337371/9789290228219-eng.pdf?sequence=1&isAllowed=y>. Acesso em: 23/04/2021.
- KENT, Chloe. What is the future of the NHS COVID-19 app? Medical Device Network. 02 mar. 2021. Disponível em: <https://www.medicaldevice-network.com/features/nhs-covid-19-app/>. Acesso em: 07/05/2021.
- MADDEN, Mary. Americans Consider Certain Kinds of Data to be More Sensitive than Others. Pew Research Center, Washington, v. 1, n. 1, p. 1-1, 12 nov. 2014. Disponível em: <https://www.pewresearch.org/internet/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more--sensitive-than-others/>. Acesso em 23/05/2021.
- MILLER, Arthur. Transcription of the 1st Meeting Part I of the Secretary's Advisory Committee on Automated Personal Data Systems of the U.S. Department of Health, Education and Welfare, p. 267.
- NATIONAL CYBER SECURITY CENTRE. NHS COVID-19: the new contact-tracing app from the NHS. Disponível em: <https://www.ncsc.gov.uk/information/nhs-covid-19-app-explainer>. Acesso em 07/05/2021.
- NHS. NHS COVID-19. Disponível em: <https://www.nhs.uk/apps-library/nhs-covid-19/>. Acesso em 07/05/2021.
- ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos, 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em 30/03/2021.
- PALHARES, Gabriela Capobianco; DOS SANTOS, Alessandro Santiago; ARIENTE, Eduardo Altomare; DE OLIVEIRA GOMES, Jefferson. *A privacidade em tempos de pandemia e a escada de monitoramento e rastreio*. 2020. DOI: 10.1590/S0103-4014.2020.3499.011.
- RICH, Jessica. How our outdated privacy laws doomed contact-tracing apps. Brookings, *Georgetown*, v. 1, n. 1, p. 1-1, 28 jan. 2021. Disponível em: <https://www.brookings.edu/blog/techtank/2021/01/28/how-our-outdated-privacy-laws-doomed-contact-tracing-apps/>. Acesso em 23/05/2021.
- RODOTÀ, Stefano. *A vida na sociedade da vigilância - a privacidade hoje*. Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.
- SUPREMO Tribunal Federal. ADI nº 6.387/DF. Relator: Ministra Rosa Weber. Disponível em: <https://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5895165>.
- THE FEDERAL GOVERNMENT. *Coronavirus warning app*. Disponível em: <https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-englisch/helps-us-in--the-fight-against-corona-1759110>. Acesso em 07/05/2021.
- UOL. Brasil breca alta de pessoas fora de casa, mas índice segue abaixo de 45%. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/05/18/lockdown-brasil-registra-alta--no-indice-de-isolamento-social-pela-1-vez.html>. Acesso em 15/06/2021.
- WAGNER, Von Gert; KÜHNE, Simon; SIEGEL, Nico. Akzeptanz der einschränkenden Corona--Maßnahmen bleibt trotz Lockerungen hoch. Diw Berlin, Berlin, n. 35, 23 abr. 2020. Disponível em: <https://www.diw.de/documents/publikationen/73/diw_01.c.761946.de/diw_aktuell_35.pdf>. Acesso em: 07/05/2021.
- WARREN, Samuel D; BRANDEIS, Louis D. "The Right to Privacy." *Harvard Law Review*, vol. 4, no. 5, 1890, pp. 193–220. JSTOR. Available from <http://www.jstor.org/stable/1321160>. Accessed 6 March 2021.

8. ANEXO - MAPEAMENTO COMPLETO DOS *APPS* UTILIZADOS NO BRASIL NO COMBATE À PANDEMIA DA COVID-19

APLICATIVO[127] REGIÕES DE ATUAÇÃO	Coronavírus SUS Federal
CONSENTIMENTO	Possui Termo de Consentimento e Política de Privacidade. Este consentimento poderá ser revogado pelo titular a qualquer momento. Não é necessário realizar nenhum pré-cadastro antes de acessar as políticas de privacidade do app. No documento é colocado que modificações no aplicativo e nos termos de uso poderão ocorrer e a menos que indique ao contrário, seu uso da aplicação indica a aceitação integral do termos de uso naquele versão vigente cada vez que for utilizado o Coronavírus SUS pelo usuário, explicitando que o usuário deve ficar atento às atualizações.
FINALIDADE	Acerca dos dados recolhidos pelo app: (i) o app não coleta dados do seu perfil como nome, sobrenome, data de nascimento, endereço, número de telefone e endereço de e-mail; (ii) não coleta nenhum dado de geolocalização, portanto movimentos não são rastreados; (iii) os dados salvos no seu smartphone e as conexões com o servidor são criptografados; (iv) seus dados são salvos em servidores no Brasil, gerenciados por órgãos públicos e mantido pelo Ministério da Saúde. Acerca da finalidade, expressa na Política de Privacidade do app tem-se os seguintes pontos: (i) identifique e entre em contato com o titular podendo informar que esteve em contato com o usuário que descobriu estar infectado; (ii) contate os usuários que estiveram em contato com o titular do dado, em face de descoberta que o mesmo identificou estar infectado com o vírus. Revelam que os dados só serão utilizados para alertar os usuários em relação ao contato com a COVID-19, como exposto nas finalidades, além da forma agregada e anônima com o objetivo de saúde pública, profilaxia, estatística ou pesquisa científica. Utilização de contact tracing, através do bluetooth, sem utilizar geolocalização ou monitoramento.
SEGURANÇA	Não serão realizados compartilhamentos dos dados com nenhuma outra instituição, sendo pública ou privada, acerca das chaves identificadoras O Ministério da Saúde se responsabiliza pela manutenção das medidas de segurança, 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 qualquer outra forma de tratamento inadequado e ilícito.

127 Todas as informações da tabela foram retiradas através do uso dos apps e, quando possuem, de suas políticas de privacidade.

SEGURANÇA	São colocados como responsáveis pelas consequências que resultem do fornecimento intencional de dados incorretos, e responsáveis pela segurança dos dados pessoais.
TÉRMINO DE USO	Garantem o sigilo e anonimato de todas as informações produzidas pelo utilizador do app. O termo deixa claro que o Ministério da Saúde poderá manter e tratar os dados do Titular durante todo o período que os mesmos forem pertinentes ao alcance das finalidades já listadas. Por fim, dados pessoais anonimizados poderão ser mantidos por período indefinido.

APLICATIVO REGIÕES DE ATUAÇÃO	**Caixa - Auxílio Emergencial** Federal
CONSENTIMENTO	Não há Política de Privacidade específica para esse aplicativo e não há Termo de Consentimento. É aplicado uma Política de Privacidade geral para todos os serviços que recolhem dados da Caixa, intitulada Aviso de Privacidade. A Política de Privacidade não está disponível no aplicativo e é necessário uma busca para acessar esse documento da Caixa.
FINALIDADE	Para acompanhar o seu benefício é necessário informar nome completo, CPF, data de nascimento e nome da mãe. Além disso, a Política de Privacidade informa que há dados coletados automaticamente quando você navega no site ou utiliza os aplicativos, inclusive por meio do uso de cookies. A justificativa é proporcionar comodidade, segurança na navegação e aprimorar os canais do banco Algumas finalidades para as quais a Caixa seus dados pessoais: (i) Realizar as atividades necessárias à execução dos contratos de produtos ou serviços que o banco tem com o consumidor/usuário, inclusive em procedimentos preliminares às contratações; (ii) Operar políticas públicas; (iii) Responder as dúvidas, solicitações, reclamações ou elogios; (iv) Verificar a identidade do usuário, visando evitar fraudes, atividades ilegais ou não autorizadas; (v) Comunicar, administrar e oferecer conteúdo e benefícios direcionados e específicos ao seu perfil e que podem ser do interesse do usuário; (vi) Enviar informações administrativas ao usuário, como termos, condições, políticas e contratos; (vii) Desenvolver novos canais, serviços ou produtos e realizar melhorias naqueles que o usuário já utiliza; (vii) Proteger a CAIXA, seus empregados, parceiros, clientes e mercado, incluindo as atividades relacionadas ao crédito; (viii) Monitorar, analisar as tendências, medir audiências, corrigir problemas e evoluir o uso do site e aplicativos; (ix) Atender a determinações legais ou regulatórias.

SEGURANÇA	A Caixa diz oferecer as mais avançadas ferramentas para evitar alteração, fraude, divulgação ou destruição das informações que detém, como criptografia com a utilização de SSL (Secure Socket Layers) e firewalls. Também diz oferecer uma verificação em duas etapas para acesso à sua conta ou aos aplicativos da CAIXA, bem como recursos de navegação segura. Diz monitorar constantemente os sistemas para proteção contra acessos não autorizados, garantindo sigilo dos dados do usuário. Qualquer tentativa de invasão e uso deliberadamente malicioso do site, aplicativos e marcas da CAIXA e parceiros serão tratados e tipificados conforme a Lei Penal determina. Ressalta que, em caso de incidente de segurança com dados pessoais que possam acarretar risco ou dano relevante, o usuário será informado pela CAIXA. Em algumas situações, a CAIXA expressa que precisará compartilhar dados pessoais dos usuários com terceiros (tais como Autoridades, entidades governamentais e órgãos reguladores) para cumprir com obrigação legal ou regulatória. Em outras situações, a CAIXA diz que precisará compartilhar os dados a fim de exercer as atividades necessárias para prestar serviços com qualidade, destaca-se: (i) Órgãos e entidades da Administração Pública para a execução de políticas públicas; (ii) Empresas subsidiárias, visando a melhoria de serviços ou produtos que beneficiem o usuário; (iii) Empresas que prestam serviços e funcionalidades para o banco, como agências de marketing e publicidade, com o intuito de oferecer conteúdos mais adequados aos interesses e necessidades do usuário; (iv) Utilização do Google Analytics.
TÉRMINO DE USO	No Aviso de Privacidade fica expresso que cada produto ou serviço da CAIXA possui um tempo de vida e obedece a legislações específicas. É dito que não será tratado e nem armazenado dados por mais tempo que o necessário para a finalidade a que foram destinados, incluindo o período adicional indicado por lei ou regulação a que nos submetemos. Porém, não há indicação de até quando os dados fornecidos no app de Auxílio Emergencial serão especificamente tratados e armazenados.

APLICATIVO REGIÕES DE ATUAÇÃO	**Monitora COVID-19** Região do Nordeste (único *app* que é iniciativa privada)
CONSENTIMENTO	Não possui Política de Privacidade própria. O consentimento é entendido pelo app no momento em que há o fornecimento dos dados pessoais. Segundo o termo, após a realização dessas ações compreende-se que o usuário está de acordo com a coleta de dados a serem utilizados pela empresa. A Política de Privacidade pode ser revisada a qualquer momento e as alterações e esclarecimentos que surtirão efeito imediatamente após sua publicação no site. No caso de alterações materiais, a empresa se compromete a notificar o usuário daquilo que foi alterado, mantendo-o ciente das informações coletadas, seus usos, e sob que circunstâncias elas serão divulgadas.

FINALIDADE	Não há menção sobre finalidade na Política de Privacidade do app. Os dados coletados pelo app são: nome, e-mail, endereço, localização, protocolo de internet do computador e endereço de IP.
SEGURANÇA	Sobre compartilhamento com terceiros, parte dos serviços prestados pelo desenvolvedor são terceirizados e, para que possam executar suas funções há o compartilhamento dos dados com essas empresas. No termo consta que essas empresas irão apenas coletar, usar e divulgar as informações na medida do necessário para permitir que eles realizem os serviços que eles nos fornecem. A maneira com a qual esses terceirizados usaram essas informações deve ser vista no termo de cada um deles. Sobre os mecanismos de segurança, o app diz que são tomadas precauções razoáveis e seguidas as melhores práticas da indústria para que as informações não sejam perdidas inadequadamente, usurpadas, acessadas, divulgadas, alteradas ou destruídas
TÉRMINO DE USO	Sobre se o sigilo/anonimato dos dados é garantido, não há determinação explícita na Política de Privacidade. Não há previsão expressa do término de uso de dados.

APLICATIVO REGIÕES DE ATUAÇÃO	**Minha Saúde** Federal
CONSENTIMENTO	Possui Política de Privacidade e Termos de Uso. Os Termos de Uso sofrem ajuste periódico, e o usuário se responsabiliza por observar estas atualizações. A equipe do App Minha Saúde poderá informar ao usuário sobre alterações significativas neste instrumento, através de avisos nas interfaces.
FINALIDADE	Os dados são coletados de duas formas: (i) dados fornecidos pelo usuário; e (ii) dados coletados automaticamente pelo Sistema. Dados fornecidos pelo usuário: são coletados todos os dados inseridos espontaneamente pelo usuário, como as informações cadastrais fornecidas para criação da conta de acesso ao Sistema, bem como os dados inseridos durante a utilização do Sistema, pelo preenchimento de campos e/ou inclusão de informações. Estes serão divididos em sensíveis ou não sensíveis. Dados coletados automaticamente pelo Sistema: São informações coletadas pelo sistema, independentemente do fornecimento pelo usuário. A cada acesso são obtidos alguns dados automaticamente, tais como, mas não se limitando a, características do dispositivo de acesso, número IP com informação de data e hora, origem do IP, funcionalidades acessadas, informações sobre cliques, entre outros. Podem ser utilizadas na coleta de tais dados algumas tecnologias padrões, como cookies, pixel tags, beacons e local shared objects, que servem para identificar o usuário e tornar seu acesso mais rápido, bem como para gerar os painéis de business intelligence (BI) e assim proporcionar uma melhor experiência na utilização do App Minha Saúde.

FINALIDADE	O usuário concorda com a utilização dessas ferramentas tecnológicas para tornar possível a utilização do sistema. O app diz que a Política de Privacidade apresentará sua "finalidade", mas não menciona nenhuma finalidade do tratamento e uso dos dados. O trecho abaixo aparenta ser o que melhor descreveria tal finalidade: Os dados tratados através do Minha Saúde podem ser usados por seus clientes (controladores) para os fins de controle e automação da gestão pública, bem como para o desenvolvimento de políticas públicas; ou pela licenciante com fins de pesquisa e desenvolvimento do sistema seguindo as normas de conformidade aplicáveis e a LGPD (Lei Geral de Proteção de Dados), respeitada a anonimização dos dados, sem qualquer relação financeira ou societária com os gestores públicos e/ou usuários.
SEGURANÇA	Sobre o compartilhamento de terceiros, as informações constantes poderão ser repassadas a terceiros, de forma gratuita, ou onerosa. Importante que o usuário esteja ciente também de que, caso o App Minha Saúde passe por integrações, seja unificado, vendido (no todo ou em parte), ou deixe de operar, as informações dos usuários comporão os ativos transferidos ou adquiridos por terceiros. Neste caso, mesmo as informações sensíveis serão repassadas a terceiros, de modo a permitir a continuidade da utilização do Software, principalmente nos contratos em andamento. As informações do Usuário, sensíveis ou não, serão guardadas de forma sigilosa, e qualquer funcionário ou prestador de serviços que entre em contato com elas se compromete com um Acordo de Confidencialidade e a não desvirtuar a sua utilização, bem como não usar de modo destoante do previsto nesta Política de Privacidade e Proteção de Dados e nos Termos de Uso. Serão empregados todos os esforços e meios disponíveis no mercado, que sejam razoáveis, para garantir a segurança dos referidos dados no sistema. Para que tais medidas se tornem viáveis, são adotadas, não se limitando a, as seguintes precauções na guarda e tratamento das informações dos Usuários: a) utilização dos métodos mais confiáveis de segurança; b) proteção contra acesso não autorizado no sistema; c) proteção contra acesso não autorizado ao armazenamento das informações; d) aqueles que entrarem em contato com as informações deverão se comprometer a manter sigilo absoluto; e) quebra do sigilo acarretará responsabilidade civil e o responsável será processado nos moldes da legislação brasileira. Tais precauções, no entanto, não garantem integralmente que todas as informações que trafegam no Sistema não sejam acessadas por terceiros mal intencionados, por meio de métodos desenvolvidos para obter informações de forma indevida. Em razão disso, a equipe do App Minha Saúde não se responsabiliza por tais acessos ilícitos e sobre eles terá também direito de regresso. A equipe do App Minha Saúde não se responsabiliza por atos de terceiros que coletem ou utilizem indevidamente, por quaisquer meios, dados cadastrais e informações disponibilizadas no sistema fornecidas indevidamente pelo

SEGURANÇA	usuário. Porém, tomará todas as medidas técnicas e administrativas cabíveis para impedir esta divulgação. Tais como incluir alertas de segurança de informações nos treinamentos presenciais e observar atividades suspeitas no uso do software.
TÉRMINO DE USO	Todas as informações coletadas são tratadas como confidenciais e sempre que possível, uma vez que serão priorizados o interesse e finalidade públicos, serão anonimizados. Os dados só serão identificáveis quando houver interesse público nesta leitura, sabendo que o levantamento de dados serve à Administração Direta e/ou Indireta. É dever da equipe entregar os resultados obtidos com a utilização do App Minha Saúde para a Administração Pública. A equipe técnica de proteção de dados agirá sempre com o intuito de entregá-los anonimizados, exceto quando tal entrega inviabilizar leitura específica necessária ao interesse público. Não há previsão expressa do término de uso de dados.

APLICATIVO REGIÕES DE ATUAÇÃO	**Atende em Casa** Estado de PE
CONSENTIMENTO	Não tem Política de Privacidade
FINALIDADE	Dados recolhidos: CPF, CEP. Não deixa as finalidades explícitas.
SEGURANÇA	Não prevê término de dados. Não há expressa questões de segurança.
TÉRMINO DE USO	Não há questões expressas sobre término de uso.

APLICATIVO REGIÕES DE ATUAÇÃO	**Saúde Osasco** Município de Osasco
CONSENTIMENTO	O app não existia no início da pandemia e, atualmente, não se encontra mais disponível. Não foi possível encontrar informações a respeito da Política de Privacidade desse app.
FINALIDADE	Não há informações sobre o fim do app e dos dados que haviam sido coletados por ele.
SEGURANÇA	Não há informações sobre o fim do app e dos dados que haviam sido coletados por ele.
TÉRMINO DE USO	Não há informações sobre o fim do app e dos dados que haviam sido coletados por ele.

APLICATIVO REGIÕES DE ATUAÇÃO	**Saúde Online Paraná** Estado do PR
CONSENTIMENTO	Possui Política de Privacidade própria, Termos de Uso, Termo de Consentimento para tratamento de dados pessoais e Termo de Consentimento para telemedicina.
FINALIDADE	O tratamento dos dados pessoais tem as seguintes finalidades: (i) Possibilitar que o usuário responda questionários de saúde para avaliação de pacientes com suspeitas de COVID- 19 e outras doenças; (ii) Possibilitar que o usuário, caso tenha COVID-19 e outras doenças, possa contar com a orientação de profissionais da área da saúde, para fins de fornecer orientações e aconselhamentos relacionados à saúde; (iii) Possibilitar a triagem prévia para o atendimento através da autoavaliação feita pelo usuário e, por consequência, garantir maior agilidade no diagnóstico e solução do problema; (iv) Possibilitar o agendamento de teleconsultas. Dados recolhidos: nome completo, data de nascimento, número e imagem do RG, CPF, número da Carteira Nacional de Saúde, fotografia 3x4, para biometria facial, gênero, endereço completo, dados referentes à saúde, telefone, WhatsApp, e-mail, celular, nome de usuário e senha específicos para uso. Termos e políticas podem ser alterados sem avisar os usuários e, por estarem cadastrados na plataforma, eles concordam automaticamente com isto.
SEGURANÇA	O Controlador responsabiliza-se pela manutenção de medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito. Em conformidade ao art. 48 da Lei nº 13.709/2018, o Controlador comunicará ao Titular e à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao Titular. O Controlador fica autorizado a compartilhar os dados pessoais do Titular com outros agentes de tratamento de dados, caso seja necessário para as finalidades listadas neste termo, observados os princípios e as garantias estabelecidas pela Lei nº 13.709/2018.
TÉRMINO DE USO	Sobre o término de uso de dados: o Controlador poderá manter e tratar os dados pessoais do Titular durante todo o período em que os mesmos forem pertinentes ao alcance das finalidades listadas neste termo. Dados pessoais anonimizados, sem possibilidade de associação ao indivíduo, poderão ser mantidos por período indefinido. O Titular tem direito a obter do Controlador, em relação aos dados por ele tratados, a qualquer momento e mediante requisição: (...) IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei nº 13.709/2018. O Titular poderá solicitar via e-mail ou correspondência ao Controlador, a qualquer momento, que sejam eliminados os dados pessoais não anonimizados do Titular.

TÉRMINO DE USO	O Titular fica ciente de que poderá ser inviável ao Controlador continuar o fornecimento de produtos ou serviços ao Titular a partir da eliminação dos dados pessoais.

APLICATIVO REGIÕES DE ATUAÇÃO	**Coronavírus SP / e-Saúde SP** Estado de SP
CONSENTIMENTO	Possui Política de Privacidade própria. Dispõe que as modificações na Política de Privacidade estão sujeitas à alterações sem aviso prévio.
FINALIDADE	Finalidade: gestão da interação do profissional de saúde com o paciente e com outros profissionais através do fornecimento de ferramentas para tal finalidade. Não há informação a respeito dos dados coletados pelo app.
SEGURANÇA	Compartilhamento com terceiros: os dados poderão ser usados em pesquisas e servir de base para políticas públicas (em conformidade com as diretrizes da SMS-SP. Mecanismos de segurança: criptografia de banco de dados, individualização e separação completa dos módulos de dados cadastrais e dados pessoais, assim como o de pessoais sensíveis.
TÉRMINO DE USO	Não há menção em relação ao término de uso de dados. Não há menção em relação à anonimização e sigilo de dados.

APLICATIVO REGIÕES DE ATUAÇÃO	**Cachoeirinha Contra o Coronavírus** Estado do RS
CONSENTIMENTO	Possui Política de Privacidade própria. Não há menção sobre modificações nas Políticas de Privacidade.
FINALIDADE	Sobre os dados coletados, não há informação direta, mas há geração de um localizador de endereço, além da possibilidade de relatar sintomas e quadro clínico. Não há especificação sobre a finalidade.
SEGURANÇA	Não há menção sobre os mecanismos de segurança. Não há menção sobre compartilhamento com terceiros.
TÉRMINO DE USO	Não há menção ao término de uso de dados. O anonimato e o sigilo dos dados são garantidos de acordo com o app.

TRANSPARÊNCIA NO TRATAMENTO DE DADOS POR UIFS:

EM BUSCA DE UM BENCHMARK

TRANSPARÊNCIA NO TRATAMENTO DE DADOS POR UIFS: EM BUSCA DE UM BENCHMARK

André Bialski
Antonio Vento
Eduardo Messina
Oliver Wiegerinck

1. APRESENTAÇÃO

1.1. PROJETO MULTIDISCIPLINAR

No 5º Semestre do curso de Direito da FGV Direito SP, os alunos são incentivados a participar dos chamados Projetos Multidisciplinares, que envolvem diversos ramos do Direito e cujo intuito é não somente capacitá-los para a visão multidisciplinar dos problemas jurídicos como também os incentivar a desenvolver habilidades de pesquisa, liderança e trabalho em grupo.

O presente relatório é um dos produtos finais do Projeto Multidisciplinar desenvolvido no primeiro semestre de 2021, cujo tema foi "Proteção de Dados e Segurança Pública", ministrado pelas Professoras Eloísa Machado de Almeida e Heloisa Estellita, com auxílio do estagiário acadêmico Douglas Norkevicius e da mestranda e monitora Bárbara Prado Simão.

O Projeto foi dividido em três ciclos: exploratório, de estruturação e de produção. O primeiro ciclo foi focado na introdução do tema aos alunos, com encontros com convidados especializados em assuntos relevantes para o projeto. Na etapa de estruturação, os alunos se dividiram em grupos propondo produtos alinhados ao tema do Projeto e, então, na terceira etapa, partiram para a pesquisa e produção do texto.

Este grupo decidiu explorar o tema do tratamento de dados pessoais pelas Unidades de Inteligência Financeira (adiante, UIFs) sob o ponto de vista da transparência. A meta final era a construção de um *benchmark* indicando padrões de avaliação de transparência e tratamento de dados por essas entidades.

1.2. AGRADECIMENTOS A PARCEIROS E ENTREVISTADOS

Os Projetos Multidisciplinares se desenvolvem sempre em parceria e trabalho conjunto com alguns profissionais, pesquisadores ou entidades que estejam envolvidos com o tema analisado. Para o presente trabalho, gostaríamos de agradecer imensamente as professoras Heloisa Estellita e Eloísa Machado de Almeida por todo o auxílio, colaboração e inestimáveis ensinamentos e sugestões e ainda gostaríamos agradecer as professoras por toda a experiência do Projeto, que foi extremamente frutífera e enriquecedora para todo o grupo. Agradecemos os monitores Douglas Norkevicius e Barbara Prado Simão pelo acompanhamento e ajuda para que este relatório se tornasse realidade.

Agradecemos, ainda, aos convidados e às convidadas que participaram do Projeto por meio de aulas e palestras acerca da proteção de dados na segurança pública e persecução penal: Nathalie Fragoso (InternetLab); João Paulo Dorini (Defensor Regional de Direitos Humanos em São Paulo, DPU); Fernanda Campagnucci (Open Knowledge Brasil); Bruno Bioni (Data Privacy Brasil).

Por fim, nossos agradecimentos a Ana Carolina Carlos de Oliveira e a Ricardo Liao que forneceram informações fundamentais sobre tratamento de dados pelas UIFs por meio de entrevistas escritas. Ana Carolina Carlos de Oliveira é doutora pela USP e pela Universidade Pompeu Fabra e tem trabalhando intensamente com o tema da lavagem de capitais em uma série de publicações, merecendo destaque sua contribuição à obra "National and International Anti-Money Laundering Law: Developing the Architecture of Criminal Justice, Regulation and Data Protection"[128]. Ricardo Liao, hoje Presidente do COAF, trabalha no órgão há muitos anos onde já desempenhou a função de diretor de supervisão e conhece por dentro e profundamente a operação da Unidade.

128 VOGEL, Benjamin; MAILLART, Jean-Baptiste (ed.). *National and International Anti-Money Laundering Law: Developing the Architecture of Criminal Justice, Regulation and Data Protection*. Cambridge, Antwerp, Chicago: Internetlab, 2020, p. 399 ss.

2. INTRODUÇÃO E OBJETIVO

2.1. PREVENÇÃO E REPRESSÃO À LAVAGEM E A COLETA DE DADOS PESSOAIS

O termo "lavagem de dinheiro" ganhou popularidade nos anos 70, com o caso Watergate nos EUA, mas apenas nas últimas décadas tem adquirido relevância jurídica e econômica a ponto de unir diversos países do mundo em torno da mesma causa: buscar formas de coibir, prevenir e detectar operações de lavagem de capitais. O FMI estima que de 2% a 5% do PIB mundial é fruto de operações de lavagem de dinheiro[129]. No Brasil, segundo estimativa do Banco Central, de 2016, cerca de R$ 6 bilhões de reais são movimentados anualmente por meio de operações de lavagem[130]. Esses números evidenciam a magnitude do problema[131].

A preocupação com a lavagem de dinheiro levou diversos países a tomarem uma série de ações na tentativa de rastrear e desmantelar complexos esquemas - muitas vezes transnacionais - de encobrimento de bens oriundos da prática de crimes. O primeiro esforço foi feito durante a Convenção de Viena, em 1988, em que foram adotadas normas para combater a lavagem de dinheiro e o tráfico de drogas, ratificada pelo Brasil em 1991. Um ano depois, em 1989, foi criado o GAFI (Grupo de Ação Financeira; FATF em inglês), que funcionaria como um órgão internacional para atuação conjunta dos países-membros contra a lavagem de dinheiro. Em 1990, o GAFI publicou 40 (quarenta) recomendações que iriam nortear as ações e medidas que os países deveriam adotar. Em 1995, durante reunião na Bélgica, foi criado o Grupo de Egmont, principal mecanismo internacional de união, cooperação e intercâmbio de informações para a prevenção e repressão da lavagem de dinheiro. O objetivo deste Grupo seria atuar através das UIFs, formando uma rede de cooperação para a troca de informações. O Brasil se juntou ao Grupo de Egmont em 1999, um ano após a criação de sua UIF, o Conselho de Controle de Atividades Financeiras (adiante, COAF) por meio da Lei nº 9.613/98 (Lei de Lavagem de Dinheiro, adiante LLD), que dispõe sobre o crime de lavagem de dinheiro, a prevenção da utilização do sistema financeiro para a prática desse crime e cria o COAF (adiante, LLD).

O financiamento de grupos terroristas também passou a ser objeto de grande preocupação, estando diretamente ligado a transações e atividades econômicas ilícitas. Em junho de 2002, os países do G-8 assinaram o documento intitulado como "Recomendações Especiais sobre Financiamento do Terrorismo", em que são previstas recomendações especificas para o GAFI sobre o financiamento ao

129 United Nations Office on Drugs and Crime. *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*: research report. Research report. Disponível em: <https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf>. Acesso em: 10 maio 2021.

130 CAMPOS, Eduardo. *Lavagem de dinheiro movimenta R$6 bilhões por ano no Brasil, diz BC*. 2016. Disponível em: <https://valor.globo.com/financas/noticia/2016/11/17/lavagem-de-dinheiro-movimenta-r-6-bilhoes-por-ano-no-brasil-diz-bc.ghtml>. Acesso em: 20 maio 2021.

131 Crítico: ALLDRIDGE, Peter. *What Went Wrong With Money Laundering?* London: Palgrave Macmillan, 2016.

terrorismo. É interessante notar que as recomendações ligadas à lavagem de dinheiro andam lado a lado com a atuação governamental contra outros crimes como o terrorismo, a corrupção e o crime organizado. Isso é assim porque a incriminação da lavagem de dinheiro, como crime "acessório" ou "de conexão", é utilizada como instrumento para permitir o desfrute dos bens oriundos de crimes ou como meio para o financiamento do terrorismo.

Um dos instrumentos fundamentais para a prevenção e persecução penal da lavagem de dinheiro é a reunião de informações sobre atividades econômicas envolvendo bens, direitos ou valores produto de crimes. Para isso, as legislações nacionais têm obrigado aqueles que exercem certas atividades econômicas (pessoas obrigadas) a monitorar certas transações de seus clientes e a reportá-las à respectiva unidade de inteligência financeira quando detectarem sinais de possibilidade de lavagem de dinheiro[132]. Com esses esforços, as UIFs acabaram sendo repositório de imensa quantidade de dados pessoais, muitos deles protegidos também por sigilo financeiro, em evidente restrição a direitos fundamentais como a privacidade e a autodeterminação informacional. Se não se deseja frustrar a própria finalidade das UIFs, alguns dos tradicionais direitos dos titulares de dados pessoais como o direito de acesso, retificação e eliminação, por exemplo, devem ser objeto de restrição, ainda que temporária. Todavia, disso não deriva uma imunidade desses órgãos às exigências de respeito aos direitos dos titulares dos dados, como, por exemplo, a transparência.

132 Lei nº 9.613, de 3 de março de 1998: Art. 9.o Sujeitam-se às obrigações referidas nos arts. 10 e 11 as pessoas físicas e jurídicas que tenham, em caráter permanente ou eventual, como atividade principal ou acessória, cumulativamente ou não: I - a captação, intermediação e aplicação de recursos financeiros de terceiros, em moeda nacional ou estrangeira; II – a compra e venda de moeda estrangeira ou ouro como ativo financeiro ou instrumento cambial; III - a custódia, emissão, distribuição, liquidação, negociação, intermediação ou administração de títulos ou valores mobiliários. Parágrafo único. Sujeitam-se às mesmas obrigações: I – as bolsas de valores, as bolsas de mercadorias ou futuros e os sistemas de negociação do mercado de balcão organizado; II - as seguradoras, as corretoras de seguros e as entidades de previdência complementar ou de capitalização; III - as administradoras de cartões de credenciamento ou cartões de crédito, bem como as administradoras de consórcios para aquisição de bens ou serviços; IV - as administradoras ou empresas que se utilizem de cartão ou qualquer outro meio eletrônico, magnético ou equivalente, que permita a transferência de fundos; V - as empresas de arrendamento mercantil (leasing), as empresas de fomento comercial (factoring) e as Empresas Simples de Crédito (ESC); VI - as sociedades que efetuem distribuição de dinheiro ou quaisquer bens móveis, imóveis, mercadorias, serviços, ou, ainda, concedam descontos na sua aquisição, mediante sorteio ou método assemelhado; VII - as filiais ou representações de entes estrangeiros que exerçam no Brasil qualquer das atividades listadas neste artigo, ainda que de forma eventual; VIII - as demais entidades cujo funcionamento dependa de autorização de órgão regulador dos mercados financeiro, de câmbio, de capitais e de seguros; IX - as pessoas físicas ou jurídicas, nacionais ou estrangeiras, que operem no Brasil como agentes, dirigentes, procuradoras, comissionárias ou por qualquer forma representem interesses de ente estrangeiro que exerça qualquer das atividades referidas neste artigo; X - as pessoas físicas ou jurídicas que exerçam atividades de promoção imobiliária ou compra e venda de imóveis; XI - as pessoas físicas ou jurídicas que comercializem jóias, pedras e metais preciosos, objetos de arte e antiguidades. XII - as pessoas físicas ou jurídicas que comercializem bens de luxo ou de alto valor, intermedeiem a sua comercialização ou exerçam atividades que envolvam grande volume de recursos em espécie; XIII - as juntas comerciais e os registros públicos; XIV - as pessoas físicas ou jurídicas que prestem, mesmo que eventualmente, serviços de assessoria, consultoria, contadoria, auditoria, aconselhamento ou assistência, de qualquer natureza, em operações: a) de compra e venda de imóveis, estabelecimentos comerciais ou industriais ou participações societárias de qualquer natureza; b) de gestão de fundos, valores mobiliários ou outros ativos; c) de abertura ou gestão de contas bancárias, de poupança, investimento ou de valores mobiliários; d) de criação, exploração ou gestão de sociedades de qualquer natureza, fundações, fundos fiduciários ou estruturas análogas; e) financeiras, societárias ou imobiliárias; e f) de alienação ou aquisição de direitos sobre contratos relacionados a atividades desportivas ou artísticas profissionais; XV - pessoas físicas ou jurídicas que atuem na promoção, intermediação, comercialização, agenciamento ou negociação de direitos de transferência de atletas, artistas ou feiras, exposições ou eventos similares; XVI - as empresas de transporte e guarda de valores; XVII - as pessoas físicas ou jurídicas que comercializem bens de alto valor de origem rural ou animal ou intermedeiem a sua comercialização; e XVIII - as dependências no exterior das entidades mencionadas neste artigo, por meio de sua matriz no Brasil, relativamente a residentes no País."

2.2. A EXIGÊNCIA DE TRANSPARÊNCIA NO DIREITO DE PROTEÇÃO DE DADOS

A transparência é um dos princípios fundamentais na matéria de proteção de dados e, como tal, está prevista pela legislação brasileira e pela legislação da União Europeia, com especial destaque para a Diretiva Europeia 680/2016[133] e para o Regulamento Europeu 679/2016[134]. Primeiramente, quanto a LGPD, a transparência é referida como um dos princípios norteadores da atividade de tratamento de dados pessoais no art. 6º, inciso VI, como forma de "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento".

Quanto à Diretiva e ao Regulamento Europeu, ambos trabalham especificamente o tema do tratamento de dados pessoais. Assim como na LGPD, a transparência é classificada como um princípio do tratamento de dados pessoais pelo Regulamento Europeu 680/2016, em seu art. 5º parágrafo 1º, alínea a. A Diretiva Europeia 680/2016, apesar de não apresentar a transparência como um de seus princípios, se ocupa em apresentar disposições sobre como os processos das autoridades competentes devem ser pautados por ela, com especial destaque para o item 26 das considerações iniciais e o artigo 21, item 1.

Especificamente quanto ao tratamento de dados para fins das medidas de controle e prevenção de lavagem, parece haver um conflito entre a exigência de transparência e a de confidencialidade sobre a forma do tratamento de dados. Sobre isso, Ricardo Liao afirma: "entendo, na prática, que a Recomendação GAFI 21, abaixo transcrita, entre outras, revela um certo conflito de 'princípios' a serem observados pelos agentes públicos, uma vez que o dever de 'revelação e confidencialidade' ali estabelecido, a nosso ver, se colocaria em sobreposição ou confrontação aos objetivos da transparência do tratamento de dados. Nesse ambiente estamos tratando de informações sobre determinadas situações e não especificamente sobre dados das pessoas envolvidas".

133 European Parliament. *Directive (EU) 2016/680*. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680>. Acesso em: 23 maio 2021.

134 European Parliament. *Regulamento (EU) 2016/679*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679#:~:text=REGULAMENTO%20%28UE%29%202016%2F%20679%20DO%20PARLAMENTO%20EUROPEU%20E,de%20Dados%29%20I%20.%20%28Atos%20%20legislativos%29%20>. Acesso em 23 de maio de 2021

2.3. PROTEÇÃO DE DADOS PESSOAIS NO DIREITO POSITIVO BRASILEIRO E ATUAÇÃO DO COAF

A legislação brasileira relativa à proteção e o tratamento de dados pessoais é recente e tímida. Há apenas um diploma legal especificamente dedicado ao tema: a Lei n. 13.709/2018, Lei Geral de Proteção de Dados (adiante, LGPD). Existem outros diplomas legais que abordam, ainda que circunstancial e parcialmente, aspectos da proteção e do tratamento de dados[135], mas não lhes dão um tratamento amplo e sistemático como o dado pela LGPD.

Ao longo de seus capítulos, a LGPD se ocupa de classificar os diferentes tipos de dados, como estes serão tratados pelo poder público e pelos entes privados, quais são os direitos dos titulares, como será feita a fiscalização e ainda dispõe sobre dois órgãos governamentais responsáveis que terão, entre outras funções, zelar pela proteção e devido tratamento dos dados pessoais dos brasileiros. Esses órgãos são a Agência Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados e da Privacidade.

No que interessa a este trabalho, um dispositivo chama a atenção: o art. 4º, inciso III. Ali se prevê que as disposições da lei não se aplicarão ao tratamento de dados feito com fins exclusivos de (i) segurança pública; (ii) defesa nacional; (iii) segurança do Estado; ou (iv) atividades de investigação e repressão de infrações penais. Para esses casos, deverá ser aprovada uma lei especial, que se encarregue de tratar da matéria da proteção de dados no âmbito penal (resumidamente, segurança pública e persecução penal). Para isso, a Câmara dos Deputados criou, no final de 2019, uma Comissão de Juristas que apresentou um Anteprojeto em 5 de novembro de 2020[136]. Até a conclusão deste relatório, o Anteprojeto não havia sido transformado em projeto de lei.

Isso implica dizer que, a depender do entendimento que se adote quanto à natureza do tratamento de dados feito pela UIF brasileira (o Conselho de Controle de Atividades Financeiras, adiante apenas COAF), poderá ele estar ou não submetido aos ditames da LGPD e, pois, à exigência de transparência instituída no art. 6º, inciso VI, como visto.

135 Quanto aos demais dispositivos legais que mencionam o tema do tratamento e da proteção de dados, a Constituição traz em seu artigo 1º, III e 5º X preceitos sobre a privacidade e a dignidade da pessoa humana. O art. 21 do Código Civil também apresenta disposição semelhante, garantindo a inviolabilidade da privacidade. Já sobre o Código de Defesa do Consumidor, em seu artigo 43, prevê que o consumidor tem direito a saber que tipo de dados pessoais estão arquivados sobre ele. Esse dispositivo do CDC faz referência direta ao remédio constitucional, previsto pelo art. 5º LXXII, do Habeas Data, em que o cidadão pode interpelar o Estado para que esse apresenta os dados que têm sobre o mesmo indivíduo, um claro indicativo feita pela Carta Magna que nem mesmo o Estado Brasileiro pode reter dados de seus cidadãos sem qualquer tipo de contrapartida ou prestação de contas. Por fim, menciona-se o Marco Civil da Internet, regulamentado em 2015, que discute brevemente o tema em seu artigo 11º, em que se prevê a aplicação de legislação específica sobre o tema, que viria a ser a LGPD, aprovada em 2018.

136 Brasil. *Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal*. Disponível em: <https://www.conjur.com.br/dl/anteprojeto-lei-disciplina-protecao.pdf>. Acesso em: 26 de maio de 2021

Segundo o art. 3º da Lei nº 13.974, é atribuição do COAF produzir "inteligência financeira para a prevenção e o combate à lavagem de dinheiro". A conjunção deste dispositivo com o disposto nos artigos 4º, III, da LGPD, e 9, 11, 14 e 15 da Lei nº 9.613/98, em combinação com o disposto na Lei Complementar nº 105 de 2001, levou o órgão a entender que sua atuação não está abrangida LGPD, a não ser naquelas atividades que não tenham fim exclusivo de segurança pública ou persecução penal[137].

Como a discussão doutrinária sobre esse tema é ainda incipiente no Brasil[138], não encontramos opiniões contrárias ao entendimento adotado pelo COAF quanto à não incidência da LGPD sobre suas atividades de inteligência financeira.

Independentemente dessa discussão, a submissão do órgão ao princípio da transparência no tratamento de dados é apenas uma questão de tempo: seja por eventual prevalecimento de entendimento de sua submissão à LGPD ou ao menos a seus princípios gerais[139], portanto, *de lege lata*; seja pelo advento de uma LGPD "Penal", portanto, *de lege ferenda*. Por estas razões, é conveniente e desejável que a atuação da UIF brasileira seja examinada à luz dos melhores *standards* em transparência de tratamento, pois o exame pode lhe auxiliar no aperfeiçoamento em momento futuro, próximo ou distante.

Esclarecidos estes pontos e feitas as devidas ressalvas, é tempo de delimitar o objetivo deste trabalho e a metodologia utilizada para alcançá-lo.

137 Conselho de Controle de Atividades Financeiras. *Tratamento de Dados Pessoais sujeito à Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: <https://www.gov.br/coaf/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais>. Acesso em: 23 de maio de 2021.

138 BORGES, Ademar. O relatório de inteligência financeira como meio de obtenção de prova no processo penal. *Revista Brasileira de Ciências Criminais*. Vol. 176. Ano 29. p. 69-105. São Paulo: Ed. RT, fevereiro/2021.

139 Não custa lembrar, de um lado, que o STF já reconheceu a vigência de um direito fundamental à proteção de dados e à autodeterminação informacional, no julgamento da ADI 6387, que obrigam toda a Administração Pública, conforme a clareza do disposto nos arts. 5º, II, e 37 da CF.

2.4. OBJETIVO, METODOLOGIA E CLASSIFICAÇÃO DOS PAÍSES EXAMINADOS

Nosso objetivo é propor diretrizes para que nossa UIF, o COAF, possa atender ao comando de transparência sobre como trata os dados que coleta. Para isso, procederemos da seguinte maneira.

Partiremos de uma breve análise do que é uma UIF, quais são suas finalidades e como se dá o tratamento de dados pessoais por elas feito. Em seguida, faremos um exame mais detalhado de como a nossa UIF, o COAF, declara a maneira como trata dados.

Após a análise do COAF, é tempo de compará-lo com o tratamento de UIFs de outros países para a construção de um *benchmark* e também para comparação entre a transparência do tratamento de dados entre UIFs. Essa comparação ajudará a realizar um diagnóstico das informações dispostas no site do órgão nacional e identificar eventuais melhorias.

Para estes fins, examinamos países membros da União Europeia e do Grupo de Egmont. Esta escolha teve o intuito de restringir o número de países e acessar informações sobre países que têm uma base comum de responsabilidades e cooperação mútua. Quanto à União Europeia, ela foi selecionada por conta de sua vasta legislação relativa à prevenção de lavagem de capitais e proteção de dados pessoais. A Diretiva 849/2015[140], por exemplo, apresenta regulamentações para prevenir a lavagem e que devem ser adotadas por todos os países membros, assim como o Regulamento 2018/1725[141] que trata sobre o processamento de dados pessoais, ademais, há a *General Data Protection Regulation* – Regulamento (UE) 2016/679[142] – que versa sobre a proteção de dados e a Diretiva 680, sobre a proteção das pessoas naturais com relação ao processamento de dados pessoais por autoridades competentes, para a prevenção, investigação, detenção ou denúncia criminal[143]. Portanto, todas as nações que compõem a UE estão sujeitas ao cumprimento dessas regras, o que parece um bom ponto de partida para a escolha de todos os 27 Estados-membros. O Grupo Egmont, por sua vez, é composto por um total de 166 países que trabalham pelo intercâmbio de informações e de inteligência relativa ao combate e prevenção à lavagem de dinheiro, além de buscar agregar e melhorar a atuação das UIFs. O grupo reúne as maiores economias do mundo e também países alvos de pessoas e empresas que buscam lavar e mascarar a origem de capitais.

140 European Union. *Directive (EU) 2015/849 of the European Parliament and of the Council*. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849>. Acesso em: 19 maio 2021.

141 European Parliament. *Regulation (EU) 2018/1725 of the European Parliament and of the Council*. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725>. Acesso em: 19 maio 2021.

142 European Union. *General Data Protection Regulation*. Disponível em: <https://gdpr-info.eu>. Acesso em: 23 maio 2021.

143 European Parliament. *Directive (EU) 2016/680*. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680>. Acesso em: 23 maio 2021.

A partir destes critérios, foi reunida uma série de países cujas sites das UIFs seriam alvo da análise. Foi feito levantamento incluindo nações da América do Sul e Norte, juntamente com a Arábia Saudita, China, Japão e Rússia, bem como membros da União Europeia. Tais países foram escolhidos por serem potências econômicas e nações de grande representatividade geopolítica. Foram analisados os sites de 41 nações, dentre elas, 27 pertencentes à União Europeia – Alemanha, Áustria, Bélgica, Bulgária, Chipre, Croácia, Dinamarca, Eslováquia, Eslovênia, Espanha, Estônia, Finlândia, França, Grécia, Hungria, Irlanda, Itália, Letônia, Lituânia, Luxemburgo, Malta, Países Baixos, Polônia, Portugal, República Tcheca, Romênia e Suécia –, 10 das Américas – Argentina, Brasil, Canadá, Chile, Colômbia, Estados Unidos da América, México, Paraguai, Peru, Uruguai –, 4 da Ásia – Arábia Saudita, China, Japão e Rússia –, possibilitando uma base bastante considerável.

A seguir, definimos critérios para que pudéssemos avaliar o grau de transparência no tratamento de dados e elegemos os seguintes: (i) navegabilidade do site da UIF; (ii) disponibilidade de informações sobre tratamento de dados; (iii) disponibilidade de informações sobre a estrutura da UIF; e (iv) disponibilidade de informações sobre quais dados o cidadão pode exigir saber. Cada um destes critério tem um peso diferente: o primeiro tem peso dois, o segundo quatro, terceiro um e o quarto tem peso três. A diferença de peso decorreu da conclusão do grupo no sentido de que o segundo e o quarto critérios são mais relevantes para uma melhor transparência por parte das UIFs, enquanto o primeiro e terceiro são importantes para uma maior compreensão do que a UIF faz, mas não necessariamente refletem como é feito o tratamento e a proteção de dados, que é o cerne de nossa pesquisa.

A partir desses critérios, foi atribuída uma nota final calculada pela divisão por 10 (soma dos pesos) da soma da nota de cada critério multiplicado pelo seu peso. Segue figura para fins de maior clareza:

CRITÉRIO	NOTA 0-10	PESO	
Navegabilidade do site	W	2	→ wX2
Informações sobre tratamento de dados	X	4	→ xX4
Informações sobre estrutura da UIF	Y	1	→ yX1
Informações sobre quais dados o cidadão pode requerer	Z	3	→ zX3

$$\frac{wX2 + xX4 + yX1 + zX3}{10} = \text{Nota final de 0 a 10}$$

soma dos pesos

Uma vez calculadas as notas, os países foram distribuídos em cinco categorias. A Categoria I é composta pelos países que apresentam nota superior a 8; a Categoria II pelos que estão no intervalo entre 6 e 8; a Categoria III pelos que estão no intervalo entre 4 e 6; a Categoria IV pelos que estão no intervalo entre 2 e 4; e a Categoria V pelos que estão no intervalo entre 0 e 2.

Definidos os critérios e separados os países em categorias, para satisfazer o objetivo da pesquisa, selecionamos os exemplos a serem seguidos dentre os países da Categoria I e que foram analisados de maneira mais ampla, focando-se, principalmente em quatro informações: (i) existência de um site ou plataforma online próprio para a UIF; (ii) definição clara no site de como é feito o tratamento de dados; (iii) uso de linguagem acessível para o público; e (iv) profundidade de informações. O primeiro critério é básico para cada UIF, mas diferentemente do esperado, muitas delas não dispõem de site próprio[144], o que pode dificultar o acesso às informações pertinentes. O segundo critério se refere à presença de documentos, relatórios ou outras fontes de informação oferecidas no site que apresentem de forma clara como é feito o tratamento de dados, sem a necessidade de apresentar todos os detalhes sobre o processo, sob o risco de cometer o chamado *tipping-off*. O terceiro critério leva em conta a importância de que as informações dispostas pelo site sejam compreendidas pelo público geral, ou seja, pelos titulares dos dados pessoais; a linguagem, pois, tem de ser acessível e não ser exageradamente jurídica e técnica. Por fim, o quarto critério avalia se as informações oferecidas no site são as mais completas possíveis para que não se tornem superficiais.

144 Países que não possuem um site próprio: Arábia Saudita, Áustria, China, Croácia, Dinamarca, Eslováquia, Irlanda, Letónia, Romênia, Polônia, Uruguai.

3. FUNCIONAMENTO DE UNIDADES DE INTELIGÊNCIA FINANCEIRA (UIFs)

3.1. FINALIDADE

As UIFs são órgãos permanentes que atuam na prevenção à lavagem de dinheiro em, atualmente, 147 países. Segundo o Egmont Group, elas devem funcionar como "um centro nacional para recebimento e análise de: (a) comunicação de transações suspeitas e (b) outras informações relevantes para lavagem de dinheiro, crimes associados e financiamento ao terrorismo, e para a disseminação dos resultados da análise"[145]. O Grupo prevê quatro modelos para estruturação das UIFs[146], dentre eles o administrativo: "uma autoridade administrativa, central e independente que recebe e processa informações do setor financeiro e as transmite para órgãos de persecução penal. Funciona como um tampão entre o setor financeiro e os órgãos de persecução penal". Foi esse o modelo escolhido pelo Brasil, no qual o art. 14 da LLD assim define a função do COAF: "finalidade de disciplinar, aplicar penas administrativas, receber, examinar e identificar as ocorrências suspeitas de atividades ilícitas previstas nesta Lei, sem prejuízo das competências de outros órgãos e entidades"[147].

145 Egmont Group. *Financial Intelligence Units (FIUs)*. Disponível em: <https://egmontgroup.org/en/content/financial-intelligence-units--fius>. Acesso em 20 de maio de 2021.

146 Egmont Group. *Financial Intelligence Units (FIUs)*. Disponível em: <https://egmontgroup.org/en/content/financial-intelligence-units--fius>. Acesso em 15 de maio de 2021.

147 BRASIL. Lei nº 9.613, de 03 de março de 1998. *Lei Nº 9.613, de 3 de Março de 1998*. Brasília, DF.

3.2. TRATAMENTO DE DADOS

A UIF deve receber comunicações de operações suspeitas e em espécie, analisar as comunicações e transmitir conclusões e resultados provenientes da análise para os órgãos de persecução penal. Essas atividades se dão em três etapas distintas, nas quais os dados podem ser tratados e utilizados de formas distintas.

Na fase de recepção das comunicações, os dados tratados pela UIF podem ter duas origens: Comunicação de Operação em Espécie (COE) e Comunicação de Operação Suspeita (COS)[148]. A primeira é devida quando uma pessoa obrigada recebe pagamento em espécie, também chamado de dinheiro vivo, acima de um determinado valor definido em norma. Nesse tipo de comunicação, envia-se ao COAF o valor da operação, a identificação do titular da conta, a pessoa que efetuou a operação e dados cadastrais bancários. Para a COE, basta que a transação ultrapasse certo patamar para que a comunicação deva ser enviada para o COAF. Já no caso da COS, as razões para a comunicação da operação são um pouco mais subjetivas e dependem das políticas adotadas pelos setores obrigados para determinar se existe suspeita de lavagem de dinheiro na operação, por meio de procedimentos e mecanismos de controle que avaliarão seu risco[149]. Cabe a cada pessoa obrigada adotar as medidas razoáveis para evitar o envolvimento em operações de lavagem de dinheiro e atender às medidas de prevenção. Nestes casos, os dados que devem ser fornecidos na comunicação envolvem, pelo menos, a pessoa que realizou a operação suspeita e como se deu a operação, ou seja, os valores pagos e demais elementos que levantem a suspeita da pessoa obrigada que a submeteu.

Em relação à fase de análise da comunicação, os dados que são utilizados pelo COAF não são de conhecimento público de forma integral, entretanto, é possível encontrar informação sobre parte da origem dos dados. Como informado no Relatório de Atividades do ano de 2020 do próprio COAF, são utilizados dados do SISCOAF, fontes abertas, Infoseg, dados da Receita Federal não cobertos por sigilo e "bases complementares"[150]. Não há qualquer especificação acerca de quais bases comple-

148 Lei nº 9.613, de 3 de março de 1998: Art. 11. As pessoas referidas no art. 9º: I - dispensarão especial atenção às operações que, nos termos de instruções emanadas das autoridades competentes, possam constituir-se em sérios indícios dos crimes previstos nesta Lei, ou com eles relacionar-se; a) de todas as transações referidas no inciso II do art. 10, acompanhadas da identificação de que trata o inciso I do mencionado artigo; e b) das operações referidas no inciso I; III - deverão comunicar ao órgão regulador ou fiscalizador da sua atividade ou, na sua falta, ao Coaf, na periodicidade, forma e condições por eles estabelecidas, a não ocorrência de propostas, transações ou operações passíveis de serem comunicadas nos termos do inciso II. § 1º As autoridades competentes, nas instruções referidas no inciso I deste artigo, elaborarão relação de operações que, por suas características, no que se refere às partes envolvidas, valores, forma de realização, instrumentos utilizados, ou pela falta de fundamento econômico ou legal, possam configurar a hipótese nele prevista. § 2º As comunicações de boa-fé, feitas na forma prevista neste artigo, não acarretarão responsabilidade civil ou administrativa. § 3o O Coaf disponibilizará as comunicações recebidas com base no inciso II do caput aos respectivos órgãos responsáveis pela regulação ou fiscalização das pessoas a que se refere o art. 9o. Art. 11-A. As transferências internacionais e os saques em espécie deverão ser previamente comunicados à instituição financeira, nos termos, limites, prazos e condições fixados pelo Banco Central do Brasil.

149 Conselho de Controle de Atividades Financeiras. *Recepção de Comunicações*. Disponível em: <https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-producao-de-inteligencia-financeira/inteligencia-financeira>. Acesso em 13 de maio de 2021.

150 Conselho de Controle de Atividades Financeiras. *2020 Relatório de Atividades*. Disponível em: <https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/relatorio-de-atividades-2020-publicado-20210303.pdf>. Acesso em: 13 maio 2021.

mentares seriam essas, nem mesmo quais são as fontes abertas. Além desses dados, são utilizados, evidentemente, os dados coletados por meio das COEs e COSs.

Por fim, na fase de transmissão, os dados utilizados são compilados, de forma analítica, em um único documento: o relatório de inteligência financeira (RIF). Nessa fase, não há agregação de novos dados, mas se trata, evidentemente, de uma forma de tratamento[151].

Em suma, o COAF receberá as comunicações, as submeterá a análises internas, nas quais serão agregados dados da própria base de dados do COAF e de outras bases complementares e, finalmente, será produzido um único documento que será enviado para outros órgãos.

151 Conselho de Controle de Atividades Financeiras. *Disseminação de Relatórios de Inteligência Financeira*. Disponível em: <https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-producao-de-inteligencia-financeira/inteligencia-financeira-em-numeros>. Acesso em 13 de maio de 2021

4. TRANSPARÊNCIA NO SÍTIO ELETRÔNICO (SITE) DO COAF

O site do COAF organiza as informações que pretende comunicar em alguns subtópicos, possivelmente com o intuito de facilitar o acesso ao público. Primeiramente, quanto ao tratamento de dados, as informações apresentadas pelo site se limitam a garantir que o tratamento de dados pessoais é realizado seguindo as exigências legais, estabelecidas pela LGPD, além de apresentar linhas de contato em que qualquer cidadão poderá enviar dúvidas e denúncias[152]. Existe ainda um local do site que se ocupa em listar as normas às quais o COAF está sujeito, citando inclusive as supracitadas Leis nº 9.613/98[153] e 13.974/20[154].

O site oferece informações sobre como é feita a produção de inteligência financeira, ou seja, como é feito o trabalho central do órgão. Essa explicação está ramificada em 3 grandes temas: (i) recepção das comunicações; (ii) análise de informações e (iii) disseminação de relatórios de inteligência financeira[155]. Os 3 temas buscam construir o panorama de como se dá o trabalho e busca garantir que os dados estarão sob sigilo e que um trâmite interno será respeitado. Em relação à "recepção das comunicações", as informações se limitam a definir o que se caracteriza como uma Comunicação de Operação em Espécie (COE) e o que se caracteriza como Comunicação de Operação Suspeita (COS). Sobre as formas de comunicação, Ricardo Liao entende que "as informações existentes numa comunicação de operação suspeita ou numa comunicação de operação em espécie(COS e COE), envolvendo determinada pessoa física ou jurídica, revelam, na visão dos sujeitos obrigados comunicantes, uma percepção de suspeição ou atipicidade a partir dos chamados 'sinais de alerta' indicados nas regulamentações editadas pelos respectivos reguladores/supervisores daquele segmento previsto no art. 9º da Lei nº 9.613, de 1998. Os dados relacionados em uma comunicação (COS ou COE) buscam, por óbvio e necessário, identificar as pessoas envolvidas na situação ou operação."

O presidente do COAF ainda complementa: "Por outro lado, diferentemente do que vem sendo afirmado, o conjunto de informações que integram um RIF, a partir das COE e COS recebidos e analisados pela UIF, não se constitui em "prova" de qualquer crime, sendo tão somente elementos que apontam a existência de indícios de suspeição da ocorrência de ilícitos previstos na regulamentação, a serem apurados e investigados pelas autoridades competentes às quais são disseminados aqueles relatórios de inteligência financeira. Esse é o procedimento observado ante o modelo de UIF administrativa existente no Brasil. Tais comunicações, da mesma forma, recebidas dentro de um sistema seguro de

152 Conselho de Controle de Atividades Financeiras. *Fale Conosco*. Disponível em: <https://www.gov.br/coaf/pt-br/canais_atendimento/copy_of_contatos>. Acesso em: 16 maio 2021.

153 BRASIL. Lei nº 9.613, de 03 de março de 1998. *Lei Nº 9.613, de 3 de Março de 1998*. Brasília, DF.

154 BRASIL. Lei nº 13.974, de 07 de janeiro de 2020. *Lei Nº 13.974, de 7 de Janeiro de 2020*. Brasília, DF.

155 Conselho de Controle de Atividades Financeiras. A Produção de Inteligência Financeira. Disponível em: <https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-producao-de-inteligencia-financeira>. Acesso em 13 de maio de 2021.

informação, são tratadas de maneira sistêmica e reservada pelos analistas de inteligência financeira, e observam o mesmo tratamento de sigilo aplicável aos comunicantes, pois tal dever é transferido para a UIF e deve ser preservado. Seu procedimento de disseminação às autoridades competentes também é conduzido dentro de um sistema seguro de intercâmbio de informações, com todos os alertas de reservas a serem observados por aquelas autoridades pois a elas isso também é imposto pela legislação."

Quanto ao tema da "análise de informações", as informações são mais abrangentes, apesar de serem ainda genéricas. Nesse setor do site é descrito o trâmite interno pelo qual a comunicação é submetida e os métodos que são utilizados para determinar se há indícios de lavagem de dinheiro nas comunicações. Após o Sistema do COAF (SISCOAF) receber as comunicações, elas são submetidas a uma primeira avaliação pelo próprio sistema, utilizando "regras de seleção previamente definidas"; em um segundo momento, é feita a análise pelo modelo preditivo e, em seguida, é distribuída, de forma randômica, a um dos analistas do órgão. Caberá ao analista submeter a comunicação a uma matriz de risco que contemplará não só a COE ou a COS, mas também fatores e elementos relativos às partes envolvidas, as regiões geográficas, existência de investigações em curso etc. Se o resultado atingir pontuação previamente definida pelo COAF, será encaminhado a um segundo analista que será responsável por produzir o RIF. Além disso, as comunicações serão confrontadas com demais informações que estejam disponíveis no SISCOAF[156].

Nesse setor do site ("análise de informações"), no final do texto, existe um link caso o usuário deseje maiores informações sobre o processo de análise das comunicações, que o direcionaria para o Relatório de Atividades do COAF, porém, até esse momento, a página não existe. O acesso a esse Relatório de Atividades, apresentado em local de fácil acesso seria fundamental para maior transparência do órgão. De qualquer forma, após pesquisa com os termos "Relatório de Atividades COAF" é possível encontrar o relatório mais recente, elaborado em 2020[157].

Passando para o tema "Disseminação de Relatórios de Inteligência Financeira", as informações ali contidas são sucintas e breves. Afirma-se que, se houver indícios do cometimento de um crime, o RIF será produzido por um dos analistas e depois encaminhado para as autoridades de persecução penal e que a transmissão não é uma opção. Reforça-se que o envio dos documentos é feito de forma eletrônica, por meio de um sistema de intercâmbio (SEI-C) e que o documento é acompanhado de ferramentas de segurança para garantir o sigilo[158].

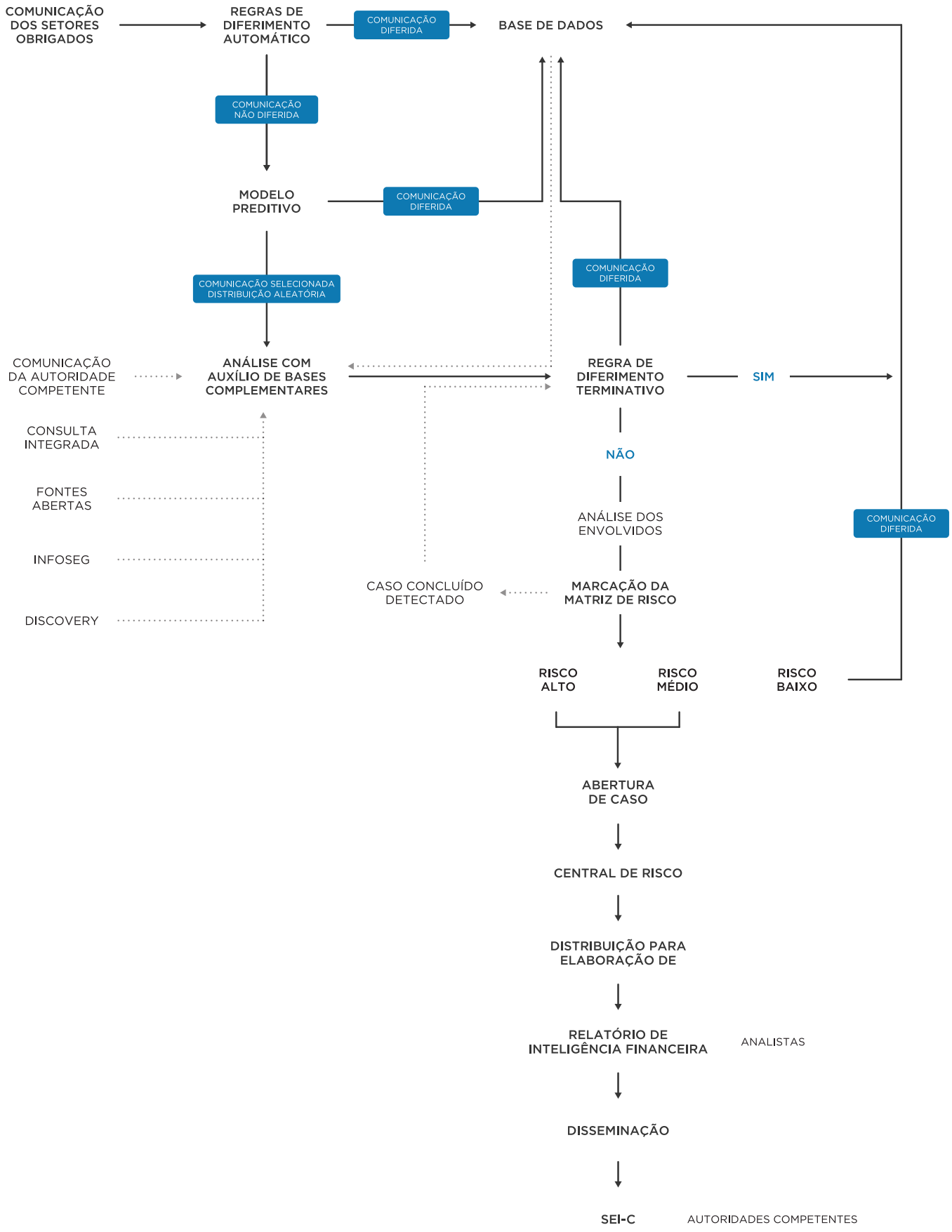
156 Conselho de Controle de Atividades Financeiras. *Análise de Informações*. Disponível em: <https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-producao-de-inteligencia-financeira/analise-de-informacoes>. Acesso em: 13 de maio de 2021.

157 Conselho de Controle de Atividades Financeiras. *2020 Relatório de Atividades*. Disponível em: <https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/relatorio-de-atividades-2020-publicado-20210303.pdf>. Acesso em: 13 maio 2021.

158 Conselho de Controle de Atividades Financeiras. *Disseminação de Relatórios de Inteligência Financeira*. Disponível em: <https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-producao-de-inteligencia-financeira/inteligencia-financeira-em-numeros>. Acesso em 13 de maio de 2021.

De forma geral, são essas as informações encontradas no site do COAF que envolvem o tema do tratamento e proteção de dados. Entretanto, é possível encontrar documentos produzidos pelo próprio órgão que apresentam informações adicionais, o Relatório de Atividades de 2020 e o documento intitulado "O que faz o COAF?"

Sobre o primeiro, o Relatório de Atividades, diversas informações e dados relativos à atuação do COAF são apresentados. No que nos interessa, há um fluxo sobre todo o processo interno que o órgão realiza e a descrição da origem dos dados utilizados para a produção dos RIF:


COMUNICAÇÃO DOS SETORES OBRIGADOS
REGRAS DE DIFERIMENTO AUTOMÁTICO
COMUNICAÇÃO DIFERIDA
BASE DE DADOS
COMUNICAÇÃO NÃO DIFERIDA
MODELO PREDITIVO
COMUNICAÇÃO DIFERIDA
COMUNICAÇÃO SELECIONADA DISTRIBUIÇÃO ALEATÓRIA
COMUNICAÇÃO DIFERIDA
COMUNICAÇÃO DA AUTORIDADE COMPETENTE
ANÁLISE COM AUXÍLIO DE BASES COMPLEMENTARES
REGRA DE DIFERIMENTO TERMINATIVO
SIM
CONSULTA INTEGRADA
FONTES ABERTAS
INFOSEG
DISCOVERY
NÃO
ANÁLISE DOS ENVOLVIDOS
COMUNICAÇÃO DIFERIDA
CASO CONCLUÍDO DETECTADO
MARCAÇÃO DA MATRIZ DE RISCO
RISCO ALTO
RISCO MÉDIO
RISCO BAIXO
ABERTURA DE CASO
CENTRAL DE RISCO
DISTRIBUIÇÃO PARA ELABORAÇÃO DE
RELATÓRIO DE INTELIGÊNCIA FINANCEIRA
ANALISTAS
DISSEMINAÇÃO
SEI-C
AUTORIDADES COMPETENTES

Além disso, existem explicações com maior grau de especificidade do que o site sobre os processos de recebimento, avaliação e transmissão das comunicações, mas ainda genéricos. Portanto, do Relatório de Atividades se extrai, como informação relevante principal, o fluxo sobre o processo interno apresentado acima, sendo que, excluída a imagem inserida, não são encontradas demais informações no Relatório de Atividades que não estejam presentes no próprio site do COAF.

Já sobre o documento "O que o faz o COAF"[159], encontrado na página inicial do site, as informações assim como o Relatório de Atividades apenas complementam os textos do site. A única exceção estaria na página 12, em que é exposto que o COAF não compartilha seu banco de dados com outros entes federativos nem mesmo tem acesso ao banco de dados dos respectivos entes e apenas tem acesso à base de dados da Receita Federal não cobertos por sigilo, o que inclui CPF, CNPJ, nome, razão social, endereço, e-mail, participações societárias, capital social das empresas, entre outros.

Concluindo, o site do COAF contém informações genéricas e está bem estruturado, mas carece de informações aprofundadas quanto ao tratamento e proteção de dados. Os textos e documentos presentes no site se concentram, em sua maioria, em reportar os resultados do trabalho feito, como o número de RIF's produzidos, o número de comunicações produzidas e para quais órgãos foram enviadas. As informações quanto ao tratamento e proteção de dados são restritas e limitadas, sendo, basicamente, descrições sobre o processo interno pelo qual passam as comunicações.

159 Conselho de Controle de Atividades Financeiras. O que faz o COAF? Disponível em: <https://www.gov.br/coaf/pt-br>. Acesso em 13 de maio de 2021.

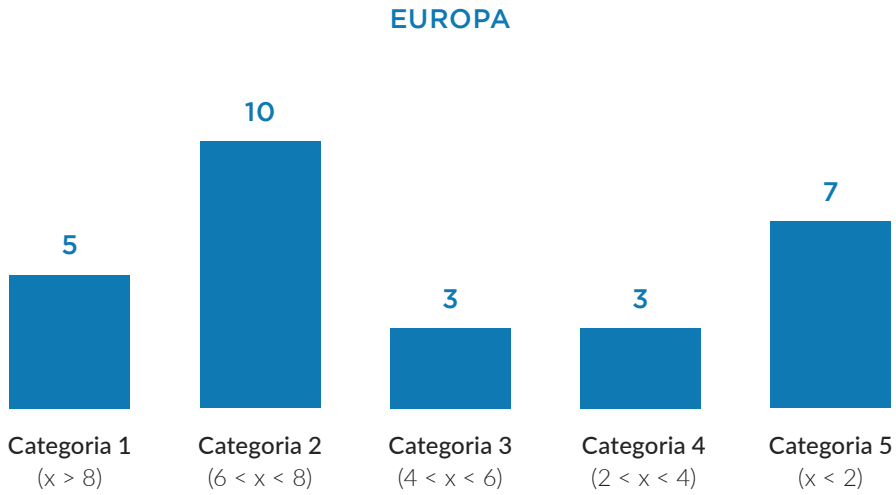
5. ANÁLISE DAS UIFS E EXPOSIÇÃO DOS RESULTADOS

5.1. CLASSIFICAÇÃO DAS UIFS ANALISADAS

Conforme vimos (acima, II, D), os países foram analisados observando quatro critérios: (i) navegabilidade do site da UIF; (ii) disponibilidade de informações sobre tratamento de dados; (iii) disponibilidade de informações sobre a estrutura da UIF; e (iv) disponibilidade de informações sobre quais dados o cidadão pode exigir saber.

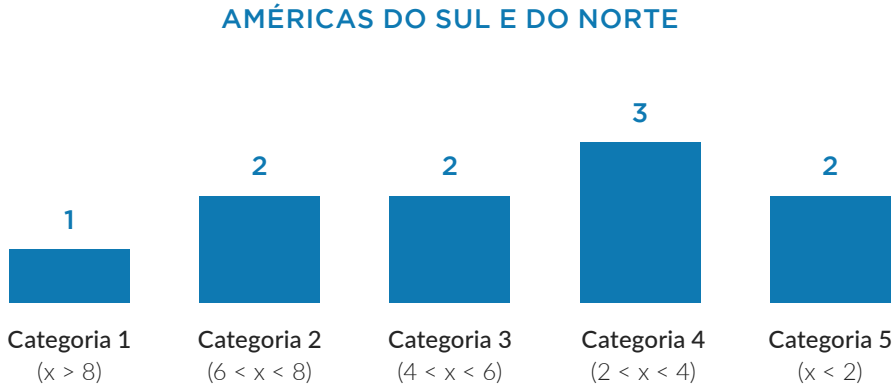
Calculando as notas atribuídas a cada um destes critérios e dividindo os respectivos países na tabela, começa-se a analisar os resultados. A começar pelos países da Europa, pode-se perceber uma média de notas arredondada para duas casas decimais de 4,79. A média é baixa em termos absolutos, porém, comparativamente, esta média é a maior dentre os grupos de países analisados e, consequentemente, é maior que a média global dos países analisados. Afora disso, o desvio padrão calculado foi de 3,14, evidenciando forte desnível entre os países que compõem este grupo.

No que toca à divisão dos países da Europa nas categorias, houve considerável dispersão dos países entre as mesmas. Há maior concentração na categoria 2. O gráfico abaixo demonstra o número de países da Europa por categoria;



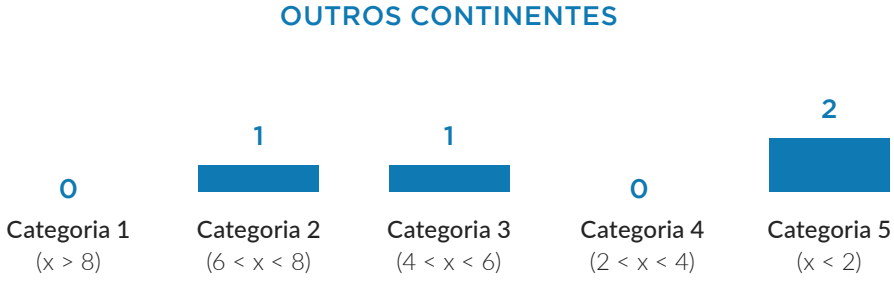
Já no que diz respeito aos resultados dos países analisados das Américas do Sul e do Norte, pode-se perceber uma média de notas arredondada para duas casas decimais de 3,98. Novamente, a média é baixa em termos absolutos, porém também em termos comparativos, estando abaixo das médias mundial e europeia. Há baixa qualidade da transparência das UIFs destes países. Já o desvio padrão calculado foi de 2,64, evidenciando que há menor desnível entre os países do que quando se considera a Europa ou o mundo.

No que toca à divisão dos países das Américas do Sul e do Norte nas categorias, houve também considerável dispersão dos países entre as mesmas. Há maior concentração na categoria 4. O gráfico abaixo demonstra o número de países por categoria.



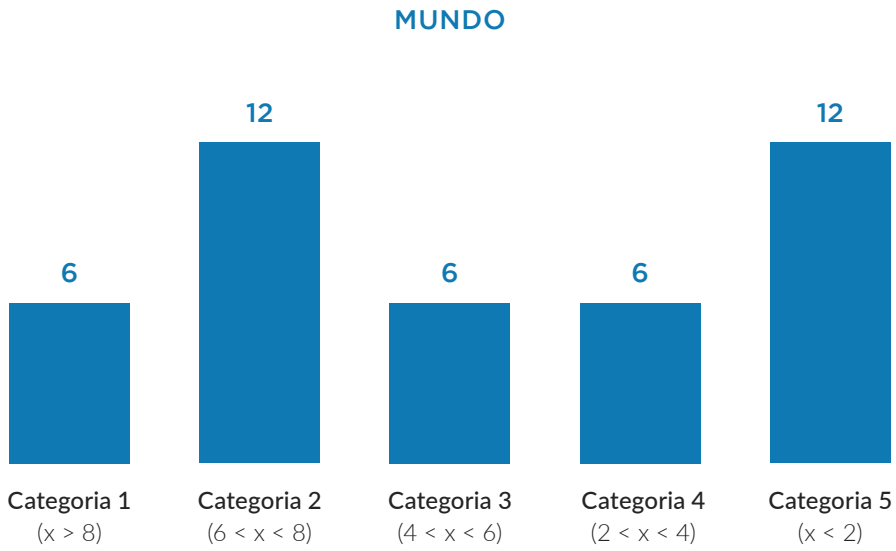
Além destes dois grupos, também foi avaliado um terceiro grupo de países, aqui denominado "Outros Continentes". O objetivo foi englobar países economicamente relevantes e não contemplados nos outros grupos. Para os países de outros continentes, pode-se perceber uma média de notas arredondada para duas casas decimais de 3,00. Esta é a média mais baixa de todos os grupos. Já o desvio padrão calculado foi de 3,47, que por sua vez foi o maior de todos os grupos, mostrando alto desnível.

No que toca à divisão dos países de outros continentes nas categorias, houve menor dispersão dos países e uma grande concentração no nível 5, devido a países que sequer possuem site de suas UIFs. O gráfico abaixo demonstra o número de países por categoria.

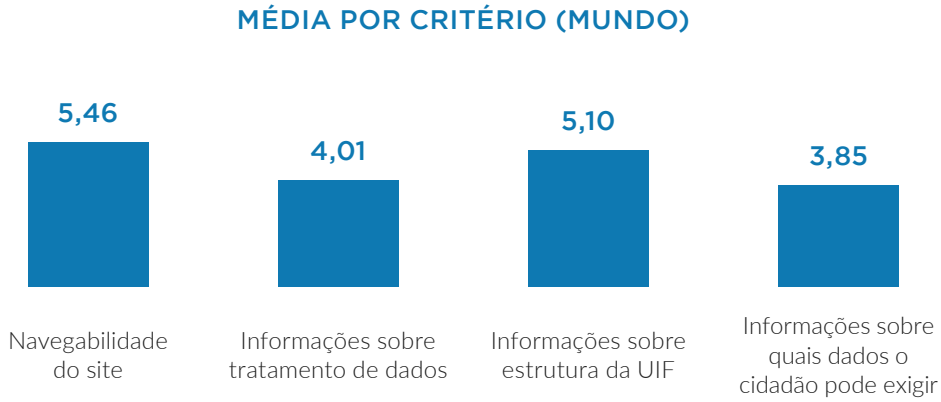


Observando os resultados de todos os países, em um grupo denominado "Mundo", calcula-se a média de 4,26, o que evidencia que, como um todo, os países apresentam baixíssima transparência relativamente às suas UIFs, já que esta média se enquadraria na Categoria III, mas ainda assim é muito baixa. O desvio padrão do Mundo é de 3,09, novamente permitindo constatar alto desnível entre os países.

O gráfico da distribuição de todos os países abaixo em categorias demonstra maior concentração nas categorias II e V, fortalecendo que há alto desnível.



Também interessa observar a média mundial das notas de cada um dos critérios observados, conforme o gráfico abaixo. Com isso, pode-se perceber que a nota é baixa para todos os critérios e os que obtêm as melhores notas são os critérios de navegabilidade do site e informações sobre estrutura da UIF:



Por fim, abaixo, é possível ver como ficou a divisão de todos os países por categoria:

Categoria 1 (x > 8)	Canadá; Espanha; Estónia; Itália; Portugal; República Tcheca
Categoria 2 (6 < x < 8)	Alemanha; Bulgária; Colômbia; Eslovénia; Finlândia; França; Grécia; Japão; Letônia; Lituânia; Luxemburgo; Peru.
Categoria 3 (4 < x < 6)	Brasil; Chile; Hungria; Países Baixos; Rússia; Suécia
Categoria 4 (2 < x < 4)	Argentina; Áustria; Bélgica; Chipre; Estados Unidos; México
Categoria 5 (x < 2)	Arábia Saudita; China; Croácia; Dinamarca; Eslováquia; Irlanda; Malta; Paraguai; Polônia; Romênia; Uruguai

5.2. ANÁLISE DOS PAÍSES DA CATEGORIA 1

Os resultados obtidos a partir das análises dos sites das 41 nações selecionadas, forneceu os resultados mencionados acima e, dentre eles, 6 (seis) foram categorizados como Categoria 1, patamar atribuído aos países que, em seus sites, apresentam nota igual ou superior a 8 (oito), o que representa seu alto grau de transparência. Os países que foram categorizados assim foram Espanha, Estônia, Itália, Portugal, República Tcheca e Canadá. Em contrapartida, ao Brasil, foi atribuída a Categoria 2, que é representada pelos países que obtiveram notas entre 6 (seis) e 8 (oito). Portanto, coube analisar de forma detalhada de que forma e que informações são apresentadas no site dos países de Categoria 1, visto que o objetivo do presente trabalho é fornecer recomendações ao COAF e assim, as recomendações devem partir daqueles países que representam um grau superior ao brasileiro.

A análise detalhada a seguir apresentada seguiu os critérios já especificados[160].

5.2.1. ESPANHA

A UIF espanhola, denominada de SEPBLAC, apresenta site próprio[161] e é facilmente encontrada após pesquisa utilizando os termos "*FIU Spain*". Passando para os critérios técnicos e mais específicos, que diferenciam os países entre as Categorias, o site espanhol se estrutura de forma eficiente e condizente com a própria estrutura do órgão. Segundo Ana Carolina Carlos de Oliveira, a "UIF espanhola tem um sistema bastante respeitado pelas UIF europeias, justamente pela qualidade dos informes respeitando os direitos do investigado".

As principais informações sobre o tratamento e a proteção de dados estão dispostas no setor "*About SEPBLAC*"[162], no subitem, "*transparency*"[163], o que é um indicativo e uma ferramenta para direcionar os usuários e facilitar o acesso às informações que procuram. Em "*transparency*", o principal documento sobre o tratamento e proteção de dados é a Lei 10/2010[164], que regulamenta a prevenção e o combate a lavagem de dinheiro e financiamento ao terrorismo.

160 (i) Existência de um site ou plataforma online próprio para a UIF; (ii) descrição clara no site de como é feito o tratamento de dados; (iii) uso de linguagem acessível para o público; e (iv) profundidade de informações; e (v) canal de comunicação.

161 Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. *Financial Intelligence Unit*. Disponível em: <https://www.sepblac.es/en/abt-sepblac/financial-intelligence-unit/>. Acesso em 20 de maio de 2021.

162 Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. *About SEPBLAC*. Disponível em: <https://www.sepblac.es/en/abt-sepblac/>. Acesso em 20 de maio de 2021.

163 Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. *Transparency*. Disponível em: <https://www.sepblac.es/en/abt-sepblac/transparency/>. Acesso em 20 de maio de 2021.

164 ESPANHA. Lei nº 10, de 28 de abril de 2010. *Lei nº 10, de 28 de abril de 2010*. Madrid.

Esse documento apresenta diversas informações relativas a esta matéria, desde como os entes privados devem tratar esses dados até medidas de controle interno que a UIF deve realizar. Em relação às medidas que os entes privados devem adotar, estão dispostas a forma que os dados devem ser armazenados, como deverão ser reportados e como deverão ser protegidos. Já sobre as medidas que a UIF deve adotar internamente, as disposições têm caráter semelhante e apresentam, de forma geral, como deverão ser recebidas, utilizadas, tratadas, protegidas e transmitidas. Porém, sobre as medidas específicas da UIF, é interessante notar que há menção às demais leis que também abordam o tema.

Um fator em que a Espanha se destaca por meio de sua UIF e que pode ser facilmente acessado em seu site é o acesso do público a seus dados. No mesmo setor de "*transparency*", é destacada a Lei 19/2013[165] que apresenta de forma extensa como o público pode requerer e acessar seus dados nos diversos órgãos do governo espanhol. Essa lei é apresentada em PDF no site e dispõe sobre o procedimento, os direitos, a forma, os prazos de como a informação poderá ser requerida, acessada e utilizada. Sobre o caso específico da SEPBLANC, na Lei 10/2010, há disposição adicional no fim do documento que reporta a qual órgão do governo a solicitação deve ser feita e que critérios deve atender para que se possa requerer dados utilizados pela UIF.

Ainda sobre os canais de comunicação, o site da SEPBLANC, contém um link destacado para o chamado "Portal de Transparência"[166] do Governo, em que as solicitações de informações mencionadas nos dispositivos citados acima poderão ser feitas.

A linguagem contida nos documentos, por se tratar de legislação, não é voltada para o público, porém, este conseguirá compreender de forma fácil o que está sendo dito, não sendo um empecilho ou barreira para o acesso à informação que o site apresenta sobre o tratamento e proteção de dados.

Por fim, importante registrar que o Governo espanhol, em 27 maio de 2021, aprovou uma nova Lei de Proteção de Dados em matéria penal, Lei orgânica nº 7/2021[167], transpondo a Diretiva UE 680/2016. Entretanto, como previsto pela 12ª disposição final, a Lei só entrará em vigor vinte dias após sua publicação no Diário Oficial do Estado, portanto, após a conclusão deste trabalho. Por esta razão, ainda não é possível notar alterações ou menções ao novo diploma legal no site, que certamente será modificado para se ajustar aos novos dispositivos.

165 ESPANHA. Lei nº 19, de 9 de dezembro de 2013. *Lei nº 19, de 9 de dezembro de 2013*. Madrid.

166 Administración General del Estado. *Portal de la Transparencia*. Disponível em: <https://transparencia.gob.es>. Acesso em: 20 de maio de 2021.

167 ESPANHA. Lei orgânica nº 7, de 27 de maio de 2021. *Lei orgânica nº 7, de 27 de maio de 2021*. Madrid.

5.2.2. ESTÔNIA

A UIF estoniana apresenta site[168] que justifica sua inclusão na Categoria I dos países analisados. Como primeiro ponto de análise, a UIF apresenta site próprio e de grande facilidade de acesso e navegabilidade, o que auxilia o usuário a identificar as informações que busca. Além disso, o site também está disponível na língua inglesa, o que pode ser considerado um ponto positivo, para que a língua não seja uma barreira ao acesso e consulta às informações ali dispostas.

Sobre as informações relativas ao tratamento e proteção de dados apresentadas, destacamos quatro documentos, tendo cada um deles referência a aspectos diversos do processo que a UIF realiza. É importante ressaltar, primeiramente, de que forma as informações estão dispostas, já que o Governo Estoniano decidiu compilar todo o conteúdo sobre cada um dos temas em diferentes documentos que podem ser acessados com um simples clique, de forma intuitiva. Todo o conteúdo citado está disposto em documentos e não no site em si, que funciona como o meio para se acessar e ter contato com estes arquivos, disponíveis em inglês e estoniano.

Na seção "*guidelines*"[169], uma das 5 seções principais em que o site é dividido, estão 2 (dois) dos 4 (quatro) documentos de absoluta relevância para a temática da proteção e tratamento de dados pessoais. Esses "*guidelines*" ou diretrizes, em português, apresentam disposições sobre: (i) como as pessoas obrigadas devem submeter as comunicações para a UIF e (ii) como podem identificar transações suspeitas. Os documentos, além de serem de extrema relevância para o público que, muitas vezes, não tem conhecimento prévio ou ciência de como identificar e reportar algum tipo de transação suspeita, também apresenta conceitos técnicos, características de uma transação suspeita, indicadores e meios de prevenção por meio do uso de linguagem acessível. Ainda se descreve de que forma a transação deve ser comunicada, ou seja, como a comunicação deve ser estruturada e que tipo de dados devem constar, um verdadeiro passo-a-passo para as pessoas obrigadas.

O terceiro documento, encontrado na seção "*Useful information*"[170], informações úteis, em português, é uma norma do Ministério do Interior da Estônia[171], em 2008, sobre o procedimento para o registro e processamento de dados recebidos. O documento está dividido em capítulos, sendo que em cada um são apresentadas regras e procedimentos internos que os funcionários e responsáveis pela UIF deverão cumprir durante os processos internos que são realizados. Os procedimentos incluem

168 Republic of Estonia. *Financial Intelligence* Unit. Disponível em: <https://www.fiu.ee/en>. Acesso em 20 de maio de 2021.

169 Republic of Estonia. *Guidelines*. Disponível em: <https://www.fiu.ee/en/guidelines-fiu/guidelines>. Acesso em 20 de maio de 2021

170 Republic of Estonia. *Useful Information*. Disponível em: <https://www.fiu.ee/en/useful-information-and-contacts/useful-information>. Acesso em 20 de maio de 2021.

171 Republic of Estonia. *Procedure for the registration and processing of data collected by the Financial Intelligence Unit*. Disponível em: <https://www.politsei.ee/files/Rahapesu/regulation-no-13-23.pdf?cbd2b18944>. Acesso em 20 de maio de 2021.

etapas como a coleta, registro, análise, transmissão e proteção das comunicações recebidas, com especificações de que medidas e ações devem ser tomadas em cada um dos processos. A linguagem utilizada é levemente mais formal e técnica do que a encontrada nas diretrizes citadas anteriormente, entretanto, o conteúdo dessa norma do Ministério do Interior é de fácil entendimento para o público, que não deve encontrar grandes dificuldades em entender o processo interno pelo qual os dados recebidos são submetidos. Este documento, portanto, reúne normas que a UIF deve seguir quando receber uma comunicação e está aberto ao público para que esse possa ter mais transparência e ciência dos procedimentos internos da UIF e segurança sobre a proteção e o tratamento de dados que é feito pelo órgão.

Por último, temos o "*Money Laundering and Terrorist Financing Prevention Act*"[172] ou Ato de Prevenção a Lavagem de Dinheiro e Financiamento ao Terrorismo, que nada mais é que uma lei estoniana, aprovada em 2017, e que regula a atuação da UIF e das pessoas obrigadas contra os crimes de lavagem de dinheiro e financiamento ao terrorismo. Essa lei pode ser encontrada também na seção "*Useful information*". Dentre diversos artigos, o documento se divide entre pessoas obrigadas e a própria UIF. Sobre o primeiro grupo, existem disposições sobre como deve ser feito o tratamento e proteção de dados, assim fornecendo aos entes privados diretrizes de como deve se regular sua atuação, como uma espécie de LGPD específica para as pessoas obrigadas. Já em relação à própria UIF, as informações presentes estão no capítulo 6 e estabelecem limites e poderes que o órgão goza durante sua atuação, entre elas, o poder de utilizar bases de dados de outros órgãos do Estado, como um banco de dados municipal, desde que cumprido o processo legal.

Em resumo, as informações encontradas no site da UIF são profundas e de extrema importância para o público que deseja acessar sua plataforma digital e entender que tipos de dados a UIF tem acesso, bem como de que forma ele será tratado e protegido. Além disso, ele poderá compreender de que forma ele, como pessoa obrigada, deve tratar e proteger os dados que recebe e como poderá identificar uma transação suspeita e comunicá-la ao órgão. A linguagem também é acessível, justamente pelos documentos serem voltados ao público e serem redigidos para que qualquer um, mesmo sem conhecimento técnico ou jurídico, possa acessar o site e esclarecer suas dúvidas. Por fim, as informações são profundas pois extrapolam a generalidade e apresentam detalhes que são fundamentais, porém, sem incorrer no risco de revelar dicas, no chamado tipping-off. Por essas razões foi conferido ao site da UIF estoniana a classificação com nota superior ou igual à 8, o que representa sua qualidade e transparência.

172 ESTÔNIA. *Money Laundering and Terrorist Financing Prevention Act*, *de 27 de novembro de 2017*. Tallinn.

5.2.3. ITÁLIA

A Itália, durante as análises, demonstrou ter sua UIF devidamente classificada na Categoria I. Seu site[173] é facilmente encontrado, bastando apenas pesquisar "*FIU Italy*" e este se demonstrou bastante acessível.

O site é dividido em algumas categorias principais – *About Us*, *Italian Anti-Money Laundering System*, *Legislation*, *Obligations of Operations e Publications* – o que facilita sua navegabilidade. Além disso, possui a versão em italiano e em inglês, permitindo uma maior compreensão do que é tratado, entretanto, faz uso de uma linguagem não acessível ao público.

Na seção *About Us*[174], o site explica de maneira geral quando que a UIF Italiana foi criada, demonstrando que segue a legislação internacional sobre a questão e trabalha de maneira autônoma para combater lavagem de dinheiro e financiamento de terrorismo. Para isso, deixa claro que funciona a partir de dados coletados de transações suspeitas reportadas. Por conseguinte, analisa as informações procurando evidências dos crimes cometidos.

Sobre a aba *Italian Anti-Money Laundering System*[175], é apresentada a legislação internacional[176] que regula a UIF e suas ações de maneira mais específica. Nessa seção, há uma explicação mais aprofundadas das organizações envolvidas na operação, quais são: o FATF (*Financial Action Task Force*), a *Egmont Group*, e a *Moneyval*, incluindo, também, as *European Union Bodies: Expert Group on Money Laundering and terrorist financing*, *EU FIUs' Platform* e *FIU.NET*. Ademais, apresenta a legislação nacional[177] quanto a esse tema, incluindo medidas para aumentar a transparência, explicação de quais são as partes nacionais envolvidas no processo e como é feito o monitoramento dos dados e seu tratamento. De modo geral, explica onde encontrar informações mais detalhadas sobre questões tipificadas em legislação, ao mesmo tempo em que as explica de maneira coerente e eficiente. Em seguida, apresenta *The Role of the Financial Intelligence Unit*[178] explicando de maneira mais organizada como ela funciona,

173 UIF – Unità di Informazione Finanziaria. *Unità di Informazione Finanziaria per l'Italia*. Disponível em: <https://uif.bancaditalia.it/homepage/index.html?com.dotmarketing.htmlpage.language=1>. Acesso em: 20 maio 2021.

174 UIF – Unità di Informazione Finanziaria. *About Us*. Disponível em: <https://uif.bancaditalia.it/homepage/index.html?com.dotmarketing.htmlpage.language=1>. Acesso em: 20 maio 2021.

175 UIF – Unità di Informazione Finanziaria. *Italian Anti-Money Laundering System*. Disponível em: <https://uif.bancaditalia.it/homepage/index.html?com.dotmarketing.htmlpage.language=1>. Acesso em: 20 maio 2021

176 UIF – Unità di Informazione Finanziaria. *The International Legislative Framework*. Disponível em: <https://uif.bancaditalia.it/sistema-antiriciclaggio/organizzazione-internazionale/index.html>. Acesso em: 20 maio 2021.

177 UIF – Unità di Informazione Finanziaria. *The National Legislative Framework*. Disponível em: <https://uif.bancaditalia.it/sistema-antiriciclaggio/ordinamento-italiano/index.html>. Acesso em: 20 maio 2021.

178 UIF – Unità di Informazione Finanziaria. *The Role of the Financial Intelligence Unit (FIU)*. Disponível em: <https://uif.bancaditalia.it/sistema-antiriciclaggio/uif-italia/index.html>. Acesso em: 20 maio 2021.

qual a legislação envolvida e quais são seus objetivos. Por fim, na aba *Italian Anti-Money Laundering System*, tem a parte *Organization*[179], em que se apresenta quem são os diretores da UIF.

Na seção *Legislation*[180] há uma área específica para *Anti-Money Laundering*[181], em que é apresentado de maneira mais específica como são as *International Standards and Legislation*, tanto no que tange às recomendações das FATFs e da União Europeia. Em seguida, explica brevemente a *National Legislation*. Na mesma seção, o subtópico *Red Flag Indicators and Anomaly Schemes*[182] explica como se dá a detecção de transações suspeitas, passando por *Anomaly Indicators e Models and Patterns of Anomalous Behaviour*.

Na parte *Obligations of Operators*[183], a UIF a divide em dois subtópicos. No primeiro – *The Reporting of Suspicious Transactions*[184] –, explica as *General Provisions*, isto é, quais são as regulações envolvidas em todo cenário de relato de atividades suspeitas. Em seguida, na seção Instructions, explica como é o passo a passo para fazer os relatórios, indicando o que deve constar neles, inclusive e, no segundo subtópico, aborda as questões relativas às *Threshold-Based Communications*[185].

179 UIF – Unità di Informazione Finanziaria. *Organization*. Disponível em: <https://uif.bancaditalia.it/sistema-antiriciclaggio/organigramma-uif/index.html>. Acesso em: 20 maio 2021.

180 UIF – Unità di Informazione Finanziaria. *Legislation*. Disponível em: <https://uif.bancaditalia.it/homepage/index.html?com.dotmarketing.htmlpage.language=1>. Acesso em: 20 maio 2021.

181 UIF – Unità di Informazione Finanziaria. *Anti-Money Laundering*. Disponível em: <https://uif.bancaditalia.it/normativa/norm-antiricic/index.html>. Acesso em: 20 maio 2021.

182 UIF – Unità di Informazione Finanziaria. *Red Flag Indicators and Anomaly Schemes*. Disponível em: <https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/index.html>. Acesso em: 20 maio 2021.

183 UIF – Unità di Informazione Finanziaria. *Obligations of Operators*. Disponível em: <https://uif.bancaditalia.it/homepage/index.html?com.dotmarketing.htmlpage.language=1>. Acesso em: 20 maio 2021.

184 UIF – Unità di Informazione Finanziaria. *The Reporting of Suspicious Transactions*. Disponível em: <https://uif.bancaditalia.it/adempimenti-operatori/segnalazioni-sos/index.html>. Acesso em: 20 maio 2021.

185 UIF – Unità di Informazione Finanziaria. *Threshold-Based Communications*. Disponível em: <https://uif.bancaditalia.it/adempimenti-operatori/comunicazioni-oggettive/index.html.> Acesso em: 20 maio 2021.

Por fim, a última seção *Publications*[186] tem sete subtópicos: são: *Annual Report*[187]; *UIF Working Papers*[188]; *NewsLetter*[189]; *Speeches – The Director of the UIF*[190]; *Speeches– The Bank of Italy on the Subject of Anti-Money Laundering*[191]; *Press Release*[192]; e, *News*[193]. Com isso, resta claro que há um interesse por parte da UIF italiana em deixar o mais público possível informações que consideram relevantes, buscando uma maior transparência.

Voltando aos critérios de avaliação, percebe-se que ele atende à maioria deles. A UIF italiana possui um site próprio que apresenta descrição clara de como é feito o tratamento de dados. Suas diferentes seções e subseções ajudam e facilitam a navegação por parte da população, tornando-o bastante acessível. Entretanto, a linguagem é relativamente complexa, mas compreensível. Quanto à profundidade de informações, é extremamente satisfatória. Por fim, há um canal de comunicação, na aba *Contact Us*, e, para fazer alguma denúncia, basta seguir as instruções contidas no site que são facilmente acessadas.

186 UIF – Unità di Informazione Finanziaria. *Publications*. Disponível em: <https://uif.bancaditalia.it/homepage/index.html?com.dotmarketing.htmlpage.language=1>. Acesso em: 20 maio 2021.

187 UIF – Unità di Informazione Finanziaria. *Annual Report*. Disponível em: <https://uif.bancaditalia.it/pubblicazioni/rapporto-annuale/index.html>. Acesso em: 20 maio 2021.

188 UIF – Unità di Informazione Finanziaria. *UIF Working Papers*. Disponível em: <https://uif.bancaditalia.it/pubblicazioni/quaderni/index.html>. Acesso em: 20 maio 2021.

189 UIF – Unità di Informazione Finanziaria. *Newsletter*. Disponível em: <https://uif.bancaditalia.it/pubblicazioni/newsletter/index.html>. Acesso em: 20 maio 2021.

190 UIF – Unità di Informazione Finanziaria. *Speeches – The Director of the UIF*. Disponível em: <https://uif.bancaditalia.it/pubblicazioni/interventi/index.html>. Acesso em: 20 maio 2021.

191 UIF – Unità di Informazione Finanziaria. *Speeches – The Bank of Italy on the Subject of Anti-Money Laundering*. Disponível em: <https://uif.bancaditalia.it/pubblicazioni/intergov/index.html>. Acesso em: 20 maio 2021.

192 UIF – Unità di Informazione Finanziaria. *Press Release*. Disponível em: <https://uif.bancaditalia.it/pubblicazioni/comunicati/index.html>. Acesso em: 20 maio 2021.

193 UIF – Unità di Informazione Finanziaria. *Newsletter*. Disponível em: <https://uif.bancaditalia.it/pubblicazioni/avvisi/index.html>. Acesso em: 20 maio 2021.

5.2.4. PORTUGAL

Analisando o site da UIF de Portugal[194], chega-se à conclusão de que ela possui as características necessárias para se encontrar na Categoria I e é de extrema relevância para o estabelecimento do benchmark.

O site está dividido em sete seções: *Início*, *Prevenção/Combate BCFT*, *Portal de Comunicações*, *Legislação*, *Autoridades Setoriais*, *Publicações e Lista Sanções*. Na seção *Início*[195], há uma explicação de quem é a UIF[196]. Nessa subseção, apresenta a legislação que rege seu funcionamento, assim como explica como funciona. Isso se dá de maneira bastante didática e acessível. Em seguida, demonstra qual é a missão[197] da UIF, deixando claro, novamente, como a legislação aborda esse ponto. Ademais, explica de maneira bem sucinta o que é a ameaça de lavagem de dinheiro[198], deixando claro onde que o branqueamento de capitais está tipificado.

A segunda seção, *Prevenção/Combate BCTG*[199], apresenta quarenta recomendações do GAFI[200], assim como um documento extenso com orientações do Grupo de Ação Financeira, que contém desde seu objetivo até as metodologias de avaliação de riscos específicos. Em seguida, relata quais são as entidades obrigadas[201], isto é, quais entidades estão envolvidas em todo o processo de prevenção/combate BCTG. Sendo assim, demonstra quais são as com sede em Portugal, no exterior, outras entidades financeiras e não financeiras, deixando clara a regulamentação que rege o ponto e, em alguns casos, o que esses órgãos fazem. Em seguida, o site oferece um documento com quais são os países de risco[202], assim quais têm uma jurisdição que está em constante monitoramento e os que têm uma jurisdição de alto risco. Vale ressaltar que eles justificam a alocação de cada um desses países. Poste-

194 UIF – Unidade de Informação Financeira. *UIF – Unidade de Informação Financeira*: prevenção e combate ao branqueamento de capitais e financiamento do terrorismo. Prevenção e Combate ao Branqueamento de Capitais e Financiamento do Terrorismo. Disponível em: <https://uif.policiajudiciaria.pt>. Acesso em: 20 maio 2021.

195 UIF – Unidade de Informação Financeira. *Início*. Disponível em: <https://uif.policiajudiciaria.pt>. Acesso em: 20 maio 2021.

196 UIF – Unidade de Informação Financeira. *Quem Somos*. Disponível em: <https://uif.policiajudiciaria.pt/sumula-historica/>. Acesso em: 20 maio 2021.

197 UIF – Unidade de Informação Financeira. *Missão*. Disponível em: <https://uif.policiajudiciaria.pt/missao/>. Acesso em: 20 maio 2021.

198 UIF – Unidade de Informação Financeira. *A Ameaça de Lavagem de Dinheiro*. Disponível em: <https://uif.policiajudiciaria.pt/ola-mundo/>. Acesso em: 20 maio 2021.

199 UIF – Unidade de Informação Financeira. *Prevenção e Combate ao BCFT*. Disponível em: <https://uif.policiajudiciaria.pt/category/bcft/>. Acesso em: 20 maio 2021.

200 UIF – Unidade de Informação Financeira. *40 Recomendações do GAFI*. Disponível em: <https://uif.policiajudiciaria.pt/40-recomendacoes-do-gafi/>. Acesso em: 20 maio 2021.

201 UIF – Unidade de Informação Financeira. *Entidades Obrigadas*. Disponível em: <https://uif.policiajudiciaria.pt/entidades-obrigadas-2/>. Acesso em: 20 maio 2021.

202 UIF – Unidade de Informação Financeira. *Países de Risco*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016R1675-20181022&qid=1496859925610&from=EN>. Acesso em: 20 maio 2021.

riormente, explica sobre a declaração de beneficiário efetivo[203] e sobre a *goAML*[204], que é a aplicação informática para recepção, processamento e análise de relatórios de instituições financeiras. Por fim, a seção aborda o Centro Nacional de Cibersegurança[205], por meio de um link para o site da organização.

A terceira seção, *Portal de Comunicações*[206], está temporariamente indisponível, entretanto, busca facilitar o contato com a UIF. Este contato pode ser para a comunicação de operações suspeitas, por exemplo, e apresenta instruções de como realizar isso[207]. Ademais, apresenta a Portaria 310/2018, de 04 de dezembro, que é o formulário de comunicação[208]. Além disso, apresenta os manuais da *goAML*[209], o manual de Registro de Utilizados e o de Registro de Entidade ou Organização. Dessa forma, deixando claro e acessível como é o passo a passo para se comunicar com a UIF.

No tópico *Legislação*[210], apresenta de maneira bem simplista a Lei nº 58/2020, de 31 de agosto[211]. Tal lei transpõe a Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, que altera a Diretiva (UE) 2015/849 e a Diretiva (UE) 2018/1673 do Parlamento Europeu e do Conselho. Em seguida, explicita qual a legislação que regula os diplomas legais ou regulamentares[212]. Vale destacar que também apresentam as normas da União Europeia[213] e a jurisprudência relevante[214]. Por fim, apresenta o link para o site do Gabinete de Recuperação de Ativos, que apresenta vastas legislações importantes.

203 UIF – Unidade de Informação Financeira. *Declaração do Beneficiário Efetivo*. Disponível em: <https://uif.policiajudiciaria.pt/declaracao-do-beneficiario-efetivo/>. Acesso em: 20 maio 2021.

204 UIF – Unidade de Informação Financeira. *GoAML*. Disponível em: <https://uif.policiajudiciaria.pt/goaml/>. Acesso em: 20 maio 2021.

205 Centro Nacional de Cibersegurança Portugal. *Centro Nacional de Cibersegurança*. Disponível em: <https://www.cncs.gov.pt>. Acesso em: 20 maio 2021.

206 UIF – Unidade de Informação Financeira. *Portal de Comunicações*. Disponível em: <https://uif.policiajudiciaria.pt/portal-de-comunicacoes/>. Acesso em: 20 maio 2021.

207 UIF – Unidade de Informação Financeira. *Registro no Portal*. Disponível em: <https://uif.policiajudiciaria.pt/registo-no-goaml/>. Acesso em: 20 maio 2021.

208 UIF – Unidade de Informação Financeira. *Portaria 310/2018 de 4/12*. Disponível em: <https://uif.policiajudiciaria.pt/portal-de-comunicacoes/>. Acesso em: 20 maio 2021.

209 UIF – Unidade de Informação Financeira. *Manuais goAML*. Disponível em: <https://uif.policiajudiciaria.pt/manuais-goaml/>. Acesso em: 20 maio 2021.

210 UIF – Unidade de Informação Financeira. *Legislação*. Disponível em: <https://uif.policiajudiciaria.pt/category/legislacao/>. Acesso em: 20 maio 2021.

211 UIF – Unidade de Informação Financeira. *Lei n.º 50/2020, de 31 de Agosto*. Disponível em: <https://uif.policiajudiciaria.pt/lei-n-o-58-2020-de-31-de-agosto/>. Acesso em: 20 maio 2021.

212 UIF – Unidade de Informação Financeira. *Diplomas Legais ou Regulamentares*. Disponível em: <https://uif.policiajudiciaria.pt/diplomas-legais-ou-regulamentares/>. Acesso em: 20 maio 2021.

213 UIF – Unidade de Informação Financeira. *Normas da União Europeia*. Disponível em: <https://uif.policiajudiciaria.pt/normas-das-uniao-europeia/>. Acesso em: 20 maio 2021.

214 UIF – Unidade de Informação Financeira. *Jurisprudência*. Disponível em: <https://uif.policiajudiciaria.pt/jurisprudencia/>. Acesso em: 20 maio 2021.

Em quarto lugar, há a seção *Autoridades Setoriais*[215]. Nela, apresenta-se quais são as autoridades setoriais, direcionando aos respectivos sites que apresentam um pouco sobre a autoridade em questão e os documentos relevantes.

Na seção *Publicações*[216], há relatórios anuais e avaliações, assim como dissertações. Todos são de fácil acesso e há a opção de se ler em inglês. Isso demonstra um comprometimento da UIF com a transparência do que ocorre dentro dela, assim como momentos de autoavaliação.

Por fim, tem-se a seção *Lista Sanções*[217], que identifica quem está envolvido em todo esse processo de maneira específica e profunda.

Dessa forma, resta claro que o site da UIF de Portugal deve ser levado em consideração para a criação de um *benchmark*. Ele apresenta todas as informações relevantes, demonstrando-se bastante transparente no tratamento de dados. Vale ressaltar, entretanto, que não possui tradução em inglês, o que pode dificultar sua navegação por pessoas que não falam português. Ademais, apresentam de maneira bastante clara um canal de comunicação, com um passo a passo a ser seguido, que envolve não somente a UIF, como também como contatar organizações envolvidas nas atividades.

215 UIF – Unidade de Informação Financeira. *Autoridades Setoriais*. Disponível em: <https://uif.policiajudiciaria.pt/category/aplicacao/>. Acesso em: 20 maio 2021.

216 UIF – Unidade de Informação Financeira. *Publicações*. Disponível em: <https://uif.policiajudiciaria.pt/category/pe/>. Acesso em: 20 maio 2021.

217 UIF – Unidade de Informação Financeira. *Lista de Sanções*. Disponível em: <https://uif.policiajudiciaria.pt/category/si/>. Acesso em: 20 maio 2021.

5.2.5. REPÚBLICA TCHECA

A UIF da República Tcheca é uma das classificadas como categoria um, sendo um bom exemplo de excelência e transparência nos quesitos levados em consideração para a classificação. O site da UIF[218] é próprio, não sendo uma subseção do site de outros órgãos como visto em alguns países de categorias inferiores. Ademais, é de fácil acesso, possuindo um botão de tradução do tcheco para o inglês, o que diminui a barreira linguística e favorece o acesso por pessoas não nativas do país, da mesma forma em que apresenta quais são os países com jurisdição que estão em constante monitoramento, juntamente com países com jurisdição com grave risco. Nesses tópicos, justificam com fatos porque essas jurisdições estão assim alocadas.

A navegação no site é simples, com categorias bem definidas e um design que facilita o acesso às informações. As categorias principais apresentadas pelo site são: Introdução, Relatórios anuais, Avaliação de risco nacional e Contatos.

Na aba de introdução[219], existem subcategorias autoexplicativas e intuitivas de acessar. A "atividades da FAU" traz informações iniciais sobre a FAU, sobre transferência de dinheiro através de fronteiras e uma sessão sobre "comunicação eletrônica", que traz informações sobre um aplicativo desenvolvido pela própria UIF, o *MoneyWEB*. Ainda na introdução, são apresentadas algumas perguntas, com as respostas para estas sendo acessadas com um clique. As mais relevantes perguntas apresentadas são: quando foi fundada a FAU, como se comunicar com a FAU, qual o orçamento da FAU e quem é o diretor da FAU.

A segunda aba é a de relatórios anuais[220]. São disponibilizados relatórios dos anos de 2020 e 2019, com informações sobre o Gabinete de Análise Financeira e o Escritório de Análise Financeira da República Tcheca. No entanto, os relatórios estão escritos apenas em Tcheco, criando assim uma barreira linguística para a análise do seu conteúdo.

A terceira aba é denominada Avaliação de Risco Nacional[221]. Esse processo, seguindo a descrição do próprio site, tem como objetivo relatar os riscos de lavagem de dinheiro e financiamento de grupos terroristas. É conduzido pela Autoridade Analítica Financeira em conjunto com outros órgãos

218 Finanční Analyticky Urad. *Finanční Analyticky Urad*. Disponível em: <https://www.financnianalytickyurad.cz/>. Acesso em: 25 maio 2021.

219 Finanční Analyticky Urad. *Introduction*. Disponível em: <https://www.financnianalytickyurad.cz/>. Acesso em: 25 maio 2021.

220 Finanční Analyticky Urad. *Annual Reports*. Disponível em: <https://www.financnianalytickyurad.cz/vyrocni-zpravy.html>. Acesso em: 25 maio 2021.

221 Finanční Analyticky Urad. *National Risk Assessment*. Disponível em: <https://www.financnianalytickyurad.cz/narodni-hodnoceni-rizik.html>. Acesso em: 25 maio 2021.

do governo, como o Banco Nacional e departamentos da polícia tcheca. Estão disponibilizados no site os relatórios produzidos na avaliação. Divididos nas categorias: versão pública, versão não pública para pessoas obrigadas, informações sobre a segunda rodada da avaliação de risco nacional, informações para organizações não governamentais sem fins lucrativos. Novamente, o conteúdo dos relatórios está disponibilizado apenas em tcheco, dificultando o acesso de não nativos.

A quarta aba é de contatos com a FAU[222]. Informações que são raras nas maiorias dos sites de UIFs e que são fundamentais para uma transparência completa. A UIF da República Tcheca é referência neste quesito, trazendo dois números de telefone de contato com a secretária do escritório, um número de FAX, o endereço de e-mail do escritório, informações do funcionamento da sala de arquivos e o endereço eletrônico do cartório.

Por fim, fica claro que a UIF da República Tcheca se enquadra em todos os parâmetros e está bem colocada na categoria 1. Com alguns pontos de excelência que podem ser usados como exemplos para UIFs de outros países, incluindo o COAF no caso brasileiro.

222 Finanční Analyticky Urad. *Contact*. Disponível em: <https://www.financnianalytickyurad.cz/kontakty.html>. Acesso em: 25 maio 2021.

5.2.6. CANADÁ

A UIF do Canadá, denominada *Financial Transactions and Reports Analysis Centre of Canada* (FINTRAC) é outra que se destaca dentre as analisadas. O site[223] é, sobretudo, muito elucidativo e completo, porém cumpre analisar como ele se conforma a cada um dos critérios definidos.

Primeiramente, no que toca ao critério navegabilidade do site, está o maior dos destaques, que lhe rende a nota 10 no quesito. As múltiplas abas permitem observar especificamente diversos aspectos do FINTRAC. De maneira geral, na aba *Obligations* são encontradas informações sobre quais são as regras que regem e instituem a UIF, bem como as leis e as penalidades que esta aplica. Já a aba Guidance possui informações sobre *compliance* com as atividades do órgão, também elaborando mais sobre como se dá a sua atuação. A aba *Reporting to FINTRAC*, conforme antecipa seu nome, trata de quem são as entidades obrigadas a reportar e como reportar à UIF. A aba *Reporting entities* elabora mais sobre o tópico de quem deve reportar. A aba *Financial Intelligence* se aprofunda no operacional do FINTRAC, demonstrando por meio de fluxogramas e texto como funciona a construção de um caso pelo órgão. Por fim, a aba *Publications* merece grande destaque, já que nela estão contidos, dentre outros, relatórios anuais que abrangem todos os aspectos da atuação da UIF, permitindo saber tudo o que foi feito, inclusive quanto ao tratamento de dados.

Quanto ao critério de informações sobre tratamento de dados, este também se mostra positivo. A nota 9,5 que foi atribuída ao quesito se deve tanto às informações que são oferecidas pelo site, como o fluxograma de como é construído um caso, quanto ao relatório anual, que inclusive tem um tópico próprio para abordar a proteção da privacidade.

Os critérios informações sobre estrutura da UIF e informações sobre a quais dados o cidadão pode exigir acesso são de menor destaque e recebem a nota 7. Isso se deve à dispersão dessas informações pelo site, sem estarem necessariamente concentradas em um local, e também à menor disponibilidade das mesmas. Muitas das UIFs analisadas apresentam um fluxograma de como se estrutura a UIF[224], porém o FINTRAC não possui isso, mas sim informações dispersas sobre sua organização. Os dados que podem ser exigidos são mais dedutíveis da regulamentação apresentada, já que não existe seção específica para abordar o tópico.

223 CANADA, Financial Transactions and Reports Analysis Centre of. Homepage. Disponível em: <https://www.fintrac-canafe.gc.ca/intro-eng>. Acesso em: 22 maio 2021.

224 Como exemplos podem ser citados os Estados Unidos (NETWORK, Financial Crimes Enforcement. *Homepage*. Disponível em: <https://www.fincen.gov/>. Acesso em: 12 jun. 2021.), ou a Colômbia (FINANCIERO, Unidad de Información y Análisis. *Homepage*. Disponível em: <https://www.uiaf.gov.co/>. Acesso em: 12 jun. 2021.), além de outros,

6. CRIAÇÃO DO BENCHMARK

6.1. ASPECTOS GERAIS

Após a análise detalhada de cada um dos seis países classificados como Categoria 1, buscou-se filtrar e encontrar exemplos positivos e boas práticas realizados por estes seis países que podem ser consideradas como ideias para o portal virtual de uma UIF. A partir disso e com base nos cinco critérios utilizados para a análise dos sites de Categoria 1, buscamos demonstrar de que forma as UIFs poderiam abordar cada um dos critérios e quais elementos são essenciais para a excelência do site no âmbito da transparência quanto ao tratamento e proteção de dados.

Sobre a existência de site próprio, consideramos que tal aspecto é de fundamental importância para que o cidadão que queira ter acesso às informações sobre tratamento de dados possa encontrar o site de maneira mais fácil e direta. Também auxiliará no entendimento da estrutura da UIF e de que forma se dará sua atuação.

Além disso, imaginamos uma estrutura básica para os sites das UIFs, contendo as principais informações que são indispensáveis para o público. O objetivo de se estabelecer uma estrutura básica para as UIFs seria, justamente, padronizar as informações apresentadas e garantir um nível comum de transparência quanto ao tratamento e proteção de dados. Nesse sentido, Ana Carolina Carlos de Oliveira afirma que a padronização dos sites do Grupo de Egmont poderia ser um caminho positivo: "Claro que sim, os sites são um verdadeiro desastre atualmente, cada país divulga o que quer, ou seja, quase nada".

1. SOBRE A UIF Com este tópico, o cidadão poderá entender qual objetivo da UIF, que tipo de atuação ela terá, bem como outras informações básicas que familiarizarão o grande público sobre o que é uma UIF, com destaque para o site do Canadá nesse quesito.

2. CONTATO Neste tópico estarão dispostos os canais de contato da UIF e de que forma o cidadão poderá contatar o órgão para quaisquer tipos de dúvidas, reclamações, sugestões ou demais comentários que deseje fazer.

3. PUBLICAÇÕES É costumeiro que as UIF realizem relatórios anuais sobre como foi sua atuação durante aquele período para informar o público sobre as atividades realizadas e a eficácia do órgão. Porém, em

alguns casos, como o da UIF estoniana, também são oferecidas outras publicações como pesquisas feitas pelo órgão. Portanto, no espaço das publicações se imaginou uma plataforma para que a UIF possa compartilhar seu trabalho com o público que a acessa, não se limitando a Relatórios Anuais.

4. LEGISLAÇÃO NACIONAL A atuação das UIF está baseada, principalmente, nas leis internas de seu país e apresentar a quais leis o órgão se submete é essencial para que se entenda que tipos de respostas e de procedimentos os titulares de dados devem esperar. No setor de Legislação Nacional, entretanto, não se deve limitar a apresentar a legislação de lavagem de dinheiro e de combate ao terrorismo e sim, expandir para a legislação de proteção de dados que, mesmo não sendo a atuação principal da UIF, é de suma importância para o público.

5. LEGISLAÇÃO INTERNACIONAL Como abordado no subtópico "Descrição do Problema", o combate e prevenção à lavagem de dinheiro tem se caracterizado como esforço global, em que países do mundo se unem para adotar práticas comuns e trocar conhecimento. Dessa forma, é imprescindível que também seja apresentada a legislação aplicável, novamente, não se restringindo à lavagem de dinheiro e combate ao terrorismo.

6 ÓRGÃOS ENVOLVIDOS Nesse tópico deve-se apresentar a quais órgãos a UIF está subordinada e para quais órgãos poderá enviar informações e receber requerimentos, para que o público entenda a extensão da atuação da UIF.

7. MANUAIS A ideia para que haja manuais no site surgiu da análise da UIF da Estônia que apresenta guidelines voltados para o público sobre como identificar operações suspeitas, o que caracteriza uma operação suspeita, de que forma deverá submeter a transação suspeita para a análise da UIF, entre outras. Esses documentos são de fundamental importância, pois auxiliam o público a compreender como deve atuar para prevenir e combater a lavagem de dinheiro. Os manuais não devem se restringir aos exemplos citados e podem abordar quaisquer informações relevantes para que o público tenha conhecimento.

6.2. TRATAMENTO DE DADOS PESSOAIS

Um limite natural à transparência do tratamento de dados pelas UIFs diz respeito à necessária evitação de alerta aos possíveis autores sobre como o processo de detecção é feito. É possível, porém, pensar em um modelo que não ultrapasse esse limite e que, mesmo assim, transmita ao público, de forma clara, qual é o procedimento de tratamento e de proteção de dados.

Para isso, destacamos os exemplos da UIFs da Estônia e da Itália que, em seus sites, apresentam informações profundas e claras sobre como é feito o tratamento e proteção de dados nas diversas etapas: recebimento da comunicação, armazenamento, transmissão, proteção e utilização dos dados. Em ambos os casos, os documentos que apresentam tais informações são a própria legislação ou leis gerais de proteção de dados. O que fazer, então, nos casos de UIFs que não tenham a legislação específica e clara que Estônia e Itália têm?

No caso de países que ainda não tem uma legislação nacional protetora de dados pessoais no setor da segurança pública e persecução penal, parece-nos que as UIFs podem esclarecer publicamente como o tratamento de dados é feito internamente, mesmo diante da inexistência de exigência legal.

Isso pode ser feito por meio de relatórios anuais que buscam quantificar e expor a atuação das UIFs. Neste ponto, destacam-se os exemplos do Canadá e da República Tcheca. Os relatórios periódicos são de fundamental importância para que se possa compreender que tipos de dados são utilizados pelas UIFs, mesmo que de forma genérica, de quais setores as comunicações estão sendo recebidas e para quais órgãos estão sendo transmitidas.

O uso de linguagem acessível é um elemento fundamental para que o público possa não só acessar as informações, mas também compreender o que está sendo dito e entender os efeitos do tratamento de seus dados pessoais. Assim, a UIF deve buscar adaptar temas muitas vezes carregados de termos técnicos ou jurídicos para uma linguagem acessível e que permita o entendimento dos temas mais complexos.

Nesse sentido, duas medidas devem ser tomadas. A primeira delas é a tradução do conteúdo. No mundo globalizado que temos, as relações pessoais e comerciais não se limitam às fronteiras nacionais e, assim, pessoas de diferentes nações podem ter interesse em entender como seus dados são tratados e protegidos em UIFs de nações estrangeiras. Dessa forma, o site deve ser redigido não só na língua nativa do país que representa, mas também em inglês ou qualquer outra opção adicional que seja útil. Ademais, a tradução para outras línguas não deve se limitar às informações básicas do site, mas deve se estender até os documentos técnicos e legislação indicada no site. Nesse sentido, destaca-se o site da UIF da Estônia que apresenta todos os documentos em inglês, além de estoniano.

A segunda diz respeito à linguagem que será utilizada, ou seja, os termos que serão empregados e a maneira como a informação será veiculada ao grande público. É preferível que se utilize termos não tão carregados de tecnicidade, mas sim os mais acessíveis para o público.

Por fim, quando nos referimos a linguagem acessível, não estamos discutindo apenas a gramática dos textos e sim, o meio de comunicação com o público. Opções como vídeos, infográficos e textos interativos podem auxiliar no entendimento do que está sendo abordado e são opções aceitáveis para se comunicar com o público.

Quanto à profundidade de informações, elas devem atender ao limite de não alertar possíveis autores do crime, mas também não devem ser genéricas. A Estônia pode ser um modelo nesse sentido. O site da UIF apresenta uma normativa interna elaborada pelo Ministério do Interior que destaca de que forma os processos internos se darão, desde o recebimento da comunicação até sua transmissão para os órgãos de persecução penal. Nesse documento é interessante notar de que formas as disposições são redigidas, trazendo termos específicos quando possível e elementos quantitativos quando não forem prejudiciais. Ao abordar o banco de dados utilizado pela UIF, o documento inclusive apresenta o nome desse banco de dados. Já sobre os elementos quantitativos, esses aparecem, principalmente, na previsão de quanto tempo os dados ficarão armazenados nos arquivos dos órgãos. Essas informações podem ser vistas em outros países da Categoria 1.

Apesar de ser considerado um aspecto positivo do site estoniano, a profundidade das informações sobre o tratamento e proteção de dados feita de maneira transparente, pode ser objeto de crítica, como a feita por Ana Carolina Carlos de Oliveira: “Eu particularmente sou contrária à transparência das informações, porque não estamos frente a um órgão policial. Entendo que a UIF é um órgão de inteligência e estratégia, e que seus meios de investigação têm que ser preservados”.

Sobre os Relatórios Anuais, apesar de repletos de informações quantitativas, pois buscam demonstrar a eficácia da atuação da UIF, mesmo essas informações são genéricas. Por exemplo, no caso de origens das comunicações, os Relatórios, geralmente, contêm apenas os setores provenientes da comunicação, sem qualquer outra qualificação para não alertar sobre os locais ou setores da sociedade mais propícios para se lavar dinheiro.

Por fim, a relação entre as UIFs e o público é fundamental, tanto para receber as comunicações suspeitas quanto para reportar de que forma se dá sua atuação. Para potencializar essa relação, devem ser abertos de canais de comunicação entre o órgão e o público, inclusive as pessoas obrigadas. Deve ser de fácil acesso e de fácil entendimento o portal onde as pessoas obrigadas, bem como terceiros, reportam operações suspeitas, com o devido sigilo. É importante que este portal esteja no próprio site da UIF e que também sejam apresentadas, ainda que de forma meramente ilustrativa,

quais características de uma operação a tornam suspeita, bem como indicar quais tipos de dados e informações devem estar constar da comunicação. É igualmente importante que haja um canal aberto para que os cidadãos e demais entes da sociedade possam requerer à UIF as informações que estão sendo ou que foram utilizadas pelo órgão. Um país que se destaca nesse sentido é a Espanha que apresenta um canal de transparência, no qual os cidadãos podem submeter suas solicitações, para quem e sobre o que as solicitações de informações devem ser feitas. De acordo com Ana Carolina Carlos de Oliveira, pode-se imaginar um modelo em que "os cidadãos podem requerer o acesso às suas informações sobre investigações já encerradas e então pedir a retificação dos seus dados", ou ainda um modelo em que: "deve haver sigilo das análises em curso. E que depois de alguns anos a UIF poderia notificar o cidadão, para que ele tenha direito de pedir a retificação dos dados".

7. CONCLUSÃO

Em síntese, cinco foram os fatores identificados para avaliação de transparência no tratamento de dados pessoais por UIFs: (i) website próprio para a UIF com navegabilidade adequada; (ii) clareza acerca de como é feito o tratamento de dados; (iii) uso de linguagem acessível ao público; (iv) profundidade adequada de informações; e (v) canal de comunicação adequado com o público.

É desejável para o fator (i) que haja no website da UIF seções de informações sobre a UIF, contato com o público, publicações, legislação nacional, legislação internacional, órgãos envolvidos e manuais. Já para o fator (ii), espera-se que haja informações sobre como é feito o tratamento de dados sem romper barreiras que imponham empecilhos ao funcionamento das UIFs, tal como se dá na Itália e Estônia. Para o fator (iii), destaca-se a clara vantagem de se ter uma UIF com conteúdos acessíveis em linguagens globais, como o inglês. Sob a ótica do fator (iv), espera-se que uma UIF proporcione profundidade de informações que permita compreender o que ocorre do momento do recebimento de uma informação até sua saída da UIF, mas personalizando àquilo que melhor se adequa ao cenário legislativo de cada país. Por fim, no fator (v), é desejável que o público possa buscar sanar dúvidas, sem que isso imponha prejuízo à prossecução penal.

A UIF brasileira, como visto, foi alocada na Categoria 2, o que é um sinal positivo considerando a inexistência, entre nós, de uma LGPD para o setor da segurança pública e persecução penal. Melhorias podem, porém, ser feitas sob a luz dos fatores acima indicados. O site deixa a desejar no fator (i) do benchmark ao não ter um site próprio que apresente todas as seções desejáveis. As informações são dispersas e escassas, e somente a seção contato é expressa e clara. Já no fator (ii), novamente há carência de informações. Há uma seção sobre tratamento de dados, mas esta se limita somente a vagas referências à LGPD, sem que haja verdadeira elucidação acerca do que é feito com os dados pessoais. No fator (iii), como só há possibilidade de consulta ao site em português, mudanças deveriam ser feitas para adequação ao benchmark estabelecido. No fator (iv), a profundidade de informações é superficial. Isso é bem exemplificado pela seção de tratamento de dados, mas também pode ser visto ao longo de toda a seção de "Acesso à informação" do site. Por fim, no fator (v), há canal de comunicação claro e de fácil acesso, muito embora sua eficiência seja desconhecida.

Quanto ao resultado geral de todos os países analisados, percebe-se pelo gráfico exposto no item II, D, que o panorama global é substancialmente abaixo do benchmark. A média de navegabilidade dos sites é baixa: 5,46 de 10. Isto se deve ao fato de que, consistentemente, são encontrados países cuja UIF sequer apresenta site próprio, de modo que não há que se falar em navegabilidade de sites tão limitados. A média de informações sobre tratamento de dados é de 4,01, pois são pouquíssimos os países que, como Itália e Estônia, dedicam seções dos sites a isso e realmente se propõem a explicitar quanto for possível o que é feito com os dados. Já a média de informações sobre estrutura das UIFs

é de 5,10, pois muitas sequer demonstram como se estruturam. A média de informações sobre quais dados o cidadão pode exigir saber é de 3,85, sendo a mais baixa de todas.

Essas informações evidenciam a distância entre o nível geral mundial e o atendimento ao benchmark traçado quanto à transparência no tratamento de dados pessoais por UIFs. Há um longo caminho a ser percorrido e o grande impulsionador, como a pesquisa demonstrou, é a aprovação de robustas leis gerais de proteção de dados no âmbito da segurança pública e da persecução penal.

8. REFERÊNCIAS BIBLIOGRÁFICAS

- Administración General del Estado. *Portal de la Transparencia*. Disponível em: <https://transparencia.gob.es/>. Acesso em: 20/05/2021.
- ALLDRIDGE, Peter. *What Went Wrong With Money Laundering?* London: Palgrave Macmillan, 2016.
- BORGES, Ademar. O relatório de inteligência financeira como meio de obtenção de prova no processo penal. *Revista Brasileira de Ciências Criminais*. Vol. 176. Ano 29. p. 69-105. São Paulo: Ed. RT, fevereiro/2021.
- BRASIL. Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal. Disponível em: <https://www.conjur.com.br/dl/anteprojeto-lei-disciplina-protecao.pdf>. Acesso em: 26/05/2021.
- BRASIL. Lei Complementar nº 105, de 10 de janeiro de 2001. *Lei Complementar nº 105, de 10 de janeiro de 2001*. Brasília, DF.
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei nº 13.709, de 14 de agosto de 2018. Brasília, DF.
- BRASIL. Lei nº 9.613, de 03 de março de 1998. Lei Nº 9.613, de 3 de março de 1998. Brasília, DF.
- BRASIL. Lei nº 13.974, de 07 de janeiro de 2020. Lei Nº 13.974, de 7 de janeiro de 2020. Brasília, DF.
- CAMPOS, Eduardo. *Lavagem de dinheiro movimenta R$6 bilhões por ano no Brasil, diz BC*. 2016. Disponível em: <https://valor.globo.com/financas/noticia/2016/11/17/lavagem-de-dinheiro-movimenta-r-6-bilhoes-por-ano-no-brasil-diz-bc.ghtml>. Acesso em: 20/05/2021.
- CANADÁ. *Financial Transactions and Reports Analysis Centre of Canada*. Disponível em: <https://www.fintrac-canafe.gc.ca/intro-eng>. Acesso em: 22/05/2021.
- Conselho de Controle de Atividades Financeiras. *Análise de Informações*. Disponível em: <https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-producao-de-inteligencia-financeira/analise-de-informacoes>. Acesso em: 13/05/2021.
- Conselho de Controle de Atividades Financeiras. *A Produção de Inteligência Financeira*. Disponível em: <https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-producao-de-inteligencia-financeira>. Acesso em 13/05/2021.
- Conselho de Controle de Atividades Financeiras. *Disseminação de Relatórios de Inteligência Financeira*. Disponível em: <https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-producao-de-inteligencia-financeira/inteligencia-financeira-em-numeros>. Acesso em 13/05/2021.
- Conselho de Controle de Atividades Financeiras. *Fale Conosco*. Disponível em: <https://www.gov.br/coaf/pt-br/canais_atendimento/copy_of_contatos>. Acesso em: 16/05/2021.
- Conselho de Controle de Atividades Financeiras. *Recepção de Comunicações*. Disponível em: <https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-producao-de-inteligencia-financeira/inteligencia-financeira>. Acesso em 13/05/2021.
- Conselho de Controle de Atividades Financeiras. *2020 Relatório de Atividades*. Disponível em: <https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/relatorio-de-atividades-2020-publicado-20210303.pdf>. Acesso em: 13/05/2021.
- Conselho de Controle de Atividades Financeiras. *Tratamento de Dados Pessoais sujeito à Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: <https://www.gov.br/coaf/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais>. Acesso em: 23/05/2021.
- Conselho de Controle de Atividades Financeiras. *O que faz o COAF?* Disponível em: <https://www.gov.br/coaf/pt-br>. Acesso em: 13/05/2021.
- COSTA, V. B. A. A. B. D. M. W. A. C. C. B. F. D. S. E. M. A. D. S. Proteção de dados pessoais e investigação criminal. 1. ed. Brasília: ANPR, 2020. p. 587-595. em: <http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf>. Acesso em: 02/06/2021.

- Egmont Group. *Financial Intelligence Units (FIUs). 2021*. Disponível em: <https://egmontgroup.org/en/content/financial-intelligence-units-fius>. Acesso em: 15/05/2021.
- ESPANHA. Lei nº 19, de 9 de dezembro de 2013. Lei nº 19, de 9 de dezembro de 2013. Madrid.
- ESPANHA. Lei orgânica nº 7, de 27 de maio de 2021. Lei orgânica nº 7, de 27 de maio de 2021. Madrid.
- ESPANHA. Lei nº 10, de 28 de abril de 2010. Lei nº 10, de 28 de abril de 2010. Madrid.
- ESTÔNIA. *Money Laundering and Terrorist Financing Prevention Act, de 27 de novembro de 2017*. Tallinn.
- European Parliament. Regulamento (EU) 2016/679. Disponível em: <https://eur-lex.europa.eu/legal content/PT/TXT/PDF/?uri=CELEX:32016R0679#:~:text=REGULAMENTO%20%28UE%29%202016%2F%20679%20DO%20PARLAMENTO%20EUROPEU%20E,de%20Dados%29%20I%20.%20%28Atos%20%20legislativos%29%20>. Acesso em 23/05/de 2021.
- European Parliament. *Directive (EU) 2016/680*. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680>. Acesso em: 23/05/2021.
- European Parliament. *Regulation (EU) 2018/1725 of the European Parliament and of the Council*. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725>. Acesso em: 19/05/2021.
- European Union. *Directive (EU) 2015/849 of the European Parliament and of the Council*. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849>. Acesso em: 19/05/2021.
- European Union. *General Data Protection Regulation*. Disponível em: <https://gdpr-info.eu>. Acesso em: 23/05/2021.
- Finanční Analyticky Urad. *Finanční Analyticky Urad*. Disponível em: <https://www.financnianalytickyurad.cz/>. Acesso em: 25/05/2021.
- MAILLART, J.B.; VOGEL, B. *National and International Anti-money Laundering Law*. Freiburg: Intersentia, 2020.
- Republic of Estonia. *Financial Intelligence Unit*. Disponível em: <https://www.fiu.ee/en>. Acesso em 20/05/2021.
- Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. *Financial Intelligence Unit*. Disponível em: <https://www.sepblac.es/en/abt-sepblac/financial-intelligence-unit/>. Acesso em 20/05/2021.
- UIF – Unidade de Informação Financeira. *UIF – Unidade de Informação Financeira*: prevenção e combate ao branqueamento de capitais e financiamento do terrorismo. Prevenção e Combate ao Branqueamento de Capitais e Financiamento do Terrorismo. Disponível em: <https://uif.policiajudiciaria.pt>. Acesso em: 20/05/2021.
- UIF – Unità di Informazione Finanziaria. *Unità di Informazione Finanziaria per l'Italia*. Disponível em: <https://uif.bancaditalia.it/homepage/index.html?-com.dotmarketing.htmlpage.language=1>. Acesso em: 20/05/2021.
- United Nations Office on Drugs and Crime. *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes: research report*. Research report. Disponível em: <https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf>. Acesso em: 10/05/2021.
- CANADA, *Financial Transactions and Reports Analysis Centre of. Homepage*. Disponível em: <https://www.fintrac-canafe.gc.ca/intro-eng>. Acesso em: 22/05/2021.
- NETWORK, Financial Crimes Enforcement. *Homepage*. Disponível em: <https://www.fincen.gov/>. Acesso em: 12/06/2021.
- FINANCIERO, Unidad de Información y Análisis. *Homepage*. Disponível em: <https://www.uiaf.gov.co/>. Acesso em: 12/06/2021.

UMA ANPD PARA A PROTEÇÃO DE DADOS NA SEGURANÇA PÚBLICA E NA PERSECUÇÃO PENAL?

UMA ANPD PARA A PROTEÇÃO DE DADOS NA SEGURANÇA PÚBLICA E NA PERSECUÇÃO PENAL?

Andrey Fortes
Frederico Amaral
Nicolas Haspo

AGRADECIMENTOS

Agradecemos, em especial, às Professoras Eloísa Machado de Almeida e Heloisa Estellita, responsáveis pela criação do "Projeto Multidisciplinar - Proteção de Dados e Segurança Pública", por proporcionarem todo o conhecimento alcançado pelo grupo e pela ajuda na elaboração do presente trabalho.

A Professora Heloisa Estellita, além disso, acompanhou de maneira mais próxima este trabalho, tendo sido essencial para sua realização por meio de enriquecedoras observações e orientações e por possibilitar o contato com as pessoas entrevistadas.

Agradecemos também ao assistente acadêmico Douglas Norkevicius e à monitora Bárbara Prado Simão, que contribuíram fortemente para a organização do Projeto. Douglas Norkevicius também nos ajudou a organizar as entrevistas, tendo acompanhado todas elas. E Bárbara Prado Simão teve grande influência no nosso trabalho, por ser coautora da pesquisa "Autoridades de proteção de dados na América Latina: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai".

Agradecemos, ainda, ao Ministro Nefi Cordeiro, ao Procurador da República Vladimir Aras, ao Professor Renato Sérgio de Lima, ao Professor Danilo Doneda e à doutoranda Jacqueline de Souza Abreu, que foram fundamentais para a nossa pesquisa por conta das informações e entendimentos compartilhados por meio das entrevistas.

Agradecemos, por fim, aos convidados e às convidadas que participaram do Projeto por meio de importantíssimas aulas e palestras acerca da proteção de dados na segurança pública: Nathalie Fragoso (InternetLab); João Paulo Dorini (Defensor federal e Defensor Regional de Direitos Humanos em São Paulo da Defensoria Pública da União); Fernanda Campagnucci (Open Knowledge Brasil); Bruno Bioni (Data Privacy Brasil).

1. INTRODUÇÃO

O desenvolvimento e uso de tecnologias que fazem uso massivo de dados pessoais e sensíveis da população é uma das características mais marcantes do século XXI. A pauta da proteção de dados vem tomando grandes proporções no mundo inteiro. Os Estados, a fim de proteger os direitos civis de seus cidadãos, vêm elaborando regulamentações abrangentes para resguardar um maior escopo de direitos e, ao mesmo tempo, específicas, no que tange à definição de conceitos imprescindíveis e de competências de autoridades fiscalizadoras.

No Brasil, uma das principais discussões sobre o tratamento de dados no âmbito de uma futura lei geral de proteção de dados para a segurança pública e para a persecução penal (adiante, SP/PP) recai na definição de um órgão governamental. Autoridade essa que supervisionaria a aplicação das leis de proteção de dados nas searas supracitadas, o que inclui a competência de fiscalizar e sancionar conforme o texto legal.

Na data da conclusão do presente trabalho, em junho de 2021, vigora a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), a qual criou a Autoridade Nacional de Proteção de Dados (ANPD)[225], um órgão submetido à Presidência da República (art. 55-A), à qual incumbe a fiscalização e a aplicação da lei. No entanto, a proteção dos dados referentes à segurança pública e à persecução penal não estão abarcados pela competência da ANPD por força do que dispõe o art. 4º, inciso III, alínea "a" e "d", LGPD[226]. Assim, atualmente, o país não conta com uma lei geral de proteção de dados para a SP/PP.

Tendo em vista a necessidade de uma legislação específica, o Presidente da Câmara dos Deputados, em 26 de novembro de 2019, instituiu uma Comissão de Juristas que elaborou o Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal[227]. Segundo a proposta, a autoridade competente para atuar na proteção de dados no setor da segurança pública e persecução penal seria a Unidade Especial de Proteção de Dados em Matéria Penal (adiante, UPDP)[228].

225 A ANPD foi inserida na LGPD pela Lei 13.853/19.

226 "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: [...] II - realizado para fins exclusivos de: a) segurança pública; [...] d) atividades de investigação e repressão de infrações penais;"

227 COMISSÃO DE JURISTAS DA C MARA DOS DEPUTADOS. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Disponível em <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf>. Acesso em: 25 maio 2021.

228 "Art. 59. O Conselho Nacional de Justiça (CNJ), por meio da sua Unidade Especial de Proteção de Dados em Matéria Penal (UPDP), será responsável por zelar, implementar e fiscalizar a presente lei em todo o território nacional."

A fim de melhor executar uma política de fiscalização e sanção dos órgãos do governo, é imprescindível que a autoridade tenha autonomia e independência perante os três Poderes. Isso porque competirá a ela a supervisão de órgãos públicos como as secretarias de segurança pública, as polícias, o Ministério Público e o Poder Judiciário. Porém, em um cenário em que se deve respeitar a independência entre os três Poderes, bem como a autonomia do Ministério Público, há evidentes dificuldades em se estabelecer um arranjo institucional em que a autoridade garanta o fiel cumprimento da lei.

Deste espectro de atuação da UPDP surgem diversas complexidades relacionadas à sua capacidade de executar plenamente os comandos legais. Dentre eles, a não submissão dos órgãos e poderes governamentais diante das determinações da autoridade é o principal problema. Alguns destes obstáculos não se limitam à futura UPDP, mas também estão postos na realidade atual, pois todos os órgãos supracitados também fazem tratamento de dados para fins não penais - por exemplo, processamento da folha de pagamento, emissão de identidade pessoal - e, assim, já estão eles sujeitos à LGPD e às determinações da ANPD, podendo-se incorrer no mesmo problema de insubmissão.

Diante de um arranjo institucional da ANPD que não se pode apenas transplantar para a regulamentação dos campos de SP/PP, surge a problemática acerca de onde alocar a "ANPD penal" de maneira a otimizar as suas competências de fiscalização e sancionamento do poder público.

À vista disso, para uma melhor compreensão acerca da alocação da instituição reguladora da proteção de dados no âmbito da segurança pública e persecução penal, faz-se necessário estabelecer, desde já, o que se entende por segurança pública e por persecução penal. A segurança pública possui duas concepções desde a reabertura democrática: a uma, pode ser relacionada ao conceito de combate, em que é dever das instituições elencadas no rol do art. 144, Constituição Federal brasileira de 1988 (CF/88), combater criminosos; a duas, conceito centrado na ideia de prestação de serviço público realizado pelo Estado, em que o cidadão é o destinatário deste serviço, executando-se políticas sociais[229]. Já a persecução penal consiste no processo de investigação penal em que se produz elementos probatórios para apurar determinada conduta delitiva e, assim, formar a convicção do órgão acusatório[230], todavia, no âmbito deste trabalho, será entendida de forma mais ampla, que é aquela escolhida pelo referido Anteprojeto de Lei:

229 SOUZA NETO, Cláudio Pereira de. Da Segurança Pública: art. 144. In: CANOTILHO, J. J. Gomes; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; STRECK, Lenio Luiz. *Comentário à Constituição do Brasil*. São Paulo: Saraiva, 2013. p. 3389.

230 NUCCI, Guilherme de Souza. *Código penal comentado*. 17. ed. rev., atual. e ampl. Rio de Janeiro: Forense, 2017. p. 693 e 898.

> "toda e qualquer atividade exercida para a investigação, apuração, persecução e repressão de infrações penais e execução de penas, por autoridades competentes, inclusive aquelas de inteligência policial, institucional e financeira realizada por autoridades competentes para a finalidade de persecução penal"(art. 5º, XXII).

Ante o exposto, o escopo deste estudo é analisar diferentes arranjos institucionais referentes à proteção de dados na esfera da SP/PP e, a partir disso, indicar aquele que melhor se aplica ao contexto brasileiro, qual seja o de que a autoridade supervisora consiga regulamentar as ações dos entes estatais, bem como garantir a aceitação e subordinação destes à decisão proferida por aquela. Para tanto, o estudo foi desenvolvido da seguinte forma: inicia-se com uma análise do papel, funções, importância e pressupostos de uma ANPD (*infra*, *2*); examina-se a ANPD na LGPD, atual estruturação e problemas (*infra*, *3*); apresenta-se o Anteprojeto de "ANPD Penal", tratando sobre a solução ali proposta, bem como seus problemas (*infra*, *4*); analisa-se modelos estrangeiros (*infra*, *5*); com o que podemos apresentar possíveis soluções para o Brasil (*infra*, *6*); apresenta-se uma sugestão de encaminhamento (*infra*, *7*); e concluir (*infra*, *8*).

2. PAPEL, FUNÇÕES, IMPORTÂNCIA E PRESSUPOSTOS DE UMA ANPD

As autoridades nacionais de proteção de dados (ANPD) são órgãos responsáveis pela implementação e cumprimento da legislação de proteção de dados pessoais[231]. Tais órgãos são definidos como:

> **[...]** órgãos públicos dotados de substancial independência do governo, caracterizados pela sua autonomia de organização, financiamento e contabilidade; da falta de controle e sujeição ao poder Executivo, dotadas de garantias de autonomia através da nomeação de seus membros, dos requisitos para esta nomeação e da duração de seus mandatos; e tendo função de tutela de interesses constitucionais em campos socialmente relevantes[232].

Dessa definição, destaca-se a característica principal de uma ANPD: independência em relação ao poder público. Como visto acima, para a implementação dessa característica, a autoridade deve ser dotada de autonomia organizacional e financeira, sendo também necessário que tenha autonomia administrativa e decisória[233]. É importante que a autoridade seja independente tanto do mercado quanto do domínio político, pois somente dessa maneira será garantido o livre fluxo transacional de dados[234], podendo a ANPD exercer seu papel de execução de políticas de privacidade e de proteção de informações pessoais, assim como a função de conscientização da população[235]. A independência é essencial para que a autoridade regule e fiscalize as atividades de dados pessoais realizadas pelo setor privado e pelo poder público[236].

231 BEZERRA, Maria Ruth Borges. *Autoridade Nacional De Proteção De Dados Pessoais: A Importância Do Modelo Institucional Independente Para A Efetividade Da Lei* in Revista Caderno Virtual, v. 2, n. 44. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3828>. Acesso em: 17 maio 2021. p. 13.

232 CARINGELLA, Francesco; GAROFOLI, Roberto. Le autoritá indipendenti. Napoli: Simoni, 2000, p. 10. apud BEZERRA, Maria Ruth Borges. *Autoridade Nacional De Proteção De Dados Pessoais: A Importância Do Modelo Institucional Independente Para A Efetividade Da Lei* in Revista Caderno Virtual, v. 2, n. 44. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3828>. Acesso em: 17 maio 2021. p. 17.

233 BEZERRA, op. cit., p. 13

234 Ibidem. p. 2.

235 SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. *Autoridades de proteção de dados na América Latina: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai*. São Paulo: Instituto Brasileiro de Defesa do Consumidor (Idec), 2019. p. 5-6.

236 GUTIERREZ, Andrei. *Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da*

No que tange à conscientização da população, é crucial o papel da autoridade nacional de promotor ativo de uma cultura de privacidade e de proteção de dados, por meio de campanhas públicas, de comunicação e iniciativas de educação com a população. Nesse ponto, a ANPD deve ser responsável por uma mudança cultural não somente da população, mas também das organizações, de modo a conscientizá-las da necessidade de preocupação em relação ao tratamento de dados pessoais[237].

Além dos papéis e funções mencionados acima, a ANPD deve garantir a proteção de direitos fundamentais[238] e a efetivação jurídica em casos de fronteira, bem como fornecer o detalhamento técnico e tutorial para efetivar as garantias previstas na lei de proteção de dados e a cooperação internacional[239]. Essa cooperação internacional diz respeito tanto a operações que envolvam fluxo transfronteiriço de dados[240] quanto à convergência regulatória com outros países, regiões ou blocos comerciais[241].

Acrescentam-se também o papel de fiscalização e aplicação das sanções administrativas[242] e as funções de "*ouvidores (ombudsman), auditores, consultores, educadores, orientadores de política pública e negociadores*"[243]. Ao exercer a função de aplicar a lei de proteção de dados, a ANPD torna eficiente a tutela da privacidade na medida em que propicia segurança jurídica na interpretação e aplicação dessa lei[244].

Outro ponto diz respeito à autonomia para a nomeação dos membros que irão compor a autoridade nacional. Para que essa autonomia seja atingida, é preciso que os processos de nomeação e afastamento de funcionário sejam transparentes, justos e imparciais[245]. Por isso a importância de que seus integrantes possuam mandatos, o que evita arbitrariedades nas demissões e garante maior

Privacidade in MALDONADO, Viviane Nóbrega (coord.); BLUM, Renato Opice (coord.). LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 399.

237 Ibidem. p. 397.

238 Esse papel de salvaguarda de direitos fundamentais se faz ainda mais relevante no Brasil, já que o Supremo Tribunal Federal reconheceu recentemente a proteção de dados pessoais como um direito fundamental (v. Referendo na Medida Cautelar na ADI 6.387/DF, Rel. Min. Rosa Weber, 1ª T., DJE 19/11/2020).

239 BEZERRA, op. cit., p. 13.

240 SIMÃO, op. cit., p. 6.

241 GUTIERREZ, op. cit., p. 402.

242 GUTIERREZ, op. cit., p. 398.

243 MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental – São Paulo: Saraiva, 2014. p. 49. apud BEZERRA, Maria Ruth Borges. *Autoridade Nacional De Proteção De Dados Pessoais: A Importância Do Modelo Institucional Independente Para A Efetividade Da Lei* in Revista Caderno Virtual, v. 2, n. 44. Disponível em: <https://www.portaldepe-riodicos.idp.edu.br/cadernovirtual/article/view/3828>. Acesso em: 17 maio 2021. p. 13.

244 BEZERRA, op. cit., p. 14.

245 Ibidem. p. 31.

idoneidade em sua conduta[246]. A nomeação deve ser feita com a participação do maior número de entidades possíveis, já que isso garante maior capacidade e incentivo para que a autoridade atue de forma justa e independente, bem como afasta o risco de perda de autonomia que decorreria de nomeação exclusiva por uma entidade governamental ou política[247].

É fundamental que seus membros possuam conhecimento técnico de diversas áreas do conhecimento e sejam especializados em dados pessoais[248]. A existência de um Conselho deve ser prevista para que se garanta uma maior representação social[249].

Quanto a uma ANPD com competência para realizar a proteção de dados no âmbito da SP/PP, além do que foi mencionado anteriormente, são necessárias outras atribuições específicas. Essa ANPD deverá atuar como responsável pela consolidação e notificação dos órgãos de persecução penal sobre infrações a normas que lhe aparentem penalmente típicas e deverá fiscalizar e sancionar sem inviabilizar a eficiência da persecução penal[250].

246 SIMÃO, op. cit., p. 37.

247 BEZERRA, op. cit., p. 33.

248 SIMÃO, op. cit., p. 37.

249 GUTIERREZ, op. cit., p. 396.

250 LODDER, George Neves. *Autoridade Nacional de Proteção de Dados: questões*. In: ASSOCIAÇÃO NACIONAL DE PROCURADORES DA REPÚBLICA. *Proteção de dados pessoais e investigação criminal*. Brasília: ANPR, 2020, p. 116.

3. A ANPD NA LGPD

3.1. ESTRUTURA

De forma a assegurar a proteção aos dados pessoais, o cumprimento da lei e outras questões apresentadas no item anterior, a LGPD criou a ANPD. Conforme o art. 55-A, *caput*, da Lei, este é um órgão da administração pública federal, integrante da Presidência da República, ou seja, está vinculada ao Poder Executivo[251]. Pertence, assim, à administração pública direta, que compreende o conjunto de órgãos integrados na estrutura administrativa da União[252].

Apesar do art. 55-A, *caput* determinar que a ANPD pertence à administração pública direta, o parágrafo primeiro do mesmo dispositivo dispõe que sua natureza jurídica é transitória, podendo ser alterada pelo Executivo para entidade da administração pública federal indireta e, nesse caso, estará submetida a regime autárquico especial e vinculada à Presidência da República. A avaliação quanto a essa transformação ocorrerá em até dois anos da data de entrada em vigor da estrutura regimental da ANPD (art. 55-A, § 2º, LGPD).

Segundo o art. 55-C, ela é composta por: (i) Conselho Diretor, órgão máximo de direção; (ii) Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, órgão consultivo; (iii) Corregedoria; (iv) Ouvidoria; (v) órgão de assessoramento jurídico próprio; (vi) unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei.

Importante ressaltar que os membros do Conselho Diretor serão escolhidos pelo Presidente da República e são por ele nomeados após a aprovação pelo Senado Federal (art. 55-D, § 1º, LGPD), o que reforça ainda mais a vinculação da Autoridade ao Poder Executivo. Os membros terão mandato de quatro anos (art. 55-D, § 3º, LGPD).

251 No mesmo sentido do *caput* do art. 55-A da LGPD, observa-se o art. 1º da Portaria nº 1, de 8 de março de 2021, a qual estabelece o Regimento Interno ANPD, in verbis: "Art. 1º A Autoridade Nacional de Proteção de Dados - ANPD, órgão integrante da Presidência da República criada pela Lei nº 13.709, de 14 de agosto de 2018, dotada de autonomia técnica e decisória, com jurisdição no território nacional e com sede e foro no Distrito Federal, tem por finalidade proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural."

252 MEIRELLES, Hely Lopes. *Direito Administrativo Brasileiro*. São Paulo: Malheiros Editores, 23ª ed., 1998. p. 603.

Em relação às competências concedidas à ANPD pela LGPD, destacam-se:

> **“ I.** zelar pela proteção dos dados pessoais, nos termos da legislação;
> **[...]**
> **III.** elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> **IV.** fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
> **[...]**
> **VI.** promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; **”**
>
> **(ART. 55-J, LGPD)**

Outra competência relevante está prevista no art. 4º, § 3º, LGPD. Segundo este, a Autoridade emitirá opiniões técnicas ou recomendações relativas às seguintes matérias: “*segurança pública*, *defesa nacional*, *segurança do Estado ou atividades de investigação e repressão de infrações penais*”, devendo também solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. A relevância desse dispositivo reside no fato de que o tratamento de dados realizado para fins exclusivos dessas matérias constituem exceções às quais a LGPD não se aplica (art. 4º, III, LGPD) e que deverão ser reguladas por legislação específica (art. 4º, § 1º, LGPD). Assim, a ANPD já possui competência, ainda que reduzida, para atuar nessas matérias, notadamente em SP/PP, que forma o escopo deste trabalho.

O art. 55-K estabelece que é de competência exclusiva da ANPD a aplicação das sanções previstas na LGPD, sendo que suas competências prevalecerão sobre as competências de outras entidades ou órgãos da administração pública no âmbito da proteção de dados pessoais. Para garantir essa disposição e as demais competências da ANPD, a Lei assegura autonomia técnica e decisória à Autoridade (art. 55-B, LGPD).

Os dispositivos mencionados representam a estrutura atual da ANPD, tendo sido incluídos pela Lei nº 13.853/2019, que alterou a LGPD para, dentre outras providências, dispor sobre a proteção de dados pessoais e para criar a ANPD. Ressalta-se que essa alteração, notadamente no que tange à ANPD, não foi uma simples mudança de palavras, mas revelou uma transformação profunda da configuração jurídica da Autoridade tal qual originariamente concebida, o que torna necessário um breve histórico sobre a criação e configuração jurídica da Autoridade.

3.2. HISTÓRICO DE CRIAÇÃO DA ANPD

No dia 13 de junho de 2012, o ex-Deputado Milton Monti, do Partido da República (PR-SP, atual Partido Liberal) apresentou na Câmara dos Deputados o Projeto de Lei (PL) nº 4.060/2012, que dispunha sobre a proteção de dados pessoais e alterava a Lei nº 12.965/2014, também conhecida como o "Marco Civil da Internet"[253]. Nesse PL, não havia qualquer previsão sobre a criação de uma autoridade nacional de proteção de dados, somente se estabelecia a possibilidade das entidades representativas de responsáveis pelo tratamento de dados pessoais instituírem Conselhos de Autorregulamentação que formulariam códigos com parâmetros éticos para o tratamento de dados (art. 23, PL nº 4.060/2012)[254]. Após diversas modificações no PL, o texto final[255] foi submetido, em 29 de maio de 2018, ao Senado Federal, agora já com a previsão da criação da ANPD, que seria integrante da administração pública federal indireta, submetida a regime autárquico especial, com objetivo de conferir independência à Autoridade, e vinculada ao Ministério da Justiça (art. 55, PL nº 4.060/2012)[256].

No Senado Federal, o PL tramitou como Projeto de Lei da Câmara (PLC) nº 53/2018[257]. Em 15 de agosto de 2018, o PLC foi aprovado como Lei Ordinária nº 13.709/2018, a LGPD, com veto parcial (Veto nº 33/2018[258]) por parte do Presidente da República. Nesse ato, o presidente à época, Michel Temer, vetou todos os dispositivos do PLC que tratavam da ANPD (arts. 55 a 59), sob a justificativa de inconstitucionalidade do processo legislativo, considerando a violação do artigo 61, § 1º, II, 'e', cumulado com o artigo 37, XIX, ambos da CF/88. O primeiro preceito constitucional determina que é de iniciativa exclusiva do Presidente da República as leis que disponham sobre a criação e extinção de Ministérios e órgãos da administração pública. Assim, a criação da ANPD não poderia ter sua origem em um projeto de lei da Câmara dos Deputados. Já em relação ao segundo preceito, a violação decorreria da exigência de que autarquias sejam criadas por lei específica, o que não ocorreu *in casu*.

253 BRASIL. Projeto de Lei nº 4.060, de 13 de junho de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 31 maio 2021.

254 BRASIL. Projeto de Lei nº 4.060, de 13 de junho de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 31 maio 2021.

255 BRASIL. Projeto de Lei nº 4.060-A, de 13 de junho de 2012. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0ksapb6v7tyhv-1fxgf17w4iqd4918642.node0?codteor=1665276&filename=Tramitacao-PL+4060/2012>. Acesso em: 31 maio de 2021.

256 "Art. 55. Fica criado o órgão competente, Autoridade Nacional de Proteção de Dados, integrante da administração pública federal indireta, submetido a regime autárquico especial e vinculado ao Ministério da Justiça. § 1º A Autoridade deverá ser regida nos termos previstos na Lei no 9.986, de 18 de julho de 2000. § 2º A Autoridade será composta pelo Conselho Diretor, como órgão máximo, e pelo Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, além das unidades especializadas para a aplicação desta Lei. § 3º A natureza de autarquia especial conferida à Autoridade é caracterizada por independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira. [...]"

257 BRASIL. Projeto de Lei da Câmara nº 53, de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>. Acesso em: 31 maio 2021.

258 BRASIL. Veto nº 33, de 2018. Veto Parcial aposto ao Projeto de Lei da Câmara nº 53 de 2018 (nº 4.060/2012, na Casa de origem), que "Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)". Disponível em: <https://www.congressonacional.leg.br/materias/vetos/-/veto/detalhe/12024>. Acesso em: 31 maio 2021.

Dessa forma, a LGPD foi publicada sem qualquer disposição sobre a autoridade responsável pela proteção de dados no país. Considerando esse vácuo legal, o Presidente da República publicou, em 28 de dezembro de 2018, a Medida Provisória (MP) nº 869[259], que alterou a Lei nº 13.709 para, dentre outras providências, dispor sobre a proteção de dados pessoais e para criar a ANPD[260]. Em relação à ANPD, a MP mudou profundamente o tratamento inicial dado pelo PL nº 4.060/2012, tendo sido determinado que a ANPD seria criada sem despesa e constituiria um órgão da administração pública federal, integrante da Presidência da República (art. 55-A, MP nº 69/2018). A MP também assegurou autonomia técnica à Autoridade (art. 55-B, MP nº 69/2018), que seria composta por: Conselho Diretor, o órgão máximo de direção; Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; Corregedoria; Ouvidoria; órgão de assessoramento jurídico próprio; e unidades administrativas e unidades especializadas necessárias à aplicação da Lei (art. 55-C, MP nº 69/2018).

Na Câmara dos Deputados, o Deputado André Figueiredo (PDT/CE) tentou alterar os dispositivos acima, por meio das emendas 31 - 33 e 113[261], de modo a retomar a estrutura criada pelo referido PL. Entretanto, após a tramitação na Câmara, a MP originou o Projeto de Lei de Conversão (PLV) nº 7/2019[262], no qual foi mantida a redação original da MP, apenas adicionando três parágrafos ao art. 55-A[263]. Esse PLV, no dia 29 de maio de 2019, foi aprovado pelo Senado Federal. A seguir, o PLV foi remetido à sanção presidencial e, no dia 09 de julho de 2019, foi transformada em norma jurídica com veto parcial sobre a receita da ANPD (art. 55-K, V, PLV nº 7/2019)[264]. Daí a atual estrutura atual da ANPD.

259 CONGRESSO NACIONAL. Emendas à Medida Provisória nº 869, de 2018, que "Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências.". Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7915984&ts=1594019729749&disposition=inline>. Acesso em: 31 maio 2021.

260 BRASIL. Medida Provisória nº 869, de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062>. Acesso em: 31 maio 2021.

261 CONGRESSO NACIONAL. Emendas à Medida Provisória nº 869, de 2018, que "Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências.". Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7915984&ts=1594019729749&disposition=inline>. Acesso em: 31 maio 2021. p. 70.

262 BRASIL. Projeto de Lei de Conversão nº 7, de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7948609&ts=1594019727977&disposition=inline>. Acesso em: 31 maio 2021.

263 "[...] § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. § 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. § 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias."

264 BRASIL. Medida Provisória nº 869, de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062>. Acesso em: 31 maio 2021.

3.3. PROBLEMAS

Como visto, a independência é característica essencial de uma ANPD e conferir essa qualidade à Autoridade foi uma preocupação sempre presente no contexto brasileiro, desde o texto final do PL nº 4.060/2012. Entretanto, considerando a estrutura atual da ANPD, caracterizada por seu um órgão da administração pública direta vinculado à Presidência da República, o grau de independência da ANPD é consideravelmente reduzido[265]. Isso significa que a autoridade brasileira não é dotada de toda a independência necessária para exercer as suas funções, o que pode prejudicar enormemente a fiscalização e aplicação de sanções a órgãos públicos independentes, como o Ministério Público e o Poder Judiciário.

Danilo Doneda afirma que a vinculação direta da atividade do órgão a um dos poderes, como ocorre ao pertencer à administração pública direta, pode ocasionar a extinção da independência da autoridade[266]. Sem essa independência, continua, tornam-se inatingíveis as funções e papéis que devem ser desempenhados pela ANPD, uma vez que estas supõem uma neutralidade em relação às próprias razões de Estado[267], pois o que deve prevalecer acima de qualquer coisa é a proteção aos dados pessoais.

Para que gozasse de independência, a ANPD deveria ser uma autarquia, pois este é o modelo ideal do ponto de vista de autonomia dentro do direito brasileiro[268] uma vez que o regime autárquico confere independência financeira, administrativa e técnica[269].

Não é só a vinculação ao Executivo que demonstra a falta de autonomia da ANPD, o próprio art. 55-B da LGPD estabelece somente autonomia técnica e decisória à autoridade, sem garantir sua independência funcional, estatutária e orçamentária[270].

Ademais, dois problemas decorrem dessa falta de autonomia. Em primeiro lugar, há o problema referente à escolha e à nomeação dos membros do Conselho Diretor da ANPD que são de atribuição exclusiva do Presidente da República (art. 55-D, *caput*, LGPD). Isso pode prejudicar a neutralidade do exercício das funções, já que quem ocupará esses cargos poderá ser escolhido com finalidades

265 SIMÃO, op. cit., p. 5.

266 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 401 apud Bezerra, op. cit., p. 17.

267 Idem.

268 BEZERRA, op. cit., p. 56.

269 O próprio Decreto-lei nº 200/1967 concede esse grau de independência às autarquias:
"Art. 5º Para os fins desta lei, considera-se: I - Autarquia - o serviço *autônomo*, criado por lei, com personalidade jurídica, *patrimônio e receita próprios*, para executar atividades típicas da Administração Pública, que requeiram, para seu melhor funcionamento, *gestão administrativa e financeira descentralizada*." (grifos nossos)

270 BEZERRA, op. cit., p. 58.

políticas, o que implica o risco de as posições perderem seu caráter técnico[271]. Em segundo lugar, a inserção comercial do país no fluxo internacional de dados pode estar prejudicada, pois a autoridade é fundamental para viabilizar essa inserção, mas, para isso, não basta sua existência, é necessário que seja independente, pois a independência é um dos requisitos para que o Brasil tenha a adequação de suas normas reconhecidas internacionalmente[272].

Outro problema diz respeito à sua capacidade técnica. Como visto, é necessário que os membros desse órgão possuam elevado conhecimento técnico acerca da proteção de dados. Entretanto, a LGPD apenas faz uma menção geral a isso ao tratar da composição da autoridade, "[...] *unidades especializadas necessárias à aplicação do disposto nesta Lei.*" (art. 55-C, VI, LGPD). Quanto aos membros do Conselho Diretor, não há qualquer menção ou exigência acerca da sua capacitação técnica, exigindo-se isso apenas dos membros do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (art. 58-A, LGPD).

Apesar do Regimento Interno da ANPD (Portaria nº 21/2021) prever a criação da Coordenação-Geral de Tecnologia e Pesquisa (art. 2º, V, "c", Portaria nº 21/2021), um órgão específico singular que detém maior conhecimento técnico acerca da proteção de dados, no que tange aos demais membros não há exigência sobre sua capacidade técnica.

Em suma, a vinculação da ANPD ao Executivo dificulta a consolidação da independência necessária a uma autoridade nacional de proteção de dados, de modo que o exercício de suas funções e papéis encontra-se prejudicado[273], o que se intensifica com a falta de capacidade técnica dos membros da autoridade.

271 SIMÃO, op. cit., p. 37.

272 BEZERRA, op. cit., p. 57.

273 SIMÃO, op. cit., p. 37.

3.4. ENTREVISTAS

Com o objetivo de compreender melhor a estrutura atual da ANPD e seus respectivos problemas, foram realizadas cinco entrevistas com representantes de diversos setores. Entrevistou-se o Ministro Nefi Cordeiro[274] (Poder Judiciário), o Procurador da República Vladimir Aras[275] (Ministério Público), o Professor Renato Sérgio de Lima[276] (FGV), o Professor Danilo Doneda[277] (IDP) e a doutoranda Jacqueline de Souza Abreu[278] (USP).

Nefi Cordeiro apontou três problemas na configuração jurídica atual da ANPD. O problema principal, segundo ele, é o da dependência da ANPD ao Poder Executivo, já que isso pode impedir que ela tenha autonomia suficiente para exercer suas competências, como impor sanções e fiscalizar outros órgãos públicos independentes. O segundo problema, que decorre do primeiro, diz respeito à indicação de membros e à própria composição da ANPD, pois ambas se encontram fortemente dependentes do Executivo, o que significa novamente falta de independência. Já o terceiro problema trata da falta de capacidade técnica da ANPD para atuar no âmbito da proteção de dados.

Visão semelhante tem Vladimir Aras, quem destacou a necessidade de a autoridade reguladora ser independente. Pontuou também que a ANPD tem que ser forte, no sentido de *accountability*, tecnicidade e autonomia na forma de ingresso (mandatos, exoneração etc.). Na ausência destas qualidades, entende que os dados estariam desprotegidos diante o risco de abuso por parte do MP, Judiciário e polícias, colocando o país em risco. Além disso, afirmou ser de extrema relevância disposições sobre matéria penal na LGPD, bem como a existência de uma autoridade que possua competência para isso.

274 É bacharel em Segurança Pública (oficial da Polícia Militar) formado pela Academia Policial Militar do Guatupê (1983), bacharel em Direito pela Faculdade de Direito de Curitiba, atual Centro Universitário Curitiba (1988), além de mestre (1995) e doutor (2000) em direito pela Universidade Federal do Paraná. Também é bacharel em engenharia civil (1998) pela Pontifícia Universidade Católica do Paraná. Foi ministro do Superior Tribunal de Justiça (STJ) de 2014 a 2021. Atualmente, é professor de direito processual penal na Universidade Católica de Brasília (UCB), no Instituto de Educação Superior de Brasília (IESB) e na Universidade do Distrito Federal (UDF).

275 É doutorando em Direito (UNICEUB), mestre em Direito Público pela UFPE, especialista (MBA) em Gestão Pública (FGV), professor assistente de Processo Penal na Universidade Federal da Bahia (UFBA), membro do Ministério Público brasileiro desde 1993, atualmente no cargo de Procurador Regional da República em Brasília (MPF), ex-secretário de cooperação internacional do MPF (2013-2017).

276 Bolsista de Produtividade do CNPq. Professor do Departamento de Gestão Pública da FGV EAESP. Diretor Presidente do Fórum Brasileiro de Segurança Pública. Possui graduação em Ciências Sociais (1995), mestrado (2000) e doutorado em Sociologia (2005) pela Universidade de São Paulo. Também possui Pós-Doutorado no Instituto de Economia da UNICAMP (2010).

277 Mestre e Doutor em Direito Civil pela UERJ. Advogado, especialista em temas de Proteção de Dados e Privacidade. Professor no mestrado em Direito do Instituto Brasiliense de Direito Público e consultor do Comitê Gestor da Internet no Brasil (CGI.br). Membro dos conselhos consultivos do Projeto Global Pulse, da Organização das Nações Unidas, do Projeto Criança e Consumo, do Instituto Alana e da Open Knowledge Brasil. Membro do conselho de orientação editorial da Revista de Direito Civil Contemporâneo.

278 Doutoranda na Faculdade de Direito da Universidade de São Paulo, atua como advogada, mestra em direito pela University of California, Berkeley (EUA), com foco em direito e tecnologia, e pela Ludwig-Maximilians-Universität München (Alemanha), com foco em direitos fundamentais, ex-coordenadora da área de Privacidade e Vigilância do InternetLab.

Em decorrência da ausência de uma LGPD penal, disse que o Brasil não atende aos requisitos mínimos de regulação necessários para poder participar do intercâmbio internacional de dados pessoais que ocorre entre autoridades estrangeiras em matéria de persecução penal.

Renato Sérgio de Lima anunciou um problema que não é particularidade da LGPD: a indeterminação acerca do conceito de segurança pública no ordenamento jurídico brasileiro. Explicou que a proteção dada à segurança pública ocorre em três momentos na Constituição: no art. 5º como um direito necessário para ao exercício da cidadania e como condição para o exercício dos demais, no art. 6º como um direito social e no art. 144 que, de fato, regulamenta as atribuições relativas à segurança pública.

Sobre este último, explicou que o entende como contraditório por se localizar no âmbito da defesa do Estado, reproduzindo a mentalidade (autoritária) presente na Constituição de 1969, em vigor no período da ditadura militar, em total dissonância com o espírito atribuído às disposições dos arts. 5º e 6º. Ainda sobre o art. 144, mencionou que define as polícias judiciárias nas figuras das Polícias Federal e Civis, sendo incumbência destas a investigação e persecução penal, enquanto à Polícia Militar compete a garantia da ordem pública, sendo compreendida como detentora do poder de polícia ostensiva (*enforcement*).

Assim, entende que o conceito de segurança pública não é uníssono, pois quando se discorre sobre esse assunto, é importante realizar esta diferenciação entre investigação e preservação da ordem. O problema reside em uma enorme contradição, na duplicidade de atribuições, em sentido oposto, a uma mesma Instituição, as Polícias Militares. O documento que as regulamenta, o Decreto nº 88.777/1983, afirma que o Exército tem a atribuição de controle das Polícias Militares Estaduais, porém, a Constituição, no art. 144, afirma que o controle e coordenação desses órgãos está subordinado aos Governadores.

Não há, contudo, nenhum questionamento acerca desta contradição perante o STF e, como resultado, na prática, as Polícias Militares operam ainda segundo uma lógica autoritária, pois há conceitos distintos, que indicam arranjos institucionais totalmente diversos, presentes em diferentes leis não recepcionadas pela Constituição, mas também não expressamente vedados por ela. Por este motivo, não há esclarecimento sobre qual de fato vincula as polícias, dando a elas margem para interpretar e agir com discricionariedade, segundo a norma que escolherem no caso concreto.

Danilo Doneda, por sua vez, entende que a ANPD tem a missão de proteger o direito dos cidadãos à proteção de dados, sendo este um direito fundamental, e que deveria ter o poder de supervisionar dados em qualquer órgão público. Entretanto, a autoridade nacional brasileira não possui a autonomia e independência necessárias para isso, pois foi alocada na administração pública direta

e vinculada ao Presidente da República, o que significa falta de autonomia e proximidade a um órgão com grande componente político. Destacou também que o arranjo institucional atual não permite uma tutela isonômica de proteção de dados.

Por fim, Jacqueline de Souza Abreu, reiterando afirmações já feitas por Vladimir Aras, afirmou que não será possível participar de mecanismos de cooperação internacional de dados. Isso porque seria necessário que o Brasil possuísse um nível básico de proteção de dados e, para isso, é preciso, dentre outras coisas, uma autoridade independente de supervisão, o que inexiste atualmente. Ressaltou também que um órgão submetido ao Presidente da República não é um órgão independente.

4. ANTEPROJETO DE ANPD PENAL

Como afirmado, a LGPD não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública e atividades de investigação e repressão de infrações penais (art. 4º, III, "a", "d", LGPD), sendo que ANPD somente tem competência nessas matérias para emitir opiniões técnicas ou recomendações e para solicitar aos responsáveis relatórios de impacto à proteção de dados (art. 4º, § 3º, LGPD). Além disso, o tratamento de dados pessoais no referido âmbito deverá ser regido por legislação específica (art. 4º, § 1º, LGPD).

Disso decorre a necessidade de criação de uma lei de proteção de dados para a SP/PP, sem a qual o tratamento de dados pessoais realizados para esses fins permanecerá desregulado, dificultando enormemente a proteção completa dos dados pessoais. Ciente dessa necessidade, a Câmara dos Deputados instituiu, por meio de ato do seu presidente, uma Comissão de Juristas para elaborar o Anteprojeto de Lei de Proteção de Dados em 26 de novembro de 2019[279]. A Comissão elaborou um Anteprojeto que, em seu art. 6º, reflete os princípios do também art. 6º da LGPD e, no arts. 18 a 28, os direitos dos titulares dos dados previstos nos arts. 17 a 22 da LGPD[280].

Destacamos outros seis pontos relevantes do Anteprojeto.

Em primeiro lugar, o âmbito de aplicação da lei deve considerar que o tratamento de dados precisa sempre ser realizado por uma autoridade competente, exercendo seu papel de controlador[281]. Essa autoridade deve ser entendida no seu sentido constitucional, qual seja: "[...] *a autoridade pública à qual está atribuída a responsabilidade para o exercício de atividades atinentes ao conteúdo deste anteprojeto, inclusive a execução de políticas públicas relacionadas à segurança pública.*"[282].

Em segundo lugar, o Anteprojeto determina que são três as condições de licitude e de legitimidade para o tratamento de dados no âmbito da segurança pública e persecução penal: (i) conformidade com as bases principiológicas da LGPD e do Anteprojeto; (ii) conformidade com os direitos do titular de dados; (iii) necessidade de um comando legal para que o tratamento de dados ocorra[283].

279 COMISSÃO DE JURISTAS DA C MARA DOS DEPUTADOS. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Disponível em <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca--persecucao-FINAL.pdf>. Acesso em: 29 maio 2021.

280 O Anteprojeto foi influenciado pelo Regulamento 679/2016 e pela Diretiva 680/2016, ambos da União Europeia (ibidem. p. 2-3).

281 COMISSÃO DE JURISTAS DA C MARA DOS DEPUTADOS. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Disponível em <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca--persecucao-FINAL.pdf>. Acesso em: 29 maio 2021. p. 3.

282 Idem.

283 Idem.

O terceiro ponto diz respeito à segurança pública e ao sigilo de dados. Essa parte teve grande influência da Diretiva nº 680/2016 da União Europeia e conta com diversas medidas para fins de proteção de dados, previstas no art. 36 do Anteprojeto (e.g. controle do acesso aos dados). Além disso, inclui como elementos fundamentais o acesso a informações e a transparência a modalidades de tratamento realizadas por uma autoridade competente[284].

Em quarto lugar, o Anteprojeto estabelece que a utilização de tecnologias de monitoramento ou o tratamento de dados por autoridade competente que sujeitem os direitos, liberdades e garantias dos titulares dos dados a elevados riscos precisam de previsão legal específica, a qual deve assegurar o que está sob risco e ser precedida de relatório de impacto de vigilância (art. 42, *caput*, Anteprojeto). O art. 42, § 1º apresenta um rol mínimo de critérios voltados à avaliação do risco[285].

Em quinto lugar, há disciplina sobre a transferência internacional de dados. Os arts. 53 a 58 preveem as hipóteses dessa transferência, estabelecem critérios para sua ocorrência, criam medidas que devem ser adotadas para a cooperação internacional de dados e dividem a transferência em três tipos principais: transferências com base numa decisão de adequação, transferências sujeitas a garantias adequadas e derrogações aplicáveis em situações específicas.

Em sexto e último lugar, à autoridade de supervisão do tratamento de dados no âmbito da segurança pública e persecução penal foi alocada no CNJ, como veremos com maior profundidade a seguir.

284 Ibidem. p. 4-5.

285 "Art. 42 [...] § 1º Para fins de avaliação do risco, deve-se considerar, pelo menos: I - a natureza dos dados pessoais envolvidos; II - as finalidades específicas do tratamento; III - a quantidade de agentes de tratamento de dados envolvidos; IV - a quantidade de titulares de dados potencialmente atingidos; V - se é utilizado algum tipo de nova tecnologia; VI - a possibilidade de tratamento discriminatório; e VII - as expectativas legítimas do titular de dados."

4.1. SOLUÇÃO PROPOSTA

Considerando que a ANPD não tem competência para atuar em matéria de SP/PP, estando restrita às hipóteses do art. 4º, § 3º, LGPD, a criação de uma autoridade com competência nessas áreas era uma questão que deveria ser enfrentada pela Comissão. Tendo isso em vista, o Anteprojeto sugeriu a criação de Unidade Especial de Proteção de Dados em Matéria Penal (adiante, UPDP), vinculada ao Conselho Nacional de Justiça (CNJ) e responsável por zelar, implementar e fiscalizar o Anteprojeto no país (art. 59, Anteprojeto).

De maneira semelhante à ANPD, é assegurada autonomia técnica e decisória à UPDP (art. 60, § 1º, Anteprojeto) e sua natureza jurídica é transitória, devendo ser avaliada após dois anos de sua criação (art. 60, § 4º, Anteprojeto). Já em relação à diretoria da UPDP, o Anteprojeto previu mandato de quatro anos aos diretores (art. 60, § 3º, Anteprojeto), que serão escolhidos pelo próprio CNJ (art. 60, § 2º, Anteprojeto). Além disso, o art. 61, caput prevê que a estrutura necessária ao funcionamento da Unidade será provida pelo CNJ por meio do remanejamento de servidores e serviços existentes, bem como a dotação orçamentária, caso necessária. Por fim, o art. 62 estabelece diversas competências à UPDP, merecendo destaque:

> **[...]**
> **I.** zelar pela proteção dos dados pessoais na segurança pública e persecução penal, nos termos da legislação;
>
> **II.** fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
>
> **[...]**
> **IV.** promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais na segurança pública e persecução penal;
>
> **[...]**
> **VI.** promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

> **VII.** solicitar, a qualquer momento, às autoridades competentes submetidas a esta lei informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;
>
> **[...]**
> **IX.** solicitar relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco aos direitos previstos nesta Lei;
>
> **XII.** comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; **[...]**

A escolha de alocação sob o CNJ, conforme a Comissão de Juristas que elaborou o Anteprojeto, justificou-se por este ser dotado de autonomia e de composição plural, o que, juntamente com a imparcialidade, são essenciais para que a Unidade possa realizar suas funções e para a adequação ao nível de proteção e de tratamento de dados internacionais[286]. Essa escolha: (a) evitaria novos gastos com a criação de um órgão específico, (b) aproveitaria a expertise do CNJ na matéria de proteção de dados[287] e (c) possibilitaria a formulação de políticas públicas uniformes para o país todo[288].

286 COMISSÃO DE JURISTAS DA C MARA DOS DEPUTADOS. *Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal*. Disponível em <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf>. Acesso em: 29 maio 2021. p. 6.

287 (Cf, Recomendação CNJ n. 73, de 20/08/2020 e Portaria CNJ n. 63/2019.)

288 COMISSÃO DE JURISTAS DA C MARA DOS DEPUTADOS. *Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal*. Disponível em <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf>. Acesso em: 29 maio 2021. p. 6.

4.2. PROBLEMAS

Apesar dos benefícios apresentados acima, a vinculação da UPDP ao CNJ também possui alguns problemas. O primeiro diz respeito às competências constitucionais do CNJ. Isso porque, caso o rol do art. 103-B, CF/88, que prevê as competência do Conselho, seja considerado taxativo, o CNJ não poderia exercer, em matéria de proteção de dados no âmbito de segurança pública e de persecução penal, a função de agente fiscalizador e aplicador de sanções a outros órgãos públicos, uma vez que não há essa previsão no referido dispositivo.

Não obstante, na hipótese de o rol ser considerado mínimo, haveria a possibilidade de inclusão de novas competências. Ressalta-se que o próprio Regimento Interno do CNJ (Resolução nº 67/2009) já amplia o rol constitucional (art. 4º, I-XXXVI, Resolução nº 67/2009), o que favorece a interpretação segundo a qual o rol não é taxativo.

Desse segundo entendimento decorre um outro problema: o da invasão de competências. Isso ocorreria, pois o art. 129, III, CF/88 determina que o controle externo da atividade policial é uma função institucional do Ministério Público, o que é reforçado pelos arts. 3º, 9º e 10, Lei Complementar nº 75/1993, que dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União. Assim, haveria um vício de competência no Anteprojeto, o que poderia ser objeto de veto e, assim, o tratamento de dados realizados pelas polícias estaria fora do escopo de fiscalização por parte da UPDP.

Além disso, verifica-se que a UPDP está separada da ANPD e, apesar dessa medida ser possível juridicamente[289], pode haver um problema relativo à eficiência da proteção de dados, já que pode ser mais difícil a coordenação entre a atuação das duas autoridades.

Questiona-se também se a vinculação ao CNJ de fato confere a autonomia necessária à UPDP devido a uma questão legal e outra administrativa.

No que tange à questão legal, existem duas controvérsias. A primeira diz respeito à possibilidade de haver recurso das decisões da UPDP ao Plenário do CNJ, uma vez que ela será parte deste. Assim, qualquer decisão poderia ser revisada pelo Plenário, o que pode diminuir a autonomia técnica e decisória da UPDP[290]. A segunda deriva do entendimento de que o Supremo Tribunal Federal (STF) não se submete ao CNJ, sendo que aquele entende que há uma relação de sujeição do Conselho ao

289 REIS, Carolina; COSTA, Eduardo; SILVA, Felipe; BAWDEN, Henrique; PEREIRA, José Renato Laranjeira de; SARMENTO, Paulo. *Nota Técnica: Sobre o Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Investigação Criminal*. Brasília: o Laboratório de Políticas Públicas e Internet - LAPIN, 2020. p. 54.

290 Idem.

Supremo, como pode ser visto no julgamento da ADI 3.367[291]. Em decorrência disso, o STF poderia acabar ignorando as regulamentações no âmbito das suas atividades administrativas e modificando as regras criadas pelo UPDP, no âmbito da sua atuação judicial[292].

No que diz respeito à questão administrativa, o problema é a escolha dos membros da UPDP pelo próprio CNJ. Isso confere ao Poder Judiciário forte influência na definição da diretoria da UPDP, já que a composição do CNJ é, em sua maioria, feita por juízes (art. 103-B, CF/88). Dessa forma, a composição da UPDP pode acabar refletindo, em grande parte, o interesse do Judiciário em detrimento do interesse da sociedade e dos objetivos do Anteprojeto e da LGPD[293].

291 "[...] 4. PODER JUDICIÁRIO. Conselho Nacional de Justiça. Órgão de natureza exclusivamente administrativa. Atribuições de controle da atividade administrativa, financeira e disciplinar da magistratura. Competência relativa apenas aos órgãos e juízes situados, hierarquicamente, abaixo do Supremo Tribunal Federal. Preeminência deste, como órgão do Poder Judiciário, sobre o Conselho, cujos atos e decisões estão sujeitos a seu controle jurisdicional. Inteligência dos arts. 102, caput, inc. I, letra "r", e 103-B, § 4º, da CF. *O Conselho Nacional de Justiça não tem nenhuma competência sobre o Supremo Tribunal Federal e seus ministros, sendo esse o órgão máximo do Poder Judiciário nacional, a que aquele está sujeito*. [...]" (ADI nº 3.367/DF, STF, Rel. Ministro Cezar Peluso, 2ª T., DJe 17/03/2006) (grifos nossos)

292 Idem.

293 Ibidem. p. 55.

4.3. ENTREVISTAS

As entrevistas acima mencionadas também contemplaram as questões relativas à atuação da ANPD no âmbito da SP/PP, bem como sobre o Anteprojeto e sobre a alocação da UPDP sob o CNJ.

Nefi Cordeiro ressaltou que se vive um vácuo legislativo no que tange à proteção de dados no âmbito da segurança pública e da persecução penal. Assim, é necessário que haja uma normatização dessa matéria, inclusive a regulamentação também é necessária para que haja controle do judiciário, já que, sem normas sobre o tema, a sociedade encontra-se sujeita à subjetividade judicial ao tratar desse assunto. Tendo isso em vista, para garantir que a fiscalização e aplicação de sanções por parte da UPDP vincule órgãos públicos independentes é necessário, além da regulamentação dessas matérias, a criação de uma autoridade independente e com competência nesse tema. Isso porque haveria uma enorme resistência por parte de órgãos públicos independentes em aceitar a sujeição a um órgão não independente, como seria o caso da atual ANPD, considerando sua forte vinculação ao Poder Executivo.

Sobre isso, Vladimir Aras afirmou que a solução para conferir a referida garantia é vincular a UPDP a entes já consolidados na estrutura do Estado, como o CNJ e o Conselho Nacional do Ministério Público (CNMP). Renato Sérgio de Lima entende que se deve assegurar à autoridade a competência para realizar o controle externo da atividade policial. E Jacqueline de Souza Abreu, por sua vez, afirmou que essa garantia não corre o risco de ser violada, pois as autoridades já estão submetidas, em parte, à ANPD no âmbito da segurança pública e persecução penal, em alusão ao art. 4º, § 3º, LGPD. Ainda, Danilo Doneda ressaltou que a ANPD já tem capacidade para fiscalizar e sancionar órgãos públicos independentes fora do âmbito da SP/PP.

Em relação às funções e competências da UPDP, Nefi Cordeiro destacou que ela deve: (i) ter competência para atuar em matérias de segurança pública e de persecução penal; (ii) ser independente dos órgãos públicos; (iii) estar protegida das intervenções do Executivo, inclusive durante o processo legislativo de criação do órgão; (iv) ser dotada de alta capacidade técnica. A independência foi uma característica também mencionada por Vladimir Aras, juntamente com a necessidade de se adotar padrões mínimos europeus de uma autoridade (art. 44 e ss., GDPR). Diferentemente, Renato Sérgio de Lima destacou que a UPDP deve estar alocada entre o CNMP e CNJ e que o Anteprojeto precisa conceituar segurança pública e revogar conceitos contrários presentes em outras normas.

Tendo isso em vista, o modelo ideal de autoridade para Nefi Cordeiro é aquele que conceda à autoridade as características mencionadas no item acima, sendo que a solução de vinculação ao CNJ é a melhor alternativa, apesar de não ser a ideal. Isso porque o CNJ de fato possui alto grau de autonomia e suas decisões têm sido aceitas por outros órgãos públicos independentes. Não obstante, haveria o problema mencionado acima relativo às competências do CNJ e outro relacionado à falta de

capacidade técnica do Conselho para as implementar no dia-a-dia da referida função, já que existiria um elevado número de demandas acerca do tema e, consequentemente, seria necessária a criação de vários cargos para suprir a demanda.

Nesse ponto, Vladimir Aras defende que a solução do CNJ não é a melhor, pois, para ele, o ideal seria alocar a autoridade abaixo do CNJ e do CNMP. Esse modelo seria capaz de compatibilizar a independência e a competência em matéria de proteção de dados no âmbito SP/PP e haveria maior controle legislativo da autoridade e um menor custo decisório. Ainda, defendeu que o risco da autoridade de não ter autonomia, accountability e independência quanto à forma de ingresso, é consideravelmente maior caso a UPDP não esteja sob a proteção dos Conselhos em questão. A única ressalva foi que nenhum dos dois conselhos têm como previsão constitucional a competência de exercer as tarefas de uma autoridade de proteção de dados.

Da mesma forma, Renato Sérgio de Lima defendeu a vinculação ao CNMP e ao CNJ, pois isso conferiria legitimidade para a UPDP atuar no âmbito da segurança pública e na seara da investigação e persecução penal, para garantir a proteção de dados no âmbito do processo penal. Assim, é contra a vinculação unicamente no CNJ, pois as decisões deste só vinculariam as instituições relacionadas à investigação e persecução penal (MP, Judiciário e polícias judiciárias) e o CNJ não tem a competência para o controle externo da atividade policial.

Danilo Doneda, por sua vez, argumentou que a solução de vincular a UPDP ao CNJ só se justifica por conta da debilidade institucional da ANPD, sendo que o ideal seria que existisse somente uma autoridade, de modo a evitar conflitos de, por exemplo, competência.

Por fim, Jacqueline de Souza Abreu defendeu que o arranjo ideal seria uma ANPD independente que não sofresse influência políticas, um órgão técnico que fizesse análises formais, e que teria competência nas matérias de SP/PP, existindo um departamento específico para cuidar disso. Em relação à escolha do CNJ, disse que foi a melhor solução que poderia ter sido feita no atual quadro legislativo. Ressaltou também que essa é uma solução provisória e que há um problema, pois o CNJ está mais próximo dos atos de juízes e da investigação criminal do que de atividades de segurança pública.

5. MODELOS ESTRANGEIROS

A existência de uma autoridade supervisora para o campo da proteção de dados não é uma pauta recente. O Conselho da Europa, em 1981 (Convenção de Estrasburgo[294]), já havia atrelado a proteção de dados aos deveres de fiscalização e regulamentação por meio de uma entidade com competências delimitadas e com sua independência resguardada[295]. Neste sentido, o ordenamento jurídico europeu sempre foi uma vanguarda no que tange aos direitos da pessoa humana. Logo, não é de se surpreender que a legislação europeia relativa à proteção de dados também tenha norteado a elaboração de normativas a respeito do tema em diversos países, incluindo o Brasil.

O Regulamento nº 2016/79 do Parlamento e Conselho Europeu, mundialmente conhecido como Regulamento Geral sobre a Proteção de Dados (ou GDPR, em inglês), é, sem dúvidas, o mais importante avanço no que diz respeito à consolidação da proteção de dados pessoais como direito dos cidadãos de todos os países pertencentes à União Europeia, com repercussões em todo o mundo.

Apesar disso, é importante compreender o histórico da cultura jurídica de proteção de dados em cada país previamente à GDPR, as particularidades com relação à transposição de tal normativa para os países europeus, bem como dos demais instrumentos normativos do Parlamento e Conselho, anteriores e subsequentes a este, para o ordenamento interno de cada Estado-membro. Para tanto, é também necessário compreender a modelagem institucional de cada país e como isso influencia as diferentes soluções de estruturas adotadas para o controle e proteção do tratamento de dados dos cidadãos.

Nesta chave, procuramos observar especificamente como se dá a fiscalização e aplicação de sanções pelas respectivas autoridades nacionais de proteção de dados, verificando se os problemas já demonstrados com relação à ANPD brasileira também foram verificados no estrangeiro durante a estruturação organizacional e funcional de tais autoridades. Para isto, serão objetos de análise as legislações relativas à proteção de dados e a estrutura das autoridades reguladoras de Itália, Portugal e Espanha, na Europa, e do Uruguai e Argentina, na América Latina.

294 UNIÃO EUROPEIA. Convenção 108 de 1981. Disponível em: <https://www.acnur.org/fileadmin/Documentos/portugues/BDL/Convencao_Europeia_sobre_a_Nacionalidade.pdf?view=1>. Acesso em: 21 maio 2021.

295 CASTRO, Maria Eugênia Bordinassi de. A estrutura e a natureza jurídica da Autoridade Nacional de Proteção de Dados com base na lei nº 13.853/2019. In: MAGRO, Américo Ribeiro; TEIXEIRA, Tarcísio (coords.). *Proteção de Dados - Fundamentos Jurídicos*. 1. ed. Salvador; JusPODIVM; 2019. p. 199 - 227.

5.1. EUROPA

5.1.1. GENERAL DATA PROTECTION REGULATION (GDPR)

O Regulamento (UE) 2016/679 é a normativa tomada como modelo por muitos sistemas jurídicos ao redor do mundo. Isso decorre do fato de que ela estabelece preceitos gerais que são de suma importância quando se trata de proteção de dados, seja o tratamento feito por entes privados ou públicos. Como será visto, a opinião da Comunidade Europeia, tomada a partir da adequação do ordenamento jurídico do país em relação à GDPR, é de grande influência e tem capacidade de resultar em reformas na legislação dos países que pretendem manter relações com a UE.

Dentre as diretrizes gerais estabelecidas pela Regulação em questão, encontram-se as características essenciais que deve ter uma autoridade supervisora, definida da seguinte maneira: "*'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51*"[296]. Em seguida, o referido artigo 51 estabelece que a(s) autoridade(s) será(ão) criada(s) por cada Estado-membro, resguardando-se sua independência.

A independência da autoridade supervisora, conforme o artigo 52 da GDPR, manifesta-se em três formas de autonomia: a) a financeira, prevista no item 6 do dispositivo, é atingida quando se separa o orçamento da autoridade de proteção de dados dos demais órgãos do governo, de forma a garantir a sua autonomia no desempenho de suas funções; b) a autonomia estrutural, que demanda que a autoridade tenha um corpo de funcionários exclusivos e submetidos tão somente ao órgão supervisor; e, c) a autonomia funcional (art. 52, item 3 e art. 53, item 4, GDPR), que consiste na estabilidade dos funcionários, no que tange à forma de ingresso, capacitação na matéria, mandato e exoneração[297].

Portanto, quando os três tipos de autonomia estão presentes em uma autoridade, esta possui independência suficiente para exercer suas funções da melhor maneira. Ademais, considerando que a GDPR é uma normativa exemplar e tomada como base em diversos ordenamentos jurídicos no mundo, os Estados não membros da UE tentam seguir os três fatores quando da elaboração das suas próprias autoridades de controle. Isso decorre do fato de que a opinião europeia sobre a qualidade da proteção de dados no país é de extrema relevância para o cenário global, fundamentando, pois, a possibilidade ou não da transferência de dados para certo país[298]. Sendo assim, será analisado a seguir o arranjo

296 Artigo 4 (21), GDPR.

297 A independência funcional é de extrema relevância para garantir o desempenho adequado das funções da autoridade supervisora, pois priva os funcionários de pressões externas, como as políticas, ou internas, como conflitos dentro do próprio órgão (ARANTES, Camila Rioja; BLUM, Renato Opice. Autoridades de Controle, Atribuições e Sanções. in: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.) *Comentários ao GDPR - Regulamento Geral de Proteção de Dados da União Europeia*. São Paulo: Revista dos Tribunais; 2018. p. 227-253).

298 Regulamento 679/2016. Artigo 45 (1): " Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma

institucional promovido por diversos países, sejam eles estados membros da Comunidade Europeia ou da América Latina, tendo por base os conceitos de autonomia financeira, estrutural e funcional supracitados dada a sua relevância para o cumprimento dos fins de uma autoridade supervisora.

organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.". Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 7 jun. 2021.

5.1.2. A DIRETIVA 2018/680

O Parlamento e Conselho Europeu expediram a Diretiva 2016/680, de extrema relevância para o presente trabalho, por tratar da "*proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados*".

Há, reconhecidamente, uma diferença entre o tratamento de dados para fins de segurança pública e aquele destinado a finalidades diversas, pois há dois fatores em jogo que se contrapõem diretamente. De um lado, tem-se que dados relativos à prevenção e à repressão de atividades criminosas são dados de extrema delicadeza, pois, quando se trata de persecução penal (*supra*, 4.3), os dados relativos a suspeitos, vítimas ou testemunhas podem, se vazados, interferir diretamente na vida dos indivíduos, em fatores importantes, como a segurança física, econômica, o convívio social do afetado e de seus familiares, etc.

Da mesma maneira, dados relativos à prevenção de crimes podem inclusive ser considerados maneiras de incriminar indivíduos de forma alternativa ao devido processo legal, aumentando o poder de vigilância do Estado sobre seus cidadãos, característica muito observada em regimes autoritários, supressores de liberdades. Assim, entende-se que esta modalidade de tratamento de dados tem uma possibilidade de ainda maior afetação de direitos fundamentais dos cidadãos do que qualquer outra categoria de dados.

Por outro lado, atividades de policiamento e persecução penal são de extrema importância para o funcionamento de uma sociedade regida pelo Estado Democrático de Direito, que também garante a todos certo nível de segurança. Dessa forma, o desafio do legislativo, dos países europeus e dos demais, é de garantir um tratamento de dados na segurança pública que, ao mesmo tempo, não exceda os limites colocados pelos direitos fundamentais do cidadãos e que garanta uma verdadeira efetividade no trabalho dos órgãos públicos competentes para a execução e aplicação da Lei[299].

299 COMISSÃO DE JURISTAS DA C MARA DOS DEPUTADOS. *Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal*. Disponível em <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf>. Acesso em: 29 maio 2021. p. 1.

Este é um desafio de alta complexidade, considerando que dificilmente haverá um dispositivo que consiga, perfeitamente, conciliar a proteção ao titular de dados contra abusos de autoridades e o acesso destas a serviços e plataformas que realmente contribuam para uma segurança pública efetiva[300]. Porém, o mais importante é haver algum tipo de legislação relativa a este tipo de tratamento de dados, pois, assim, ao menos há segurança jurídica conferida tanto às autoridades competentes quanto aos titulares dos dados.

A citada Diretiva 2016/680 certamente foi um passo importante rumo a este objetivo, proporcionando efeitos positivos similares aos Estados-membros que a transpuseram para seus ordenamentos em forma de Lei interna, como se verá a seguir a partir do exame do que sucedeu em Portugal e na Itália.

300 Idem.

5.1.3. PORTUGAL

Portugal tem um interessante histórico de reconhecimento da proteção de dados pessoais como Direito do cidadão. A primeira menção a esse Direito aparece na Constituição da República Portuguesa, de 1976, em seu texto original, no art. 35, no 1 e 2, que afirmam[301]:

> **1.** Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização.
>
> **2.** A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos **[...]**

Percebe-se que, já neste momento, havia uma preocupação do constituinte com a proteção de dados. Em 1981, teve lugar o próximo avanço na questão, não somente para Portugal, mas para toda a Europa, com a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro, conhecida como Convenção de Estrasburgo. Este é reconhecido como o primeiro documento juridicamente vinculativo com relação à garantia da liberdade individual e privacidade no que tange à nova era tecnológica de tratamento automatizado de dados[302].

Apesar de ser de extrema relevância o reconhecimento inicial, mesmo que com preceitos gerais relativos a direitos da personalidade (afirmados na Convenção), ou artigos constitucionais pouco específicos quanto à proteção de dados, a sua consolidação, aprofundamento e verdadeiro reconhecimento no ordenamento jurídico português veio em 1991, com a Lei 10/91, de 29 de abril, conhecida como "Lei da Proteção de Dados Pessoais face à Informática". Esta marcou o que seria compreendida como

301 PORTUGAL. Constituição da República Portuguesa, de 1976. Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Acesso em: 31 maio 2021.

302 MARZOCCHI, Ottavio. *Fichas técnicas sobre a União Europeia - 2021*: Proteção de Dados. Disponível em: <https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf>. Acesso em: 31 maio 2021.

a "primeira geração" legislativa, portuguesa, com relação à proteção de dados pessoais[303] [304].

A "segunda geração" legislativa sobre proteção de dados foi marcada pela Diretiva 95/46/CE, do Parlamento Europeu e Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados. Esta Diretiva foi transposta para o Direito Português na forma da Lei 67/98, denominada "Lei da Proteção de Dados Pessoais". Nesse momento, medidas importantes foram tomadas, no sentido de reconhecer um desequilíbrio na relação entre a pessoa e entidades que coletam e processam dados e fortalecendo sua posição relativa face a estas[305].

Mas o que realmente merece atenção é a previsão do art. 28[306], do capítulo VI da Diretiva 95/46, que instituiu, pela primeira vez, a obrigação de instituição, pelos Estados-membros, de uma autoridade de controle e fiscalização da aplicação das normas relativas à proteção de dados pessoais[307].

A transposição desse dispositivo resultou no art. 21, Lei 67/68, que efetivamente instituiu a Comissão Nacional de Proteção de Dados, como uma "entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República"[308]. A análise do art 8o da Lei em questão se mostra de extrema relevância para o foco central do presente trabalho, na medida que dispõe sobre o tratamento de dados pessoais relacionados à segurança pública e atividade policial, assim dispondo:

303 MASSENO, Manuel David. A Proteção de Dados Pessoais em Portugal e nos Outros Países de Língua Portuguesa, uma cartografia das Fontes Legislativas. Disponível em: http://direitoeti.com.br/artigos/a-protecao-de-dados-pessoais-em-portugal-e-nos-outros-paises-de-lingua-portuguesa-uma-cartografia-das-fontes-legislativas/. Acesso em: 31 maio 2021.

304 Cabe, aqui, um esclarecimento quanto ao modelo normativo da União Europeia: os regulamentos se diferenciam de diretivas, na medida que o primeiro é diretamente aplicável aos países e imediatamente vinculante, como se fosse parte do Direito nacional. Enquanto isso, as diretivas representam objetivos a serem atingidos pelos Estados-membros, cabendo a eles decidir os meios legislativos pelos quais realizarão tais objetivos, respeitando os preceitos basilares das diretivas#. Dessa forma, o Conselho Europeu estabelece um prazo para que os países respeitem as Diretivas e a transponham para o Direito interno. Quanto aos regulamentos, não há proibição de uma lei no direito interno que os complemente, porém, conforme afirmado, já são documentos juridicamente vinculantes desde o início de sua vigência.

305 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 212. apud BEZERRA, Maria Ruth Borges. *Autoridade Nacional De Proteção De Dados Pessoais: A Importância Do Modelo Institucional Independente Para A Efetividade Da Lei* in Revista Caderno Virtual, v. 2, n. 44. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3828>. Acesso em: 17 maio 2021. p. 10.

306 "1. Cada Estado-membro estabelecerá que uma ou mais autoridades públicas serão responsáveis pela fiscalização da aplicação no seu território das disposições adoptadas pelos Estados-membros nos termos da presente directiva. Essas autoridades exercerão com total independência as funções que lhes forem atribuídas. [...]".

307 UNIÃO EUROPEIA. *Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:31995L0046>. Acesso em: 31 maio 2021.

308 PORTUGAL. Lei nº 67, de 26 de outubro de 1998. Lei da Protecção de Dados Pessoais que transpõe para a ordem jurídica portuguesa a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados. Disponível em: <https://dre.pt/pesquisa/-/search/239857/details/maximized#:~:text=Qualquer%20pessoa%20que%2C%20agindo%20sob,por%20for%C3%A7a%20de%20obriga%C3%A7%C3%B5es%20legais>. Acesso em: 31 maio 2021.

> **1.** A criação e a manutenção de registos centrais relativos a pessoas suspeitas de actividades ilícitas, infracções penais, contra-ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias só podem ser mantidas por serviços públicos com competência específica prevista na respectiva lei de organização e funcionamento, observando normas procedimentais e de protecção de dados previstas em diploma legal, com prévio parecer da CNPD.
>
> **2.** O tratamento de dados pessoais relativos a suspeitas de actividades ilícitas, infracções penais, contra-ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias pode ser autorizado pela CNPD, observadas as normas de protecção de dados e de segurança da informação, quando tal tratamento for necessário à execução de finalidades legítimas do seu responsável, desde que não prevaleçam os direitos, liberdades e garantias do titular dos dados.
>
> **3.** O tratamento de dados pessoais para fins de investigação policial deve limitar-se ao necessário para a prevenção de um perigo concreto ou repressão de uma infracção determinada, para o exercício de competências previstas no respectivo estatuto orgânico ou noutra disposição legal e ainda nos termos de acordo ou convenção internacional de que Portugal seja parte.

A Lei também atribuiu, além do poder fiscalizatório, de fazer cessar tratamento indevido de dados na esfera da investigação e suspeita de atividades ilícitas, poderes sancionatórios ("deliberar sobre a aplicação de coimas", art. 23, no 1, "n"), inclusive mais danosos ao infrator no caso de descumprimento do estipulado no art 8o, conforme se observa da leitura do art. 38, no 2 e 43, no 2, que dobram as penas para estes casos. Após a presente análise, resta claro que Portugal, em 1998, já havia consolidado na legislação princípios do atual Regulamento Geral de Proteção de Dados, tais como os princípios da limitação da finalidade e *accountability*[309].

309 UNIÃO EUROPEIA. *Diretiva 2016/679 (General Data Protection Regulation - GDPR)*: artigo 5. Disponível em: <https://gdpr.algolia.com/pt/gdpr-article-5>. Acesso em: 31 maio 2021.

Seguindo o percurso histórico, importa ressaltar a promulgação da Lei 43/2004, conhecida como "Lei de organização e funcionamento da Comissão Nacional de Protecção de Dados". A Lei novamente reforça a ideia de total independência administrativa da Comissão e suas disposições confirmam essa afirmação. A forma de nomeação e de retirada dos membros diz muito sobre autonomia de uma entidade pública, na medida que, se os membros tiverem estabilidade em seus cargos, estão menos sujeitos a arbitrariedades e pressões políticas, gozando, assim, inclusive, de maior autonomia decisória[310]. Isto se verifica na Lei 43/2004, especialmente nos arts. 5o, da "Inamovibilidade", 7o, da "Perda do Mandato" e 10o das "Garantias". Estes dispositivos revelam que os membros da CNPD somente serão retirados do cargo por ineficiência, impedimento ou descumprimento de obrigações legais, jamais, contudo, por influências externas. É interessante apontar o nível de completude dessa Lei, evidenciado pelo fato de que ela está vigente até hoje, com modificações pequenas e pontuais[311], mesmo com as diversas alterações legislativas que vieram a ter lugar na década seguinte[312].

Por fim, chega-se à "terceira geração" legislativa relativa à proteção de dados em Portugal, com o advento da GDPR. Como dito, o Regulamento é vinculante mesmo sem transposição para o direito interno. No entanto, muitos países redigem as disposições do regulamento, em forma de Lei nacional, para assegurar sua execução na ordem interna. Foi o caso de Portugal, que, com a Lei 58/2019, reforçou os preceitos centrais da GDPR.

Uma disposição interessante, do art. 2o, no 1, afirma que a Lei se aplicará ao tratamento de dados realizado no território nacional, independentemente da natureza pública ou privada do ente controlador. Essa disposição já esclarece a natureza vinculante da atuação da autoridade controladora, de modo a garantir, de fato, sua efetividade e independência, inclusive frente a órgãos públicos que tratam dados e estão, por consequência, sujeitos a fiscalização[313].

Concomitantemente, o Parlamento e Conselho Europeu expediram a já mencionada Diretiva 2016/680, transposta para o ordenamento português pela Lei 59/2019, trazendo uma série de disposições cruciais sobre o tratamento de dados para fins de segurança pública.

310 BEZERRA, Maria Ruth Borges. *Autoridade Nacional De Proteção De Dados Pessoais: A Importância Do Modelo Institucional Independente Para A Efetividade Da Lei* in Revista Caderno Virtual, v. 2, n. 44. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3828>. Acesso em: 17 maio 2021. p. 33.

311 PORTUGAL. Lei n.º 43, de 2004. *Lei de organização e funcionamento da Comissão Nacional de Protecção de Dados*. Disponível em: <https://dre.pt/web/guest/legislacao-consolidada/-/lc/122101697/diploma?_LegislacaoConsolidada_WAR_drefrontofficeportlet_rp=diploma&filter=Filtrar>. Acesso em: 31 maio 2021.

312 Ainda nesta década, cabe, contudo, menção a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, transposta para o ordenamento português pela Lei 41/2004.

313 BEZERRA, Maria Ruth Borges. *Autoridade Nacional De Proteção De Dados Pessoais: A Importância Do Modelo Institucional Independente Para A Efetividade Da Lei* in Revista Caderno Virtual, v. 2, n. 44. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3828>. Acesso em: 17 maio 2021. p. 28.

Dada a importância justificada do controle do tratamento de dados nesta esfera, a Lei traz, notadamente nos arts. 14o ("Informações a disponibilizar ou a fornecer pelo responsável pelo tratamento"), 15o ("Direito de acesso do titular dos dados aos seus dados pessoais") e 18o ("Exercício dos direitos do titular dos dados e verificação pela autoridade de controlo"), disposições que atribuem, ao titular de dados, maiores direitos face aos responsáveis pelo tratamento destes, bem como reforça, concretamente, princípios como o da finalidade e adequação no tratamento.

Contudo, há de se atentar para alguns fatores desta Lei, tal como as disposições do art. 17o ("Limitações do direito de acesso") que se repetem em outros artigos, que atribuem um certo nível de discricionariedade ao responsável pelo tratamento de dados[314]:

> **1.** O responsável pelo tratamento pode recusar ou restringir o direito de acesso do titular dos dados enquanto tal limitação constituir uma medida necessária e proporcional para
>
> **a)** Evitar prejuízo para investigações, inquéritos ou processos judiciais;
> **b)** Evitar prejuízo para a prevenção, deteção, investigação ou repressão de infrações penais ou para a execução de sanções penais;
> **c)** Proteger a segurança pública; **[...]**

Há outro ponto essencial, sobre o qual é necessário se discorrer: a previsão do art. 43, no 2, Lei 59/2019, que afirma que a competência da CNPD de garantir e fiscalizar o cumprimento da Lei "*não se aplica ao tratamento de dados pessoais efetuado pelos tribunais e pelo Ministério Público no exercício das suas competências processuais*". Isso esclarece que a Lei decidiu retirar do âmbito de sua aplicação a atividade jurisdicional. Isso não significa, contudo, que tais atividades escapem de qualquer regulação, pois, além das garantias constantes da Lei processual, tal previsão não exclui a aplicação das demais

314 Quanto a isto, questiona-se se não seria de extrema conveniência, para o responsável, alegar, quase em todas as ocasiões, que não é possível o exercício do direito de acesso aos dados, por parte do titular, por "prejudicar as investigações". Disso coloca-se um outro ponto, já apresentado no presente trabalho, de que o tratamento de dados para fins de segurança pública é de extrema relevância para a efetividade da atividade policial e da atuação do Ministério Público e Tribunais, por isso, em tese, não pode sofrer limitações que talvez inviabilizem suas atividades. Contudo, isso não significa que este tratamento possa ser realizado sem respeito pelos direitos fundamentais dos cidadãos, positivados no ordenamento pelas Leis relativas à proteção de dados. Por isso o tema é de tamanha complexidade.

disposições relativas ao tratamento de dados, pelas mesmas entidades, para fins diversos dos relacionados à competência processual.

Verifica-se, assim, que Portugal tem um robusto histórico legislativo relativo à proteção de dados, bem como leis atuais vigentes[315] quanto à proteção geral de dados e a proteção especificamente relacionadas ao tratamento de dados na esfera da segurança pública e persecução penal. Isto garante segurança jurídica às autoridades públicas que tratam dados pessoais, à CNPD, que exerce o controle sobre todos os tipos de tratamento, e ao titular dos dados, que tem seus direitos positivados e tutelados em Lei, mesmo no caso de estarem sujeitos à investigação policial e à persecução penal.

315 Destaque para a não citada Lei 41/2004, que transpôs para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas.

5.1.4. ITÁLIA

A Itália é também um país cuja história legal revela uma preocupação com a fiscalização do tratamento dos dados pessoais de seus cidadãos. Seu arranjo normativo está vinculado ao regime jurídico de proteção de dados europeu, de modo que as disposições sobre as quais se discorreu na seção anterior também serviram como base para o desenvolvimento das leis relativas ao tratamento de dados no ordenamento italiano.

O regime jurídico de proteção de dados, de qualquer que seja o país, evolui conforme o avanço das tecnologias de informatização e automatização do tratamento dos dados, sendo necessária constante adaptação das leis à realidade[316]. O legislador italiano percebeu este fenômeno, como se observa pela Lei 675/96, aprovada no dia 31 de dezembro de 1996, que transpôs, para o ordenamento italiano, a citada Diretiva 95/46/CE do Parlamento e Conselho Europeu.

Com a promulgação desta Lei, foi instituído um sistema de autorizações e responsabilidades para os responsáveis pelo tratamento de dados pessoais, bem como direitos aos titulares, princípios norteadores do tratamento e, finalmente, um órgão responsável pela fiscalização e aplicação da lei, a Autoridade Garante para a proteção de dados pessoais[317]. Em seguida, literalmente no mesmo dia, foi aprovada a Lei 676/96, que delegava ao Executivo a função de legislar sobre diretrizes para o aditamento e correção da Lei 675/96. Isto revela justamente a supracitada preocupação com o paradoxo de se estabelecer parâmetros fixos para a regulação de um âmbito em constante transformação tecnológica.

De fato, o Executivo introduziu diversas modificações direcionadas à integração da Lei 675/96 por meio de dois decretos presidenciais e nove decretos legislativos[318] que passaram a compor, à época, todo o arranjo normativo relativo à proteção de dados na Itália. Em seguida, o Parlamento aprovou a Lei Delegada n. 127, de 24 de março, com o objetivo de estipular um prazo final para que o próprio Poder Executivo reunisse todas as leis esparsas, que compunham este arranjo normativo, em um único documento, efetuando as modificações e inovações cabíveis[319].

Assim o fez. O resultado deste esforço foi a promulgação do Decreto Legislativo 196, de 30 de junho de 2003, denominado Código em Matéria de Proteção de Dados. O Código reforçou os princípios basilares do justo tratamento de dados, tais como a transparência (informação ao titular

316 DONEDA, Danilo. Um Código para a Proteção de Dados Pessoais na Itália. *Revista Trimestral de Direito Civil*, Rio de Janeiro, v. 16, p. 78-99, 2003. p. 79.

317 Ibidem, p. 5.

318 Idem.

319 Ibidem, p. 6.

quanto ao tratamento de seus dados), finalidade (adequação do tratamento ao fim proposto), limitação da conservação (de forma que os dados não sejam armazenados por mais tempo que o necessário para o fim especificado) e exatidão (que o titular dos dados tenha acesso e possa retificar ou apagar informações inexatas que lhe digam respeito).

O Código também reiterou, na sua terceira e final parte[320], as disposições da Lei 675/96 que tratavam da Autoridade Garante, reafirmando sua total independência decisória e funcional, verificada, dentre outros fatores, pela estrutura de eleição de seus quatro membros, marcada pela imposição de mandatos de sete anos, sem possibilidade de reeleição, e pela eleição de dois membros pela Câmara dos Deputados e dois pelo Senado da República, selecionados dentre pessoas com capacitação técnica e reconhecida competência em matéria de direito ou tecnologia da informação[321].

Dentre suas principais funções, estão as de (i) adotar as medidas previstas na legislação quanto à proteção de dados pessoais, tais como denunciar os fatos que possam ser considerados infracções passíveis de ação penal e proibir, no todo ou em parte, o tratamento de dados ou bloqueá-lo se o tratamento for ilegal ou incorreto; (ii) informar o Parlamento e outros organismos e instituições sobre a necessidade de se adotar atos normativos e administrativos relativos à proteção de dados pessoais, conforme previsão do art. 31, nº 1, "m", Lei 675/96 e; (iii) participar de discussões sobre iniciativas legislativas em audiências no Parlamento, bem como particpar da elaboração e assinar códigos deontológicos de diferentes setores, no que tange aos respectivos tratamentos de dados por eles realizados[322].

Como se sabe, a Diretiva 95/46, que deu origem à Lei 675/96 e às normas subsequentes que a complementaram, foi revogada, pelo Parlamento e Conselho Europeu, pelo Regulamento Geral de Proteção de Dados (Regulamento 2016/679). Por consequência, adveio o Decreto Legislativo no 101, de 2018, que adaptou o Código em Matéria de Proteção de Dados (de 2003) para conformá-lo às disposições do Regulamento. Nota-se que o Decreto especificou ainda mais os princípios e dispositivos já contidos no Código, facilitando sua aplicabilidade nos casos concretos para os diferentes setores que lidam com o tratamento de dados pessoais e, assim, aumentou o nível de segurança jurídica para os atores envolvidos em tais operações.

Com relação às atribuições e competências da Autoridade Garante, não houve mudanças significativas. Foi mantida como uma autoridade administrativa independente, de caráter para-jurisdicional, com poder sancionatório, que tem a função de proteger os direitos e liberdades fundamentais dos indivíduos no que diz respeito ao tratamento de dados pessoais e facilitar o livre fluxo de dados

320 Ibidem, p. 8.

321 BEZERRA, op. cit., p. 38.

322 Idem.

dentro da União Europeia. O fato de ser para-jurisdicional significa que há a possibilidade de recurso, no caso da aplicação de sanções pecuniárias ou de interferência no tratamento indevido de dados, à própria autoridade, podendo-se naturalmente preferir o judiciário[323].

Já as disposições da Diretiva 2016/680 foram transpostas para o Direito italiano na forma do Decreto Legislativo no 51, de 2018. Nele, interessam especialmente os Capítulos V ("Proteção e sanções administrativas") e VII ("Disposições Suplementares sobre o Tratamento das Forças Policiais")[324].

Apesar das disposições principiológicas importantes do Capítulo I, art. 3, que asseguram e estendem os princípios da finalidade e adequação do tratamento de dados à autoridades públicas responsáveis pelo policiamento, merece atenção a disposição do art. 37, no 6, que afirma que o Decreto não se aplica para tratamento de dados realizados no âmbito das competências judiciais dos Tribunais e Ministério Público. Além disso, o art. 14, no 1, aponta que:

> Os direitos a que se referem os artigos 10.º, 11.º e 12.º, relativos aos dados pessoais contidos em decisão judicial, em títulos ou documentos sujeitos a tratamento no decurso da investigação ou das investigações, no registro criminal ou em processo sujeito a tramitação no decurso do processo penal ou na fase de execução penal, são exercidas de acordo com as disposições da lei ou dos regulamentos que regem esses atos e procedimentos. Qualquer pessoa interessada nisso, durante o processo penal ou após a sua definição, pode requerer, com as modalidades a que se refere o artigo 116.º do código de processo penal, a retificação, o cancelamento ou a limitação dos dados pessoais que lhe digam respeito. O juiz dispõe sobre os formulários do artigo 130 do Código de Processo Penal[325].

323 DONEDA. op. cit, p.14.

324 Versão traduzida do Decreto Legislativo 51. Disponível em <https://www.gazzettaufficiale.it/atto/vediMenuHTML?atto.dataPubblicazioneGazzetta=2018-05-24&atto.codiceRedazionale=18G00080&tipoSerie=serie_generale&tipoVigenza=originario>.

325 Idem.

Disso depreende-se que a Lei, de fato, não se aplica para a persecução penal, ao menos quando os dados são utilizados para finalidades exclusivamente processuais. Mesmo assim, observa-se que há uma extrema preocupação, ao mesmo tempo, com o abuso no processamento de dados pelas autoridades públicas responsáveis pela segurança e com o não engessamento das atividades policiais e judiciárias, assegurado pelas "Limitações ao exercício dos direitos do interessado", presentes no referido art. 14.

Mesmo com as ditas limitações, percebe-se uma consolidação, concretização e formalização das disposições relativas ao tratamento de dados para fins de segurança pública. Isto, conforme já discorrido, é essencial para que os cidadãos possuam maior controle sobre seus dados e noção de seus direitos perante os operadores de dados, bem como para que a Autoridade Garante tenha segurança jurídica para agir autonomamente, dentro de suas competências legais, para fiscalizar e garantir o cumprimento do arranjo normativo italiano relativo ao controle do tratamento de dados pessoais, seja este realizado por entidades públicas ou privadas.

5.1.5. ESPANHA

Recentemente, o Governo espanhol, mediante proposta de sua autoridade nacional de proteção de dados, aprovou o Real Decreto 389/2021, de 1o de junho, que instituiu o Estatuto da Agência Espanhola de Proteção de Dados. Entretanto, o arranjo normativo relativo à proteção de dados já havia sido transformado e consolidado no ordenamento espanhol ao longo do tempo, acompanhando a evolução do regime jurídico Europeu.

A Constituição Espanhola de 1978 já previa, no art. 18.4, que o legislativo deve limitar o uso da informática para proteger os Direitos Fundamentais do cidadão[326]. O advento da Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, conhecida como Convenção de Estrasburgo, trouxe a discussão específica sobre o tratamento de dados à tona, tendo o documento sido ratificado pelo Governo espanhol em 1984, com entrada em vigor no ano seguinte.

Sete anos depois, em 1992, o parlamento espanhol aprovou a "*Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos Personales*" (LORTAD), em conformidade com o prazo estabelecido pela Convenção para que os países incluíssem no ordenamento interno uma legislação referente ao tratamento de dados. A LORTAD foi a primeira Lei a instituir, no Título VI, art. 34, a Agência Espanhola de Proteção de Dados[327], bem como suas atribuições e arranjo organizacional. Nela, a Agência foi descrita como um ente do Direito Público, com personalidade jurídica própria, capacidade de atuação nos âmbitos público e privado e que atua com plena independência da Administração Pública no exercício de suas funções.

Quanto às funções da AEPD, tem-se como principal a de fiscalizar o cumprimento da LORTAD, especialmente no que tange à realização dos direitos de acesso, retificação e cancelamento dos dados dos cidadãos cujos dados sejam objeto de tratamento automatizado. É interessante ressaltar que à Agência também foram atribuídos poderes sancionatórios, conforme dispõe o art. 36, alínea "g", LORTAD. As sanções encontram-se listadas no Título VII da Lei e variam de acordo com a gravidade das infrações, de leves a muito graves.

Importa, igualmente, a análise do art. 45, que estabelece, para as infrações cometidas pelo Poder Público, um regime sancionatório diferente do estipulado para infrações cometidas por entes privados. Impõe que, no caso das referidas violações, o Diretor da Agência deve emitir uma resolução

326 AGENCIA ESPAÑOLA PROTECCIÓN DADOS. *Historia*. Disponível em: <https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/historia>. Acesso em: 07 jun. 2021.

327 ESPANHA. Lei Orgânica 5/1992, de 29 de outubro. Regulamenta o tratamento automatizado de dados pessoais. Disponível em: <https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189>. Acesso em: 07 jun. 2021.

que estabeleça as medidas a serem adotadas para que cessem ou sejam corrigidas tais infrações. O Diretor também pode requerer o início de processo disciplinar contra membros da administração que julgar responsáveis pelas violações da LORTAD e, nesse caso, as disposições procedimentais e sancionatórias serão as especificadas no Real Decreto 33/1986, chamado de "Regulamento do Regime Disciplinar dos funcionários da administração do Estado".

Com relação à independência funcional, tem-se que a Agência é estruturada por um Conselho Consultivo, composto por nove membros, sendo o Diretor escolhido, dentre eles, pelo governo, mediante Real Decreto. O conselho é formado da seguinte maneira: um deputado, proposto pelo Congresso dos Deputados, um senador, proposto pela Câmara correspondente, um representante da Administração Central, nomeado pelo Governo, um representante da Administração Local, proposto pela Federação Espanhola de Municípios e Províncias, um membro da *Royal Academy of History*, proposto por ela própria, um especialista na área, proposto pelo Conselho Superior de Universidades, um representante dos usuários e consumidores, selecionado a partir do que seja previsto no regulamento, um representante das Comunidades Autônomas, cuja proposta será feita através do procedimento estabelecido nas disposições da Lei e um representante do setor de arquivos privados.

Com relação à independência orçamentária, tem-se que o orçamento é definido e aprovado anualmente pela própria Agência para o exercício de suas funções (segundo a LORTAD, de 1992), devendo então ser enviado ao governo para que componha, "com a devida independência"[328], o Orçamento Geral do Estado.

Por fim, cumpre destacar a disposição adicional primeira, de nome "*Exclusão de aplicação dos Títulos VI e VII*", que justamente exclui o exercício do poder da Agência Espanhola de Proteção de Dados de fiscalização da LORTAD e aplicação de sanções quando se tratar de ficheiros automatizados de dados pertencentes às Cortes Gerais (Parlamento espanhol), ao Defensor do Povo (uma espécie de Procuradoria Geral da República, com estrutura diversa), ao Tribunal de Contas, ao Conselho Geral do Poder Judicial (equivalente ao CNJ) e ao Tribunal Constitucional (equivalente ao Supremo Tribunal Federal). As disposições da LORTAD foram então concretizadas no Real Decreto 428/1993, que criou o primeiro Estatuto da Agência Espanhola de Proteção de Dados.

Como já foi dito, em 1995, foi expedida a Diretiva 46/95/CE, do Parlamento e Conselho Europeu, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. A Diretiva foi transposta para o Direito Espanhol pela Lei Orgânica 15/1999, que adaptou suas disposições de forma a cumprir com os já citados princípios gerais da proteção de dados, dentre os quais ganham destaque os da finalidade, exatidão e transparência no

328 Idem.

tratamento de dados pessoais. Nesta Lei, chama atenção o art. 22, nos 1 e 2, que discorrem sobre o tratamento de dados em ficheiros de corpos policiais e responsáveis pela segurança pública:

> **1.** Os arquivos criados pelas Forças e "Corpos de Segurança" que contém dados pessoais que, por terem sido coletados para fins administrativos, devem estar sujeitos a registro permanente, eles estarão sujeitos ao regime geral desta Lei.
>
> **2.** Coleta e tratamento para fins policiais de dados pessoais pelas Forças e "Corpos de Segurança" sem o consentimento das pessoas afetadas é limitada a essas suposições e categorias de dados que são necessários para a prevenção de um perigo real para a segurança pública ou para a repressão de ofensas criminais, e deve ser armazenado em arquivos específicos estabelecidos para esse fim, que devem ser classificados por categorias de acordo com seu grau de confiabilidade **[...]**

Com o advento da GDPR e da Diretiva 2016/680, do Parlamento e Conselho Europeu, os Estados-membros se viram obrigados a transpor para seus respectivos ordenamentos as disposições nelas contidas. Como dito, a GDPR, tendo a natureza jurídica de Regulamento da União Europeia, já possui natureza vinculante, de modo que as leis nacionais que a transponham apenas servem como adaptações e especificações da mesma. Foi o que fez a Espanha ao editar a Lei Orgânica 3/2018, de 5 de dezembro, relativa à proteção dos dados pessoais e à garantia dos direitos digitais.

Por outro lado, a Diretiva 2016/680, justamente por se qualificar juridicamente como Diretiva da União Europeia, não possui, de imediato, natureza vinculante, sendo necessária, para que tenha vigência nos países, sua transposição para o Direito interno, em forma de Lei. A Espanha pecou em não realizar tal transposição, até o término do prazo final estabelecido pela Diretiva, qual seja, dia 6 de maio de 2018. Como resultado, o Tribunal de Justiça da União Europeia condenou o país ao pagamento de multa de quinze milhões de euros[329].

329 INTERNETLAB. *O Tribunal Europeu impõe multa à Espanha por descumprimento à Diretiva de proteção de dados para investigações criminais*. Disponível em: <https://www.internetlab.org.br/pt/itens-semanario/uniao-europeia-tribunal-europeu-impoe-multa-a-espanha-por-descumprimento-a-diretiva-de-protecao-de-dados-para-investigacoes-criminais/>. Acesso em: 07 jun. 2021.

A Lei Orgânica 3/2018 afirma, na disposição transitória quarta, que os tratamentos submetidos à Diretiva 2016/680 estariam ainda sob tutela da Lei 15/1999, especialmente do referido art. 22, enquanto não fosse transposta ao ordenamento espanhol a Diretiva. Foi então que, após imposta sanção, o Parlamento espanhol editou a Lei Orgânica 7/2021, de 26 de maio, relativa à proteção de dados pessoais tratados para fins de prevenção, detecção, investigação, ajuizamento de ações penais e execução de sanções penais, finalmente tendo realizado a transposição.

E, por fim, como destacado no início deste tópico, o Real Decreto 389/2021, de 1o de junho, que revogou o Real Decreto 428/1993 e reuniu as disposições presentes na GDPR, na Lei Orgânica 3/2018 e na Lei Orgânica 7/2021 para criar o novo Estatuto da Agência Espanhola de Proteção de Dados. Com isso, segue-se à análise do quadro normativo atual relativo à proteção de dados pessoais na Espanha, que trouxe algumas mudanças com relação ao arranjo anterior.

A Agência Espanhola de Proteção de dados é tida como uma Autoridade administrativa independente de âmbito estatal, dotada de personalidade jurídica própria, plena capacidade de investigação e de atuação nos âmbitos público e privado, com poderes corretivos e sancionadores, que atua com plena independência do Poder Público no exercício de suas funções e se relaciona com o Governo através de sua vinculação ao Ministério da Justiça. Segundo o art. 4 do Estatuto, seus membros não podem aceitar nem solicitar instruções de nenhuma entidade pública ou privada.

Não há mais um Diretor da Agência, mas sim um Presidente, auxiliado por um adjunto. Ambos serão nomeados pelo Governo, mediante proposta do Ministério da Justiça, entre pessoas de competência profissional reconhecida, em especial no domínio da proteção de dados. A nomeação se dá da seguinte forma: após avaliação do mérito, capacidade, competência e idoneidade dos candidatos, o Governo envia ao Congresso dos Deputados proposta para a Presidência e Adjunto, acompanhado de relatório de apoio que, após realização da audiência obrigatória dos candidatos, deve ser ratificado pela Comissão de Justiça (do Parlamento) em votação pública, com maioria de três quintos de seus membros no primeiro voto ou, se isso não for alcançado, por maioria absoluta em uma segunda votação, que ocorrerá imediatamente após a primeira. Neste último caso, os votos favoráveis devem vir dos Deputados pertencentes a pelo menos dois grupos parlamentares distintos[330].

330 ESPANHA. Lei Orgânica 3/2018, de 5 de dezembro. Da proteção de dados pessoais e garantia dos direitos digitais. Disponível em: <https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>. Acesso em: 07 jun. 2021.

O Presidente deve exercer sua competência com absoluta exclusividade e autonomia, e os mandatos da Presidência e do Adjunto têm duração de cinco anos, com a possibilidade de serem renovados por outro período de igual duração. Seus mandatos somente cessarão antes da duração prevista, nos casos renúncia ou consenso do Conselho de Ministros, nas hipóteses de (i) violação grave de suas obrigações, (ii) incapacidade superveniente para o exercício de sua função, (iii) incompatibilidade, ou (iv) condenação final por crime doloso.

A eleição do Conselho Consultivo da Agência Espanhola de Proteção de Dados segue em parâmetros similares às disposições da antiga LORTAD, com a diferença do aumento no número de membros e consequente participação de um maior número de entidades, públicas e privadas, na nomeação, conforme dita o art. 49, Lei Orgânica 3/2018 (o Estatuto faz reiteradas referências a esta Lei para explicar a organização da Agência).

Quanto à independência orçamentária, há uma mudança relevante para o antigo arranjo normativo dado pela Lei 15/1999. Atualmente, segundo o art. 44 do Estatuto, o orçamento deve ser feito nos moldes ditados pelo Ministério da Fazenda, não mais depende da exclusiva elaboração e aprovação pela própria Agência.

Finalmente, quanto ao tratamento de dados para fins de persecução penal e segurança pública, não há disposições próprias no Estatuto. Contudo, este afirma, em seu preâmbulo, que a Agência Espanhola de Proteção de Dados também fiscaliza o cumprimento da Lei Orgânica 7/2021. Esta, por sua vez, traz uma perspectiva do que é ou não permitido na seara do tratamento de dados para a finalidade de segurança pública. O art. 19, por exemplo, lista o que são consideradas infrações disciplinares muito graves, por parte das Forças e "Corpos de Segurança", sendo elas a divulgação de imagens e áudios de segurança para entidades não autorizadas e a utilização de tecnologias de tratamento de dados para fins diversos dos acobertados pela sua competência legal.

O art. 24 estabelece limitações ao direito de acesso do titular a seus dados pessoais, de forma similar à observada em Portugal e Itália, ou seja, quando o acesso aos dados resulte, de alguma forma, no impedimento de investigações ou na obstrução de procedimentos judiciais e quando a limitação ao acesso evite danos à prevenção, detecção, investigação de infrações penais e execução de sanções penais. Da mesma forma, o art. 26 estabelece que o exercício dos direitos de acesso, retificação, supressão ou limitação do tratamento de dados, quando relacionados ao processo penal, deverá ocorrer em conformidade com as normas processuais penais.

Por fim, a disposição adicional quarta estabelece que as autoridades competentes podem, sem o consentimento do interessado (titular dos dados), tratar dados pessoais, como documentos de identidade, nomes, sobrenomes, endereços, sexo e datas de nascimento que constam no registro municipal de habitantes e no censo eleitoral correspondente, com a imposição de que tal tratamento seja, novamente, para fins exclusivos de prevenção, detecção, investigação de infrações penais e execução de sanções penais.

Percebe-se que há margem para discricionariedade no tratamento de dados para fins de SP/PP, porém, chega-se aqui a uma conclusão similar à obtida na análise dos demais países da União Europeia: o importante é que exista uma legislação referente a este tipo de tratamento, que, no mínimo, respeite os preceitos gerais presentes na GDPR, pois, dessa forma, é possível que o país obtenha, ao mesmo tempo, segurança jurídica interna e uma posição de confiabilidade com relação à circulação de dados provenientes de outros países.

5.2. AMÉRICA LATINA

5.2.1. ARGENTINA

A Argentina foi o primeiro país da América Latina a sancionar uma lei de proteção de dados, a Lei 25.326/2000[331], que teve especial influência da Diretiva 96/45/CE[332] e da legislação espanhola. Porém, em menos de um ano as disposições referentes à autoridade supervisora foram revogadas pelo Decreto 995/2000[333], pois implicaria em um aumento das despesas públicas e violaria pressuposto de iniciativa do Executivo já que se tratava de uma entidade da Administração Pública indireta.

Em 2001, o Presidente Fernando de la Rúa, por meio do Decreto 1.558/2001[334], instituiu a *Dirección Nacional de Protección de Datos Personales*, alterando o art. 29 da Lei 25.326/2000. A normativa estabelece que a autoridade fazia parte da administração direta e se vinculava ao *Ministerio de Justicia y Derechos Humanos de la Nación*. Ainda, o dispositivo supracitado determinou que a autoridade seria administrada por um diretor escolhido pelo Poder Executivo e aceito pelo Senado, com mandato de quatro anos.

À vista disso, tem-se uma autoridade que carece de independência financeira e estrutural, tendo em vista que está subordinada ao Poder Executivo, que determinará o orçamento e nomeará o diretor da entidade. Diante disso, Delgado e Saltor (2020) afirmam que a falta de autonomia e independência da autoridade de controle argentina relaciona-se diretamente a sua vinculação com o órgão Executivo, que resulta na perda de eficácia das funções da entidade[335].

O mesmo entendimento foi expressado pela Comissão da Comunidade Europeia, conforme a decisão 2003/490/CE[336]:

331 ARGENTINA. Ley nº 25.326, de 02 de novembro de 2000. Disponível em: <https://bit.ly/37Zuyuh>. Acesso em: 21 maio 2021.

332 UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:31995L0046>. Acesso em: 31 maio 2021.

333 ARGENTINA. Decreto nº 995 de 02 de novembro de 2000. Disponível em: <https://bit.ly/2YycxQW>. Acesso em: 23 maio 2021.

334 ARGENTINA. Decreto nº 1.588 de de 29 de novembro de 2001. Disponível em: <https://bit.ly/3dB3liF>. Acesso em: 21 maio 2021

335 DELGADO, Lucrecio Rebollo; SALTOR, Carlos Eduardo. *El Derecho a Protección de Datos en España y Argentina - Orígenes y Regulación Vigente*. Madrid: Editorial DYKINSON; 2011, p. 159 apud GIMENES, Lucas de Souza. *Autoridade nacional de proteção de dados: análise da sua estrutura através de uma perspectiva de direito comparado*. 63 f. TCC (Bacharelado) - Curso de Direito, Universidade de Lavras, Minas Gerais, 2020

336 A manifestação contrária da União Europeia em relação ao arranjo institucional realizado pela Lei 25.326/2000 foi um dos principais motivos para a reforma institucional e promulgação da Lei 27.275/2017 [SIMÃO. op. cit. p. 12]. Neste sentido: "However, the Working Party draws attention to the fact that the head of the data protection supervisory authority is nominated and may be dismissed by the Minister of Justice and Human Rights, who also decides on the staffing of the authority. The authority is integrated within the structure of the Ministry of Justice. The Working Party considers that this situation does not guarantee that the authority may act in complete independence, and therefore urges that the necessary elements for that purpose be put in place, including changed modalities for appoint-

> Existem fortes probabilidades para supor que as normas de protecção não estão a ser cumpridas; existem motivos suficientes para crer que as autoridades competentes argentinas não tomam ou não tomarão as decisões adequadas na altura devida para resolver o caso em questão; a continuação da transferência dos dados possa representar risco iminente de graves prejuízos para as pessoas em causa, embora as autoridades competentes nos Estados-Membros envidem esforços razoáveis, dadas as circunstâncias, para facultar à organização responsável pelo tratamento estabelecida na Argentina a informação e oportunidade para responder[337].

Diante das críticas e da não confiabilidade do cenário internacional perante a normativa argentina, em 2017, promulgou-se a Lei 27.275/2017[338], pela qual foi instituída a *Agencia de Acceso a la Información Pública*. Esta autoridade de controle, por sua vez, é uma autarquia da Administração indireta com independência financeira, estrutural e funcional, conforme o art. 19 da normativa[339]. Esta lei se aplica a todos os entes estatais e privados[340] em todas as bases de dados, excetuado um rol de matérias elencadas no art. 8°[341] - mas é feita a ressalva de que esta exceção não pode ser ampliada quando a

ment and dismissal of the head of the authority". Disponível em <https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2002/wp63_en.pdf>. Acesso em: 24 maio 2021.

337 UNIÃO EUROPEIA. Decisão nº 2003/490/CE de 30 de junho de 2003, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais na Argentina. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32003D0490&from=EN>. Acesso em: 21 maio 2021.

338 ARGENTINA. Ley N° 27.275/2016. Disponível em: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/texact.htm>. Acesso em: 24 maio 2021.

339 "ARTÍCULO 19. Créase la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, como ente autárquico que funcionará con autonomía funcional en el ámbito de la JEFATURA DE GABINETE DE MINISTROS. La AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA debe velar por el cumplimiento de los principios y procedimientos establecidos en la presente ley, garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover medidas de transparencia activa y actuar como Autoridad de Aplicación de la Ley de Protección de Datos Personales N° 25.326".

340 "ARTÍCULO 7° — *Ámbito de aplicación*. Son sujetos obligados a brindar información pública: a) La administración pública nacional, conformada por la administración central y los organismos descentralizados, comprendiendo en estos últimos a las instituciones de seguridad social; b) El Poder Legislativo y los órganos que funcionan en su ámbito; c) El Poder Judicial de la Nación; d) El Ministerio Público Fiscal de la Nación; e) El Ministerio Público de la Defensa; f) El Consejo de la Magistratura;[...]".

341 "ARTÍCULO 8° — *Excepciones*. Los sujetos obligados sólo podrán exceptuarse de proveer la información cuando se configure alguno de los siguientes supuestos: a) Información expresamente clasificada como reservada o confidencial o secreta, por razones de defensa o política exterior.La reserva en ningún caso podrá alcanzar a la información necesaria para evaluar la definición de las políticas de seguridad, defensa y de relaciones exteriores de la Nación; ni aquella otra cuya divulgación no represente un riesgo real e identificable de perjuicio significativo para un interés legítimo vinculado a tales políticas; [...]".

sua divulgação não oferece um risco ou quando consiste em uma informação necessária para avaliar a política de segurança.

Além disso, a Lei estabelece a escolha do diretor que, agora, passa ter um mandato de cinco anos e ainda é escolhido pelo Executivo, embora tenha que passar pelo crivo da população por meio de audiências públicas e atender a uma série de outros requisitos (art. 20 e 21, Lei 27.275/2017), como idoneidade e dedicação exclusiva. O cargo de diretor passa a ser superior na hierarquia, operando na função de Secretário, e está respaldado por um processo de exoneração específico, em que o Executivo inicia e uma comissão bicameral do Congresso decide sobre a matéria.

Por fim, insta mencionar que a autoridade, com a lei mais recente, atingiu independência funcional, ao ser vinculada ao Gabinete de Ministros. Assim, tem-se uma menor interferência política e maior neutralidade na tomada de decisão do órgão. Na linha de conferir maior autonomia à *Agencia*, esta tem capacidade de deliberar sobre seu próprio orçamento, sem depender diretamente de outros poderes, e também sobre o corpo técnico e administrativo (art. 25, Lei 27.275/2017).

Destarte, após a reforma institucional em 2017, a autoridade argentina demonstrou um alto nível de autonomia funcional, estrutural e financeira. Isso porque ela é uma autarquia da Administração indireta com um distanciamento considerável do Poder Executivo, não sofrendo influência de quaisquer outras fontes políticas. Com isso, a autoridade ganhou independência quando comparada à antiga que fazia parte da Administração direta e vinculava-se ao Presidente do Executivo, o que demonstrou resultados práticos quanto ao modo operacional da autoridade - passou de um órgão consultivo para um fiscalizador[342].

342 SIMÃO, op. cit., pp. 20-21.

5.2.1. URUGUAI

O ponto de destaque do Uruguai em relação aos seus vizinhos na América Latina é que o debate sobre proteção de dados já havia se iniciado em 1981 no país, sendo o único país da América Latina a assinar e ratificar a Convenção nº 108. Com isso, alguns preceitos gerais referentes ao tratamento de dados já faziam parte do ordenamento jurídico uruguaio.

Porém, apenas em 11 de agosto de 2008, o país promulgou a Lei 18.331[343] - *Ley de Protección de Datos Personales y Acción de Habeas data* -, sendo o segundo da América Latina a ter uma lei geral de proteção de dados. A Diretiva nº 95/46/CE norteou o ordenamento jurídico uruguaio na seara da proteção de dados, mas nota-se que, embora a normativa do país seja diversificada - composta por uma lei geral, decretos, resoluções e notas técnicas -, a complexidade quando comparada aos dispositivos europeus é consideravelmente menor.

Diante disso, a Lei 18.331/2008 foi regulamentada pelo Decreto 414[344] de 31 de agosto de 2009, que buscava delimitar o arranjo institucional e o funcionamento da autoridade de controle do país, *Unidad Reguladora y de Control de Datos Personales*[345]. Segundo o Decreto, tem-se que a Unidad faz parte da Administração direta, vez que integra a *Agencia de Gobierno Eletronico y Sociedad de la Informacion y del Conocimento* (AGESIC)[346], órgão que está subordinado ao Presidente do Executivo. Dessa forma, entende-se que a autoridade é um órgão desconcentrado[347] integrante da Presidência da República e tem personalidade jurídica própria.

343 URUGUAI. Ley nº 18.331 de 18 de agosto de 2008. Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008>. Acesso em: 21 maio 2021.

344 URUGUAI. Decreto nº 414 de 31 de agosto de 2009. Disponível em: <https://www.impo.com.uy/bases/decretos/414-2009>. Acesso em: 21 maio 2021.

345 Interessante mencionar que o "Artículo 3", item C, da Lei 18.331/08 estabelece que a lei de proteção de dados uruguaia não se aplica às matérias de segurança pública e persecução penal. E, nesse sentido, não há referência a nenhuma outra disposição acerca da matéria, constatando-se o mesmo vácuo legislativo encontrado no Brasil.

346 "Artículo 31. Órgano de Control.- Créase como órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), dotado de la más amplia autonomía técnica, la Unidad Reguladora y de Control de Datos Personales. Estará dirigida por un Consejo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que por sus antecedentes personales, profesionales y de conocimiento en la materia aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos."

347 "Um órgão desconcentrado é aquele que a lei determina alguma competência permanente, mantendo, assim, a hierarquia com relação ao Poder Executivo" (DROMI, Roberto. *Derecho administrativo*. 10a. ed., Buenos Aires: editora, 2000, p. 496 e 497. apud SIMÃO, op. cit., p. 29). No mesmo sentido entende a doutrina nacional: "em razão da pluralidade e complexidade das sociedades e dos Estados contemporâneos, a administração pública se apresenta de modo desconcentrado, assim entendida a distribuição de competências para vários órgãos da administração direta, com manutenção do vínculo hierárquico" (FRANCISCO, José Carlos. Comentário ao artigo 87. In: CANOTILHO, J. J. Gomes; MENDES, Gilmar F.; SARLET, Ingo W.; STRECK, Lenio L. (Coords.). Comentários à Constituição do Brasil. São Paulo: Saraiva/Almedina, 2013, p. 2.556). Nesta estrutura, "o Presidente da República tem atribuições de coordenação e de subordinação em relação a todos os órgãos desconcentrados que integram a administração direta (assim entendidos órgãos da União como pessoa jurídica de direito público), salvo exceções constitucionais ou legais (que podem ser estabelecidas com amparo no art. 48, XI, da Constituição). Dessa função hierárquica em face de todos os integrantes extrai-se a competência do Presidente da República para fiscalizar, alterar, revogar, anular e avocar quaisquer atribuições de seus subordinados, bem como a função disciplinar ou punir integrantes da administração direta, mantendo a unidade político administrativa da União." [FRANCISCO, José Carlos, obra citada, p. 2.749).

Conforme dispõe o Capítulo VII da Lei 18.331/2008, a diretoria da Autoridade é composta pelo *Consejo Director e Consejo Consultivo*. O primeiro tem um papel central nas funções da autoridade e possui três membros, o diretor da AGESIC (nomeado pelo Presidente do Executivo) e outros dois indicados também pelo Executivo, tendo estes um mandato de quatro anos podendo ser exonerados por meio de devido processo legal. O segundo tem um papel secundário de analisar mudanças legislativas e é composto por um ex-membro do Legislativo; representante do Poder Judiciário; um do Ministério Público; um da Academia e outro do setor privado[348]. Enfim, os demais funcionários da autoridade são selecionados por meio de concurso público.

Isto posto, questiona-se a independência funcional da *Unidad* apesar da lei já ter resguardado a sua autonomia técnica e competência exclusiva. Isso decorre do fato de que a autoridade integra a AGESIC que tem alta proximidade com o Executivo, dependendo dele em termos de infraestrutura e nomeação de diretores. Dessa forma, a Unidad, de fato, possui independência técnica, mas não política, para tomadas de decisão, pondo em dúvida a sua capacidade de executar suas funções de maneira neutra e imparcial[349].

Além disso, tendo em mente a autonomia financeira da *Unidad*, a autoridade deve elaborar um orçamento que integrará com o da AGESIC, o qual faz parte do orçamento do Executivo, responsável por levar a proposta para o Congresso (art. 33, Lei 18.331/2008). Diante disso, observa-se que a autoridade tem independência financeira e que, mesmo que ocorra esta cadeia de repasses internos nas estruturas governamentais, não há quaisquer tipos de limitações orçamentárias por parte do Executivo. Por fim, é válido mencionar que, embora o país tenha um arranjo institucional em que a autoridade de controle não goza de plena independência e autonomia, o Uruguai é considerado pela União Europeia adequado para a transferência de dados. Neste sentido:

> **(6)** As normas de proteção dos dados pessoais da República Oriental do Uruguai baseiam-se em grande medida nas normas da Diretiva 95/46/CE e encontram-se estabelecidas na Lei n.o 18.331 de proteção dos dados pessoais e ação de habeas data (Ley n.o 18.331 de protección de datos personales y acción de habeas data), de 11 de agosto de 2008, que é aplicável tanto às pessoas singulares como às pessoas coletivas.

348 SIMÃO, op. cit., p. 32.

349 SIMÃO, op. cit., p. 29.

(7) A referida lei é regulamentada pelo Decreto n.o 414/009, de 31 de agosto de 2009, aprovado no intuito de clarificar diversos elementos da lei e regular a organização, os poderes e o funcionamento da autoridade nacional de proteção de dados. O preâmbulo deste decreto indica que, quanto a esta questão, a ordem jurídica nacional deve ser adaptada ao regime jurídico comparável mais comummente aceite, sobretudo o estabelecido pelos países europeus através da Diretiva 95/46/CE.

(8) Também existem disposições de proteção de dados em algumas leis especiais que criam e regulam bases de dados, nomeadamente leis que regulam determinados registros públicos (escrituras notariais, propriedade industrial e marcas, atos pessoais, direitos reais, atividade mineira ou informação financeira). A Lei n.o 18.311 aplica-se supletivamente às questões que não são especificamente regidas por esses diplomas específicos, nos termos do artigo 332.o da Constituição.

(9) As normas de proteção de dados aplicáveis na República Oriental do Uruguai cobrem todos os princípios básicos necessários para assegurar um nível adequado de proteção das pessoas singulares e preveem também exceções e limitações de modo a salvaguardar interesses públicos importantes. Estas normas de proteção de dados e as exceções referidas refletem os princípios consagrados na Diretiva 95/46/CE.[350]

Em suma, quando se trata do arranjo institucional escolhido pelo Uruguai, tem-se uma disposição em que a autoridade de proteção de dados não é completamente autônoma. O Poder Executivo ainda tem influência na nomeação dos cargos mais altos na entidade. No entanto, resguarda-se certas garantias que aproximam o órgão de uma autonomia plena, como o devido processo legal quando da exoneração de membros e a elaboração de um próprio orçamento sem a interferência do Executivo, apenas do Legislativo. Portanto, há certas fragilidades no modelo uruguaio que dificultam a execução de todas as competências da autoridade, mas observa-se um certo grau de autonomia na entidade que atende a requisitos internacionais.

350 UNIÃO EUROPEIA. Decisão de Execução da Comissão de 21 de agosto de 2012, 2012/484/UE. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32012D0484&from=ES#:~:text=As%20normas%20de%20prote%C3%A7%C3%A3o%20dos,habeas%20data%2C%20de%2011%20de>. Acesso em 24 maio 2021.

5.3. ENTREVISTAS

Os modelos estrangeiros de autoridades nacionais de proteção de dados foram outro ponto discutido nas entrevistas. Em relação a isso, Nefi Cordeiro, apenas ressaltou que a independência é uma característica fundamental que pode ser observada em diversas autoridades de outros países. Vladimir Aras apresentou o sistema português como um modelo a ser observado pelo Brasil. Este exemplo permite, segundo ele, ilustrar a compatibilidade de uma autoridade que pode ser ministrada por dois órgãos do governo (MP e Judiciário, no caso de Portugal), como ocorreria caso a ANPD fosse alocada sobre o CNJ e CNMP. Assim, o exemplo evidencia a possibilidade de a autoridade ter membros dos dois órgãos administrando-a.

Renato Sérgio de Lima, por sua vez, citou a GDPR, sendo este o "grande case" no âmbito da proteção de dados. Ele explicou que essa legislação define claramente os riscos do mau tratamento de dados pessoais, as sanções cabíveis e os órgãos responsáveis pela fiscalização. Contudo, esclareceu que o exemplo europeu não é muito compatível com o funcionamento das instituições brasileiras, sendo o exemplo estadunidense possivelmente mais agregador, pelo fato de existir lá o debate a respeito de arranjos federativos e competências institucionais. Nesse sentido, os EUA têm muitas polícias, então há uma discussão similar à brasileira a respeito da base legal de regulamentação dessas instituições.

Os EUA também foram citados por Jacqueline de Souza Abreu, a qual destacou que o país adota algum tipo de conselho (regional) para identificar a opinião pública acerca das políticas da autoridade, de modo a democratizar as políticas, o que deveria ser feito no Brasil. Por fim, Danilo Doneda, ao retomar o sistema europeu, ressaltou que a segurança pública não é matéria de direito comunitário na Europa e, portanto, a regulação do tema no âmbito da proteção de dados varia conforme o país membro.

6. POSSÍVEIS SOLUÇÕES PARA O BRASIL

6.1. RETOMADA DOS PROBLEMAS

Como exposto (*supra*, 3.3) um dos maiores entraves hoje observados em relação à atual ANPD diz respeito à independência perante as influências de outros órgãos governamentais, seja estrutural, funcional ou financeiramente. Diante disso e do disposto no art. 4º, III, da LGPD, há um debate quanto à alocação de uma autoridade que atuará nestas exceções do referido dispositivo, uma vez que esta supervisionará e aplicará sanções aos órgãos públicos que fazem tratamento de dados no âmbito da SP/PP. Dessa forma, o atual arranjo em que se localiza a ANPD - órgão da Administração direta, submisso ao Presidente da República - não se coaduna com o posicionamento da autoridade penal, em que esta possa executar suas funções da melhor maneira, isto é, de modo independente.

À vista disso, uma possível alocação do futuro órgão de supervisão penal no mesmo arranjo institucional atual da ANPD impossibilitaria que aquele fosse neutro e imparcial na tomada de decisão, deixando em segundo plano a proteção de dados. Neste sentido, observa-se no modelo previsto na LGPD uma ausência de independência conforme os três tipos de autonomias previstas na GDPR (*supra*, 5.1.1). As questões funcionais, estatutárias e orçamentárias ficam à cargo e disposição do Executivo, o qual passa a ter extrema relevância no que tange à nomeação, à exoneração e aos recursos relacionados aos membros e orçamento da autoridade.

Isto posto, há um problema de autonomia no atual arranjo institucional da ANPD, que de maneira alguma pode ser transplantado para a "ANPD - penal". Isso porque, tendo em mente a última, esta poderia ser utilizada como meio para embates políticos por conta das competências atribuídas a ela, desviando-a da sua principal função que é a proteção dos dados nos tratamentos realizados nos âmbitos de SP/PP. Logo, um arranjo diferente do hodierno deve ser elaborado a fim de garantir plena independência do órgão de controle.

O Anteprojeto de LGDP para a SP/PP propôs um arranjo institucional diferente daquele previsto na LGPD, ou seja, um em que a autoridade de controle penal, UPDP, estaria alocada no CNJ. Os diretores deste órgão teriam mandatos de quatros anos e seriam escolhidos pelo CNJ. Ainda, haveria um intercâmbio dos servidores, que atuariam tanto nos serviços do Conselho como na UPDP. A Comissão justificou tal desenho institucional por meio da autonomia que este conferiria à autoridade, por ter uma composição diversificada e por maximizar a imparcialidade nas decisões do órgão. Para além disso, argumentou que este arranjo evitaria o aumento de gastos com a criação de um novo órgão específico, aproveitaria a expertise do CNJ e possibilitaria uniformização de políticas públicas para todo o país, assim atingindo o nível adequado segundo os parâmetros europeus para a transferência e proteção de dados.

Como vimos, o modelo encontra três objeções (*supra*, 4.2): (a) a Constituição Federal não confere competência ao Conselho Nacional de Justiça para executar as funções de uma autoridade de controle de dados. O CNJ tem o seu rol de competências taxativo listado na Magna Carta, que não conta com as atribuições para regular e supervisionar o tratamento de dados no âmbito da segurança pública. No entanto, há entendimentos contrários à taxatividade que ampliam as competências do órgão, como fora melhor trabalhado acima.

Além disso, (b) a possível invasão de competências caso o CNJ venha executar as funções de uma "ANPD penal". Isso decorre de a CF/88 conferir ao Ministério Público o controle externo da atividade de polícia. Diante disso, haveria um conflito negativo entre agências, que dificultaria a proteção de dados.

Ainda, (c) a autonomia e a eficiência da autoridade de controle em face do novo arranjo institucional proposto são questionadas por duas razões: a uma, porque existiriam duas entidades de proteção de dados, a ANPD e a UPDP, o que poderia incorrer em uma concorrência negativa e falta de coordenação entre elas; a duas, pois não necessariamente a vinculação ao CNJ conferiria a autonomia necessária à UPDP. Do ponto de vista legal que poderia influenciar na independência do órgão, há a possibilidade de haver recurso das decisões da UPDP ao Plenário do CNJ, podendo ser questionada eventual determinação do órgão; some-se a isto que o STF já manifestou que não se submete ao CNJ. Já do ponto de vista administrativo, o Poder Judiciário teria grande influência na UPDP, tendo em vista que o CNJ, composto em sua maioria por magistrados, nomearia os diretores da entidade.

De outro lado, os entrevistados apresentaram posicionamentos diversos acerca dos resultados que poderiam decorrer do novo arranjo institucional proposto no Anteprojeto mencionado: (a) Vladimir Aras compreende que a melhor solução para enfrentar a forte associação da autoridade com o Poder Executivo é vincular a UPDP a entes estatais já consolidados, como o CNJ e o CNMP. No entanto, adverte, seria necessária a vinculação a ambos os órgãos, pois haveria um menor custo decisório e compatibilizaria a independência e a competência da autoridade. Ainda, no arranjo pensado por Vladimir Aras haveria uma maior transparência da autoridade, bem como uma maior independência e autonomia na forma de ingresso.

Nefi Cordeiro (b) entende que faz-se necessário uma autoridade independente para o controle de órgãos públicos também independentes, a fim de não ter resistência destes perante as decisões e regulamentações daquela. Porém, entende ser a solução de vinculação ao CNJ a que melhor garante autonomia e aplicação das decisões da autoridade.

Já (c) Renato Sérgio de Lima compartilha da visão de que a UPDP deveria ser alocada sobre o CNMP e CNJ, pois conferiria à autoridade a competência de atuar no âmbito da persecução penal das

atividades de polícia. Além disso, ressalta que é imprescindível que o anteprojeto de uma LGPD penal conceitue segurança pública e revogue os demais significados em outras normativas.

Jacqueline de Souza Abreu (d) defende que o arranjo institucional ideal seria aquele em que haveria apenas a ANPD independente de influência política e composta por um órgão técnico capaz de aplicar suas decisões. No entanto, compreende que os órgãos públicos que fazem tratamento de dados para fins de SP/PP já estão submetidos à ANPD, conforme o art. 4º, § 3º, LGPD. Por fim, entende a entrevista que a opção pelo CNJ foi a melhor solução em face do processo legislativo.

Danilo Doneda (e) entende que a ANPD já possui capacidade de fiscalizar e sancionar órgãos públicos independentes em determinadas matérias. Com isso, uma vinculação ao CNJ ou ao CNMP apenas se justificaria diante da falha institucional da ANPD, que apesar de ter competências suficientes para arbitrar decisões, não tem capacidade de aplicá-las aos outros órgãos.

Destarte, a configuração proposta pelo corpo de juristas selecionados para elaborar o Anteprojeto de Lei supracitado, poderá incorrer em diversas falhas que dificultarão a capacidade de tomada de decisão da UPDP. Diante disso, destaca-se a dependência ao Judiciário, invasão de competências e conflito entre agências, que poderão comprometer a neutralidade e o exercício de suas funções. Em contrapartida, poderão ser estas falhas mitigadas ou inexistentes na prática, conferindo ao órgão de controle a tão desejada independência institucional. Neste sentido, os diferentes posicionamentos e soluções apresentadas pelos entrevistados indicam a dificuldade de se pensar em todos os cenários que poderiam decorrer de determinado arranjo institucional, bem como a não uniformidade de opiniões acerca de qual seria o melhor desenho a ser elaborado.

6.2. O QUE PODE SER APROVEITADO DOS MODELOS ESTRANGEIROS

Ante os problemas expostos acima e a análise de diferentes modelos estrangeiros, a presente seção tem como escopo apontar as qualidades identificadas nos diferentes arranjos institucionais examinados, que podem ser aproveitadas no sistema brasileiro para alocação de uma autoridade de controle no âmbito da segurança pública e persecução penal. Para tanto, analisar-se-á a alocação e as autonomias estrutural e funcional das diferentes autoridades, tomando como base apenas os pontos julgados interessantes para uma possível transposição para o modelo brasileiro.

Em primeiro lugar, no que tange ao posicionamento da autoridade nas estruturas do Estado, observa-se diferentes estratégias de alocação que asseguraram a autonomia do órgão. A Argentina, a Itália e a Espanha adotam um modelo ideal ao intitular sua autoridade como uma autarquia da Administração indireta, atendendo a um maior grau de autonomia da entidade. Já Portugal aborda a temática de maneira diferente, mas que ainda protege os interesses de uma autoridade independente. O país decidiu por alocar a autoridade sob a Assembleia da República, órgão componente do Poder Legislativo.

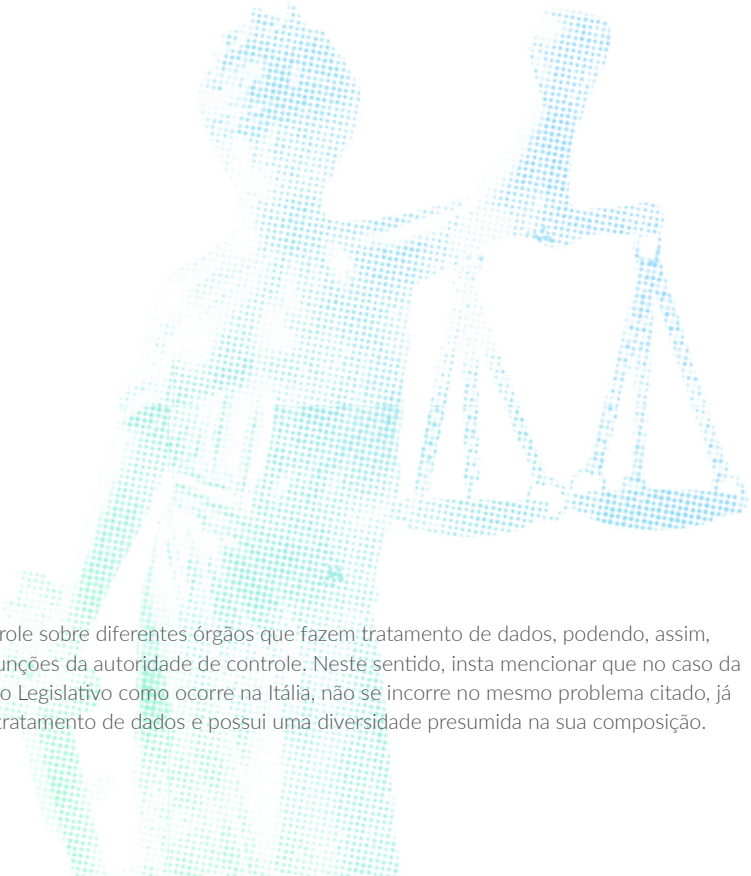
Em que pese a escolha dos modelos estrangeiros, optou-se por excluir do aproveitamento o arranjo institucional da autoridade do Uruguai. Isso decorre do fato de que o órgão de controle encontra-se vinculado ao Poder Executivo, o que, como já dito, é prejudicial ao funcionamento da autoridade. Ainda, ao comparar este modelo estrangeiro com os demais, observa-se uma disparidade quanto à efetividade operacional e proteção à autonomia da autoridade.

Em segundo lugar, os modelos estrangeiros demonstram diferentes abordagens quanto à autonomia estrutural e à funcional, que são interessantes para o arranjo brasileiro. A Argentina adota um sistema de freios e contrapesos, em que o Poder Executivo nomeia e exonera o diretor, mas para tanto é necessário passar por audiências públicas ou pelo Congresso. De maneira semelhante, na Espanha, o Ministério da Justiça seleciona os candidatos e o Legislativo decide por aprovar. Diferentemente, Portugal opta por um arranjo que preza pela diversidade da composição da Diretoria desde sua origem. No país, o Executivo, Legislativo, respectivo CNMP e CNJ nomeiam membros da direção da autoridade de controle, que representarão os interesses dos seus respectivos órgãos de origem. Por fim, na Itália, há um arranjo diferenciado pouco semelhante aos demais. O Poder Legislativo é responsável por nomear os diretores da autoridade de controle.

Optou-se novamente por não abordar o modelo uruguaio no que se refere à autonomia estrutural e funcional. Isso porque os membros da diretoria são nomeados exclusivamente pelo Poder Executivo - excetua-se aquela diretoria secundária com competências consultivas apenas. Diante disso, tem-se como preferência neste trabalho aqueles modelos que prezam pela diversidade na composição;

que funcionam com mais de uma entidade envolvida na nomeação e exoneração dos membros da autoridade; ou que não dependam de forma exclusiva do Executivo[351].

Por fim, insta mencionar que todos os modelos estrangeiros abordados, exceto o uruguaio, possuem legislação aplicável ao tratamento de dados realizados para fins de SP/PP. A hipótese de um arranjo falho, que não abrange uma autoridade de controle completamente autônoma, ainda é melhor do que um cenário sem lei alguma, em que não há qualquer tipo de regulação nas matérias em questão, deixando os direitos da população desprotegidos. Infelizmente, é o caso do Brasil.



351 Isso decorre do fato de que o Executivo possui controle sobre diferentes órgãos que fazem tratamento de dados, podendo, assim, enviesar a tomada de decisão ou mesmo execução das funções da autoridade de controle. Neste sentido, insta mencionar que no caso da nomeação de membros estar vinculada exclusivamente ao Legislativo como ocorre na Itália, não se incorre no mesmo problema citado, já que é um Poder que não se envolve diretamente com o tratamento de dados e possui uma diversidade presumida na sua composição.

7. SUGESTÃO DE ENCAMINHAMENTO

Ante todo o exposto, parece ao grupo que a melhor solução para o problema de independência da autoridade de controle é transformar a atual Autoridade Nacional de Proteção de Dados em uma autarquia integrante da Administração indireta, que teria dentre outras competências a de supervisionar e sancionar os tratamentos de dados realizados para segurança pública e persecução penal. Para tanto, a Constituição Federal exige, em um primeiro momento, uma lei específica originada do Executivo para convertê-la em autarquia.

Isso decorre do fato de que, com isso, não haveria duas entidades competindo entre si pela proteção de dados, reduzindo os custos e economizando recursos humanos para o Estado, já que haveria um intercâmbio dos funcionários dentro da própria autoridade. Ainda, o artigo 55-A, § 1º, LGPD já prevê a natureza transitória deste órgão, facilitando este processo de transição de uma ANPD dependente do Executivo para uma autarquia dotada de independência.

A autoridade contaria com sete membros diretores, sendo designados da seguinte maneira: 1 pelo CNJ; 1 pelo CNMP; 3 pelo Legislativo; 2 pelo Executivo; 1 pela Defensoria Pública da União; 1 pela Ordem dos Advogados do Brasil (OAB). Os membros teriam mandatos de quatros anos sem a possibilidade de reeleição, a fim de garantir a imparcialidade e rotatividade do cargo. Estes membros teriam funções exclusivas, não podendo exercer outra função pública ou privada durante o mandato. Dessa forma, esta composição da autoridade garantiria uma representatividade dos órgãos envolvidos no tratamento de dados de segurança pública, bem como resguardaria a independência funcional e estrutural da agência.

Ademais, o problema de não aceitação por parte de órgãos como o Ministério Público e polícias seria amenizado, já que a decisão da autoridade não estaria respaldada pelo Executivo ou mesmo pelo Judiciário (caso a proposta da "LGPD - penal" venha se materializar), mas vincular-se-ia à imagem de um órgão independente sem influências dos outros poderes.

Em contrapartida, esta solução ideal teria que enfrentar uma série de obstáculos.

De início, a ANPD não possui competência para regular tais matérias. Neste sentido, para concretização desta solução seria necessário alterar a LGPD, de maneira a atribuir à ANPD competências para supervisionar e regular os tratamentos de dados realizados no âmbito da SP/PP. Além disso, seria necessário incluir diversas disposições acerca de como se daria essa regulamentação como fora realizado no Anteprojeto da "LGPD - penal", bem como adicionar um parágrafo ao art. 3º, LGPD estabelecendo: "Esta lei também se aplica ao tratamento de dados pessoais realizados para fins exclusivos de segurança pública e persecução penal".

Um segundo obstáculo para aplicação da solução proposta se refere à relutância do Executivo em editar uma lei de competência exclusiva sua, que limite os seus poderes e influências. Diante disso, a transformação de uma entidade totalmente submissa ao Executivo para uma independente, que poderia aplicar-lhe sanções, pode gerar um estranhamento quando da elaboração da normativa e demandaria um altivo senso democrático e republicano.

Em suma, o arranjo institucional proposto no presente trabalho atingiria todas as formas de autonomia, sendo elas estrutural, financeira e funcional. Apesar de apresentar dificuldades quanto à aprovação, extrai-se dos modelos estrangeiros e das entrevistas realizadas no início do trabalho as qualidades que melhor proporcionam uma execução neutra e livre de influências das funções da autoridade.

8. CONCLUSÃO

A proteção de dados é um tema que só tem ganhado importância nos últimos anos com o desenvolvimento tecnológico na sociedade da informação. Diante disso, a elaboração de leis e criação de entidades supervisoras é de extrema importância para se regular o tratamento de dados, seja na esfera privada ou na pública. Sobretudo nesta última, surge a discussão acerca de qual seria o melhor arranjo institucional em que uma autoridade de controle conseguiria desempenhar todas as suas funções sem sofrer influências e incorrer em decisões parciais.

À vista disso, o presente trabalho apresentou esta discussão à luz do ordenamento jurídico brasileiro. A fim de mapear o cenário e esclarecer o espaço no qual se dá o debate, apresentou um histórico da regulamentação da proteção de dados no país, bem como um panorama geral do atual arranjo institucional instituído pela LGPD e também um arranjo hipotético desenhado no Anteprojeto de uma "LGPD - penal". Neste sentido, apontou uma série de problemas relacionados à temática, os quais orbitam uma questão central: a independência da autoridade de controle na seara da proteção dos dados tratados para fins de SP/PP.

Buscou-se as respostas dadas por modelos estrangeiros, nos quais o debate já existe. A autonomia financeira, estrutural e funcional da autoridade é um ponto sensível que pode ser facilmente minada a depender da alocação do órgão de controle. A título de exemplo, no Brasil, a ANPD - que carece de competência para regular o tratamento de dados para fins de segurança pública e persecução penal - está alocada sob a Presidência da República. Neste sentido, em estruturas semelhantes encontradas em outros países, os doutrinadores entendem que a autoridade supervisora carece de independência e não conseguiria exercer de maneira neutra e imparcial as suas funções de regulamentação dos órgãos governamentais.

Diante desse cenário, propôs-se uma solução para o problema de uma autoridade supervisora do tratamento de dados utilizados SP/PP: a criação de uma autarquia com competências para regular todos os segmentos de tratamento de dados, independente do seu fim. No entanto, é válido mencionar que esta autoridade de controle, quando se trata da regulamentação de entes públicos, deve ter uma independência ainda mais acentuada para que não tenha sua função central de proteção dos titulares dos dados prejudicada.

9. REFERÊNCIAS BIBLIOGRÁFICAS

- ABREU, Jacqueline de Souza. *Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD* in DONEDA, Danilo et. al. (coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 583-603.
- ARANTES, Camila Rioja; BLUM, Renato Opice. *Autoridades de Controle, Atribuições e Sanções*. in: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.) Comentários ao GDPR - Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Revista dos Tribunais; 2018. p. 227-253.
- ARGENTINA. Decreto nº 995, de 02 de novembro de 2000. Disponível em: <https://bit.ly/2YycxQW>. Acesso em: 23 maio 2021.
- ARGENTINA. Decreto nº 1.588 de de 29 de novembro de 2001. Disponível em: <https://bit.ly/3dB3liF>. Acesso em: 21 maio 2021.
- ARGENTINA. Ley nº 25.326, de 02 de novembro de 2000. Disponível em: <https://bit.ly/37Zuyuh>. Acesso em: 21 maio 2021.
- ARGENTINA. Ley Nº 27.275/2016. O texto da Lei está disponível em: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/texact.htm>. Acesso em: 24 maio 2021.
- AGENCIA ESPAÑOLA PROTECCIÓN DADOS. *Historia*. Disponível em: <https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/historia>. Acesso em: 07 jun. 2021.
- BEZERRA, Maria Ruth Borges. Autoridade Nacional De Proteção De Dados Pessoais: A Importância Do Modelo Institucional Independente Para A Efetividade Da Lei in *Revista Caderno Virtual*, v. 2, n. 44. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3828>. Acesso em: 17 maio 2021.
- BRASIL. Projeto de Lei, de 13 de junho de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 31 maio 2021.
- BRASIL. Projeto de Lei nº 4.060-A, de 13 de junho de 2012. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0ksapb6v7tyhv1fxgf17w4iqd4918642.node0?codteor=1665276&filename=Tramitacao-PL+4060/2012>. Acesso em: 31 maio de 2021.
- BRASIL. Projeto de Lei da Câmara nº 53, de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>. Acesso em: 31 maio 2021.
- BRASIL. Veto nº 33, de 2018. Veto Parcial aposto ao Projeto de Lei da Câmara nº 53 de 2018 (nº 4.060/2012, na Casa de origem), que "Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)". Disponível em: <https://www.congressonacional.leg.br/materias/vetos/-/veto/detalhe/12024>. Acesso em: 31 maio 2021.
- BRASIL. Medida Provisória nº 869, de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062>. Acesso em: 31 maio 2021.
- BRASIL. Projeto de Lei de Conversão nº 7, de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7948609&ts=1594019727977&disposition=inline>. Acesso em: 31 maio 2021.
- CANOTILHO, J. J. Gomes; MENDES, Gilmar F.; SARLET, Ingo W.; STRECK, Lenio L. (Coords.). *Comentários à Constituição do Brasil*. São Paulo: Saraiva/Almedina, 2013. 2.380 p.

- CASTRO, Maria Eugênia Bordinassi de. *A estrutura e a natureza jurídica da Autoridade Nacional de Proteção de Dados com base na lei nº 13.853/2019*. In: MAGRO, Américo Ribeiro; TEIXEIRA, Tarcísio (coords.). *Proteção de Dados - Fundamentos Jurídicos*. 1. ed. Salvador; JusPODIVM; 2019. p. 199 - 227.
- COMISSÃO DE JURISTAS DA C MARA DOS DEPUTADOS. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Disponível em <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf>. Acesso em: 29 maio 2021.
- CONGRESSO NACIONAL. Emendas à Medida Provisória nº 869, de 2018, que "Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências.". Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7915984&ts=1594019729749&disposition=inline>. Acesso em: 31 maio 2021.
- DELGADO, Lucrecio Rebollo; SALTOR, Carlos Eduardo. *El Derecho a Protección de Datos en España y Argentina - Orígenes y Regulación Vigente*. Madrid: Editorial DYKINSON, 2011, p. 159.
- DROMI, Roberto. *Derecho administrativo*. 10a. ed., Buenos Aires: editora, 2000.
- DONEDA, Danilo. Um Código para a Proteção de Dados Pessoais na Itália in *Revista Trimestral de Direito Civil*, Rio de Janeiro, v. 16, p. 78-99, 2003.
- ESPANHA. Lei Orgânica 5/1992, de 29 de outubro. Regulamenta o tratamento automatizado de dados pessoais. Disponível em: <https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189>. Acesso em: 07 jun. 2021.
- ESPANHA. Lei Orgânica 3/2018, de 5 de dezembro. Da proteção de dados pessoais e garantia dos direitos digitais. Disponível em: <https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>. Acesso em: 07 jun. 2021.
- GIMENES, Lucas de Souza. *Autoridade nacional de proteção de dados: análise da sua estrutura através de uma perspectiva de direito comparado*. 63 f. TCC (Bacharelado) - Curso de Direito, Universidade de Lavras, Minas Gerais, 2020.
- GUIDI, Guilherme. *Modelos regulatórios para proteção de dados pessoais*. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 31 maio 2021.
- GUTIERREZ, Andriei. *Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade* in MALDONADO, Viviane Nóbrega (coord.); BLUM, Renato Opice (coord.). LGPD: *Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2019, p. 387-402.
- INTERNETLAB. Tribunal Europeu impõe multa à Espanha por descumprimento à Diretiva de proteção de dados para investigações criminais. Disponível em: <https://www.internetlab.org.br/pt/itens-semanario/uniao-europeia-tribunal-europeu-impoe-multa-a-espanha-por-descumprimento-a-diretiva-de-protecao-de-dados-para-investigacoes-criminais/>. Acesso em: 07 jun. 2021.
- LODDER, George Neves. *Autoridade Nacional de Proteção de Dados: questões* in ASSOCIAÇÃO NACIONAL DE PROCURADORES DA REPÚBLICA. *Proteção de dados pessoais e investigação criminal*. Brasília: ANPR, 2020, p. 116-139.
- MARZOCCHI, Ottavio. Fichas técnicas sobre a União Europeia - 2021: Proteção de Dados. Disponível em: <https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf>. Acesso em: 31 maio 2021.
- MASSENO, Manuel David. A Proteção de Dados Pessoais em Portugal e nos Outros Países de Língua Portuguesa, uma cartografia das Fontes Legislativas. Disponível em: <http://direitoeti.com.br/artigos/a-protecao-de-dados-pessoais-em-portugal-e-nos-outros-paises-de-lingua-portuguesa-uma-cartografia-das-fontes-legislativas/>. Acesso em: 31 maio 2021.
- MEIRELLES, Hely Lopes. Direito Administrativo Brasileiro. São Paulo: Malheiros Editores, 23ª ed., 1998.
- MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental – São Paulo: Saraiva, 2014.
- NUCCI, Guilherme de Souza. *Código penal comentado*. 17. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2017.

- PORTUGAL. Lei nº 67, de 26 de outubro de 1998. Lei da Protecção de Dados Pessoais que transpõe para a ordem jurídica portuguesa a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados. Disponível em: <https://dre.pt/pesquisa/-/search/239857/details/maximized#:~:text=Qualquer%20pessoa%20que%2C%20agindo%20sob,por%20for%C3%A7a%20de%20obriga%C3%A7%C3%B5es%20legais>. Acesso em: 31 maio 2021.
- PORTUGAL. Lei n.º 43, de 2004. Lei de organização e funcionamento da Comissão Nacional de Protecção de Dados. Disponível em: <https://dre.pt/web/guest/legislacao-consolidada/-/lc/122101697/diploma?_LegislacaoConsolidada_WAR_drefrontofficeportlet_rp=diploma&filter=-Filtrar>. Acesso em: 31 maio 2021.
- PORTUGAL. Constituição da República Portuguesa, de 1976. Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Acesso em: 31 maio 2021.
- REIS, Carolina; COSTA, Eduardo; SILVA, Felipe; BAWDEN, Henrique; PEREIRA, José Renato Laranjeira de; SARMENTO, Paulo. *Nota Técnica: Sobre o Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Investigação Criminal.* Brasília: o Laboratório de Políticas Públicas e Internet - LAPIN, 2020.
- SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. *Autoridades de proteção de dados na América Latina: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai*. São Paulo: Instituto Brasileiro de Defesa do Consumidor (Idec), 2019.
- SOUZA NETO, Cláudio Pereira de. *Da Segurança Pública: art. 144*. In: CANOTILHO, J. J. Gomes; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; STRECK, Lenio Luiz. Comentário à Constituição do Brasil. São Paulo: Saraiva, 2013.
- UNIÃO EUROPEIA. Diretiva 2016/679 (General Data Protection Regulation - GDPR): artigo 5. Disponível em: <https://gdpr.algolia.com/pt/gdpr-article-5>. Acesso em: 31 maio 2021.
- UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:31995L0046>. Acesso em: 31 maio 2021.
- UNIÃO EUROPEIA. Decisão nº 2003/490/CE de 30 de junho de 2003, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais na Argentina. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32003D0490&from=EN>. Acesso em: 21 maio 2021.
- UNIÃO EUROPEIA. Decisão de Execução da Comissão de 21 de agosto de 2012, 2012/484/UE. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:-32012D0484&from=ES#:~:text=As%20normas%20de%20prote%C3%A7%C3%A3o%20dos,habeas%20data%2C%20de%2011%20de>. Acesso em 24 mai. 2021.
- UNIÃO EUROPEIA. Convenção 108 de 1981. Disponível em: <https://www.acnur.org/fileadmin/Documentos/portugues/BDL/Convencao_Europeia_sobre_a_Nacionalidade.pdf?view=1>. Acesso em: 21 maio 2021.
- URUGUAI. Ley nº 18.331 de 18 de agosto de 2008. Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008>. Acesso em: 21 maio 2021.
- URUGUAI. Decreto nº 414, de 31 de agosto de 2009. Disponível em: <https://www.impo.com.uy/bases/decretos/414-2009>. Acesso em: 21 maio 2021.

PODCAST:

RECONHECENDO SEU DIREITO

PODCAST:
RECONHECENDO SEU DIREITO

Ana Carolina Dias
Antonio Piva
Beatriz Baccaro
Beatriz Crisostomo
Paula Rodovalho

1. INTRODUÇÃO

1. (ANTONIO PIVA)
Olá, querido ouvinte. Bem-vindo ao Reconhecendo seu Direito. Nesse Podcast eu, Antonio, eu Paula (Paula Rodovalho) e eu Bia (Beatriz Baccaro), alunos da graduação da Escola de Direito da FGV-SP, falaremos a respeito do projeto de implementação de câmeras com capacidade de reconhecimento facial no metrô de São Paulo pela Companhia do Metropolitano de São Paulo.

2. (ANTONIO PIVA)
A ideia central desse episódio é apresentar questões relativas às inconsistências e problemas advindos desse projeto. Em primeiro lugar, faremos uma contextualização a respeito do funcionamento dos sistemas de reconhecimento facial e o projeto do metrô. Em seguida, vamos fazer uma análise a respeito da adequação, necessidade e proporcionalidade do projeto, abordando questões como violação e abuso de direitos, como o de privacidade, e falta de transparência por parte da empresa a respeito da tecnologia e seu uso de dados pessoais, entrando em discussão a Lei Geral de Proteção de Dados. Somado a isso, demonstraremos os principais argumentos dos agentes responsáveis pelo procedimento judicial iniciado contra a Companhia Metropolitana nesse projeto do Metrô. Por fim, apresentaremos algumas questões que passaram pelo projeto na relação existente entre o metrô e o usuário, ao final sendo trazidas possíveis soluções para tal.

3. (ANTONIO PIVA)
Antes de expor o projeto em si, cabe o questionamento inicial: o que é e como funciona o reconhecimento facial?

4. (ANTONIO PIVA)
Você pode nos falar um pouco sobre isso, Bia?

5. (BEATRIZ BACCARO)
Claro, Antonio.

6. (BEATRIZ BACCARO)
O reconhecimento facial é um sistema que, com o uso de algoritmos e softwares, mapeia padrões nos rostos dos indivíduos e detecta rostos. Inicia-se com a coleta da imagem da pessoa, por meio da câmera. Em seguida, classificam as pessoas em padrões com base em suas características. Essas características são transformadas em “pontos”, que são gravados e armazenados em um banco de dados e que, analisados em conjunto por um sistema

de cálculos, identifica o rosto de determinado indivíduo no processo de autenticação, ou seja, quando a câmera registra a imagem e o sistema busca nos dados face semelhante.

7. (BEATRIZ BACCARO)
A ideia de utilizar esse sistema para fins de segurança vem se tornado uma tendência mundial, com diversos casos, internacionais e nacionais, de presença de câmeras de reconhecimento facial em ruas, estabelecimentos públicos e privados, transportes, shoppings centers, entre outros.

8. (BEATRIZ BACCARO)
No entanto, apesar do crescimento de tais iniciativas para uso dessa ferramenta de reconhecimento de faces, ainda falta clareza sobre como estão sendo e serão empregadas e sob quais custos. Também já existem casos em que o reconhecimento facial se mostrou tecnicamente falho, resultando em situações de constrangimento e até penalmente preocupantes.

9. (BEATRIZ BACCARO)
Surgem questões relativas à privacidade, segurança dos dados, transparência e discriminação no âmbito dessa tecnologia e é nesse ponto que entra o Caso do Metrô de SP.

10. (BEATRIZ BACCARO)
O projeto trata de implantar um sistema de monitoração eletrônica com reconhecimento facial nas linhas azul, verde e vermelha do metrô de São Paulo. A Companhia do Metropolitano de São Paulo abriu edital, em 2019, para a compra de um sistema de reconhecimento facial cujo projeto previa a instalação de câmeras com tal tecnologia nas linhas 1 – Azul, 2 – Verde e 3 – Vermelha.

11. (BEATRIZ BACCARO)
O vencedor da licitação foi o Consórcio Engie Ineo Johnson, com um valor do contrato de mais de 58 milhões e prazo de aproximadamente 47 meses para execução.

12. (ANTONIO PIVA)
Acho que a Paula pode começar com a primeira problemática do projeto, não é mesmo?

13. (PAULA RODOVALHO)
Sim, claro. A primeira questão alarmante com a qual podemos nos deparar é a da finalidade dessa proposta de implementar câmeras de reconhecimento facial nas linhas do metrô.

2. DESENVOLVIMENTO

2.1. FINALIDADE E ADEQUAÇÃO

14. (ANTONIO PIVA)
Exato. Por que utilizar esse método de reconhecimento facial?

15. (PAULA RODOVALHO)
Olha, Antonio, muito provável que isso advenha da nova moda do tecno solucionismo. A ideia da tecnologia como aliada em vários setores trouxe, na tentativa de suprir recursos falhos de segurança pública, esse anseio de utilizar-se de mecanismos precisos e invasivos na busca por seguridade.

16. (PAULA RODOVALHO)
A Companhia Metropolitana informou algumas das justificativas para implantar esse sistema de monitoração eletrônica no metrô, o que inclui o reconhecimento facial. Sinteticamente seriam (i) aumentar a quantidade de locais monitorados; (ii) melhorar a qualidade do armazenamento de imagens; (iii) implementar um sistema capaz de gerar alarmes; (iv) integrar sistemas de monitoração eletrônica em um só, centralizando equipamentos; e (v) monitorar áreas de circulação restrita para pessoas/animais.

17. (PAULA RODOVALHO)
Ainda, a Companhia também alegou que a modernização contratada teria por objetivo aperfeiçoar a tecnologia voltada à segurança pública e ao atendimento de órgãos públicos que demandam colaboração da Companhia para auxiliar na investigação e repressão de infrações.

18. (PAULA RODOVALHO)
Em um documento de resposta à decisão do TJ-SP no âmbito de uma ação cautelar interposta pela Defensoria Pública contra a Companhia Metropolitana neste caso do metrô, como será abordado mais pra frente neste podcast, a Companhia também disse que a funcionalidade do software que identifica facialmente as pessoas só será utilizada em casos específicos, para atender demandas esporádicas, como por exemplo a busca de pessoas desaparecidas ou identificação de usuário que eventualmente tenha praticado algum crime nas dependências do metrô.

19. (BEATRIZ BACCARO)

Sim. E nesse mesmo sentido, recentemente, o Projeto de Lei (nº 865/19) da ALESP, ao tentar tornar obrigatória a instalação de câmeras de reconhecimento facial em todas as estações do Metrô e da CPTM, pautou-se na finalidade de coibir a ação de criminosos nas estações e nos trens, preservando a segurança dos usuários. O projeto também previa a possibilidade de investigar casos de assédio nos transportes por meio do sistema e, também, encontrar pessoas desaparecidas, podendo o Metrô e a CPTM manter parcerias com autoridades públicas e órgãos de segurança pública para auxiliar na localização de foragidos.

20. (PAULA RODOVALHO)

Justamente. A primeira grande questão polêmica em relação à finalidade reside nessa justificativa de segurança pública.

21. (PAULA RODOVALHO)

A Nova Lei Geral de Proteção de Dados, publicada em 2018, traz uma série de princípios e diretrizes com objetivo de contribuir para a proteção de dados pessoais. Buscando padronizar normas e práticas, a lei veio para criar um cenário de segurança jurídica no âmbito digital em relação a dados pessoais. Além de garantias, regras e preceitos, a LGPD também previu sanções para os casos em que não fossem cumpridos os parâmetros de proteção de dados presentes na lei.

22. (PAULA RODOVALHO)

Logo no início de sua redação, a Lei já traz alguns conceitos necessários para o entendimento da problemática do caso do metrô. Em seu artigo 5º, inciso III, por exemplo, traz o conceito de dado pessoal sensível, que seria o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Também traz o conceito de tratamento, qual seja, a operação de coleta, produção, utilização, acesso, reprodução, processamento, armazenamento, controle da informação, difusão ou extração realizada com dados pessoais.

23. (PAULA RODOVALHO)

Esses conceitos são os mais relevantes tratando-se de reconhecimento facial, pois estamos falando de dados pessoais, grande parte sensíveis e de caráter biométrico, num cenário em que haverá tratamento desse dado pelo sistema de reconhecimento facial. Dessa forma, passível estariam a empresa responsável pela tecnologia, a Engie Ineo Johnson, e a Metropolitana, às regulações e parâmetros da LGPD.

24. (PAULA RODOVALHO)

O que aconteceu na verdade foi que a Companhia Metropolitana, quando foi perguntada, a respeito da falta de uma especificação de como funcionaria de fato a tecnologia e como seriam utilizados os dados, e questões nesse sentido, falou que a coleta de dados realizada nas estações de Metrô estaria ligada à Segurança Pública e/ou atividades de investigação e repreensão a infrações penais, de forma que o caso vai ser enquadrado no artigo 4º da LGPD, como tratamento de dado necessário à execução de políticas públicas de segurança.

25. (ANTONIO PIVA)

O que isso significa? (Paula Rodovalho) O artigo prevê que a lei não se aplica, para os casos de tratamento de dados pessoais para fins de segurança pública e atividades de investigação e repressão de infrações penais. Assim, não estariam sujeitas às regulações da LGPD pelo argumento de que o projeto seria segurança pública.

26. (PAULA RODOVALHO)

Mas, não podemos nos esquecer de que apesar do artigo excepcionar a aplicação da lei quando os dados coletados forem utilizados para fins de segurança pública, há um certo perigo nessa abrangência por 2 motivos.

27. (PAULA RODOVALHO)

Primeiro, há um risco de as empresas que vencerem a licitação utilizarem as informações e os dados para outros fins. A implementação do projeto abrira margem para apropriações indevidas dos dados dos usuários do metrô. A LGPD não pode ser de toda descartada nesses casos de segurança pública, portanto.

28. (PAULA RODOVALHO)

Segundo, nem tudo é segurança pública. E no caso concreto não é mesmo. A própria Metropolitana afirmou, em sede do procedimento judicial comentado, que esses casos em que haveria uso do reconhecimento facial seriam muito excepcionais. Assim, a segurança pública é um pequeno detalhe que compõe o projeto para excepcionar a aplicação da LGPD.

29. (BEATRIZ BACCARO)

Concordo com você, Paula. Não podemos nos deixar levar por tal leviandade e permitir que qualquer projeto seja feito utilizando essa justificativa, muitas vezes abordada genericamente, como é o caso, para fugir da rigorosidade da LGPD. Inclusive, para esse tipo de situação, já há um projeto de LGPD Penal que busca regular o uso dessas tecnologias

na área de segurança para que os projetos não passem com argumentos genéricos de segurança pública e investigação criminal. Também, a LGPD prevê que, mesmo em casos excepcionais (parágrafo 1º do art. 4º), o tratamento de dados pessoais deverá respeitar 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. A Companhia Metropolitana não informou como vai cumprir com essas condições...

30. (PAULA RODOVALHO)
Sim, exatamente. Continuando, acho que a segunda grande questão polêmica a respeito da finalidade está no fato de que esse projeto está sendo implementado no metrô.

31. (ANTONIO PIVA)
Nos conte, Paula, o que faz do metrô a melhor opção para se implantar esse sistema, ainda que estivéssemos falando de segurança pública?

32. (PAULA RODOVALHO)
Nada. Não há motivo concreto e suficiente para justificar tal escolha. Pelo contrário, os efeitos colaterais são intensos. O fato de que as empresas que administram o transporte público em SP não possuem competência para utilizar e gerir tais sistemas para tais fins, já que a segurança pública é exercida pelos órgãos de polícia (CF, art 144), já é um primeiro ponto problemático. Ou ainda, o fato de o metrô envolver a prestação de um serviço essencial, entrando na discussão, portanto, questões de consumo e proporcionalidade.

33. (ANTONIO PIVA)
Bom, então podemos brevemente concluir com a questão da finalidade que o reconhecimento facial por si só e, ainda, no metrô, não é a medida mais adequada para o fim que se procura.

34. (PAULA RODOVALHO)
Exato, Antonio. É uma medida ineficiente em duplo sentido: finalístico e técnico. Não é a melhor opção para fins de segurança pública por ser em um ambiente em que não faz sentido falar em segurança pública. Ademais, não estamos falando de segurança pública, pois ela está sendo utilizada apenas para excepcionar a aplicação da lei.

35. (PAULA RODOVALHO)
Ainda que estivéssemos falando de segurança pública e o metrô fosse uma ótima opção, o projeto não é adequado por estar rodeado de muitas dúvidas e inconsistências ainda.

Isso inclusive é reiteradamente analisado no mundo privado, em que o reconhecimento facial gera receio, apesar de sua utilização abastada, por estas razões de inconsistência, principalmente da tecnologia e também, pensando na privacidade e outros direitos atingidos dos indivíduos. Pensando em segurança pública, com viés vinculado à esfera penal, nos parece ainda mais problemático adotar tecnologia existindo dúvidas em relação a sua segurança, utilização e precisão. Se na esfera privada obstáculos já atrapalham sua expansão e utilização, por que na esfera pública e nas áreas envolvidas seria uma boa ideia?

2.2. QUESTÃO DA PROPORCIONALIDADE E NECESSIDADE

36. (BEATRIZ BACCARO)
E além do debate a respeito da finalidade e essa questão de adequação do projeto, também há uma discussão a respeito da proporcionalidade dele em relação ao reconhecimento facial.

37. (BEATRIZ BACCARO)
Digo isso porque a utilização de sistemas de reconhecimento facial, mesmo com o cumprimento das recomendações de boas práticas, implica riscos a direitos fundamentais. Assim, antes de implementar qualquer sistema de videomonitoramento, a empresa, ou órgão público, deve avaliar se se trata da única forma de atingir seus objetivos, em respeito ao princípio da proporcionalidade. No caso de haver outras soluções menos invasivas e com menores riscos, elas devem ser adotadas.

38. (BEATRIZ BACCARO)
As eventuais transformações positivas e os benefícios que poderiam ser trazidos com o sistema de reconhecimento facial, como a identificação de criminosos e busca de pessoas desaparecidas, não podem anular alguns riscos como o (i) cerceamento de direitos e liberdades individuais, (ii) o mau uso dos dados coletados, para fins diversos daqueles pretendidos inicialmente pelo agente coletor, e (iii) o risco de vazamento em grande escala, entre outros.

39. (BEATRIZ BACCARO)
Pelo contrário, os riscos se mostram tão grandes em comparação aos possíveis benefícios que o teste de proporcionalidade fica até fácil de ser feito.

40. (ANTONIO PIVA)
E quais são esses riscos, Bia?

A. (BEATRIZ BACCARO)
Em primeiro lugar, o abuso de direitos e controle: se mal utilizada, essa tecnologia de reconhecimento facial pode servir como uma ferramenta poderosa de controle e pode acarretar em práticas abusivas, discriminatórias e em invasão da privacidade do indivíduo.

B. (BEATRIZ BACCARO)
Em seguida, os riscos potenciais a direitos fundamentais: risco de uma vigilância em

massa, criação de uma cidade permanentemente vigiada, no estilo 1984 de George Orwell, na qual seus residentes são continuamente controlados, impedidos, na prática, de exercer o anonimato e a privacidade.

I. (BEATRIZ BACCARO)

É nesse mesmo sentido que, alarmados com a iminente invasão de privacidade, protestantes anti-governo de Hong Kong, contestaram a instalação de câmeras e sistemas de reconhecimento facial pelo governo em postes inteligentes pelo território chinês. Os protestos começaram em agosto de 2019 e os manifestantes reclamavam que essa tecnologia poderia ser usada pelas autoridades chinesas para fomentar uma vigilância em massa, prejudicando assim, a democracia, o direito à proteção de dados e a privacidade individual. Os protestantes destruíram torres que contavam com essas câmeras e alegaram abuso de direitos por parte das autoridades do governo.

C. (PAULA RODOVALHO)

Também tem o risco de dicriminacão: é necessário se atentar ao viés algorítmico - que é a reprodução de padrões discriminatórios resultado de um processo de "machine learning" -, desses sistemas de reconhecimento facial que levam a práticas preconceituosas e discriminatórias nas quais as ferramentas tecnológicas reproduzem estereótipos nocivos de gênero e raça.

I. (PAULA RODOVALHO)

Dessa forma, apesar de se apresentarem como objetiva e imparcial, a tecnologia de reconhecimento facial parte de um algoritmo que ainda é alimentado por indivíduos repletos de valores culturais, sociais e pessoais que faz dessa neutralidade uma tão sonhada utopia. Nesse sentido, é evidente como questões de identidade, nacionalidade, preconceitos e outras tantas dinâmicas de poder influenciam no processo de desenvolvimento da tecnologia, como é o caso absurdo do Google Fotos que marcava pessoas negras nas imagens como gorilas. Isso ocorreu uma vez que a máquina foi alimentada com mais fotos de pessoas brancas e, dessa forma, demonstrava uma dificuldade maior em reconhecer imagens de pessoas de pele escura.

II. (BEATRIZ BACCARO)

Exatamente. Ainda, os riscos à privacidade: a utilização e o descumprimento a finalidadede da coleta de dados pessoais sensíveis como gênero, sexo e idade, pode representar uma violação a privacidade dos indivíduos.

D. (BEATRIZ BACCARO)

Ademais, a falha de segurança: um ponto que requer grande atenção é a segurança e armazenamento desses dados pessoais, uma vez que por envolver dados biométricos sensíveis imutáveis as consequências de potenciais vazamentos são bem maiores. Além disso, os dados biométricos recebem tratamento especial por lei, exatamente por que oferecem riscos elevados à proteção à privacidade dos indivíduos, fato esse que deve ser considerado no teste de proporcionalidade.

I. (BEATRIZ BACCARO)

Dessa forma, ao contrário de uma senha ou endereço de email, o indivíduo não pode mudar sua face, daí a preocupação com a garantia de segurança dessa tecnologia. Essa é uma questão técnica exigida pela LGPD uma vez que o tratamento de dados pessoais deve observar a boa-fé e os princípios listados pela lei em seu art.6º,

II. (BEATRIZ BACCARO)

É preciso fazer as seguintes perguntas: por quem será feito o tratamento desses dados? Quem terá acesso a esses dados sensíveis? Sobre quem iria recair a responsabilidade por um possível vazamento? Acompanhamos estarrecidos, recentemente o maior vazamento de dados cadastrais do Brasil, foram 223 milhões de dados pessoais vazados, e se esse vazamento fosse com as caras dos cidadãos?

41. (PAULA RODOVALHO)

Tendo todas essas problemáticas em vista, as empresas que pretendem instalar essa tecnologia devem tanto observar os possíveis riscos que você trouxe, como atentar-se aos princípios da legislação aplicável. Devem fazer um teste de proporcionalidade para constatar se a finalidade da coleta está sendo respeitada, se há medidas de responsabilização e prestação de contas e se os riscos da implementação não superam os benefícios.

42. (BEATRIZ BACCARO)

Exatamente. Dessa forma, a fim de analisar o embate “Riscos vs Benefícios” que essa tecnologia enseja, esses sistemas devem ser orientados conforme os princípios previstos na LGPD, como a finalidade, a necessidade, a transparência, a segurança da informação e a não discriminação.

A. (BEATRIZ BACCARO)

A finalidade é posta em relação às razões que conduzem o tratamento de dados pes-

soais. Essas razões devem ser sempre legítimas, específicas e explícitas. É necessário que os sistemas de reconhecimento facial justifiquem claramente qual a finalidade do tratamento desses dados.

B. (BEATRIZ BACCARO)

A necessidade diz respeito ao uso que se pretende fazer dos dados coletados. É preciso garantir que o tratamento e uso dos dados seja limitado à estrita necessidade do agente coletor, sem desvio de finalidade. Faz-se necessário determinar quais são os limites impostos aos sistemas de reconhecimento facial e os protocolos de uso desses sistemas.

C. (BEATRIZ BACCARO)

A transparência busca garantir que todas as informações sejam precisas, completas, claras e de fácil acesso pelos cidadãos. Conforme esse princípio, é preciso que os titulares dos dados sejam informados a respeito do tratamento de seus dados pessoais, a forma de tratamento, as finalidades para as quais esses dados são tratados, o prazo e as condições de armazenamento, as medidas de segurança adotadas para sua proteção e por fim, as hipóteses em que podem ser compartilhados a terceiros. Falando especificamente de transparência pública, também é essencial que as empresas implementadoras de sistemas de reconhecimento facial disponibilizem quais são as medidas de controle, responsabilização (accountability) e quais as autoridades competentes.

I. (BEATRIZ BACCARO)

Para que seja garantido o direito do acesso à informação, é preciso que na entrada dos estabelecimentos, sejam disponibilizados vários alertas indicando o uso dessa tecnologia de videomonitoramento para que os titulares tenham a capacidade de exercer o consentimento e tomar decisões conscientes sobre o uso de seus dados biométricos.

II. (ANTONIO PIVA)

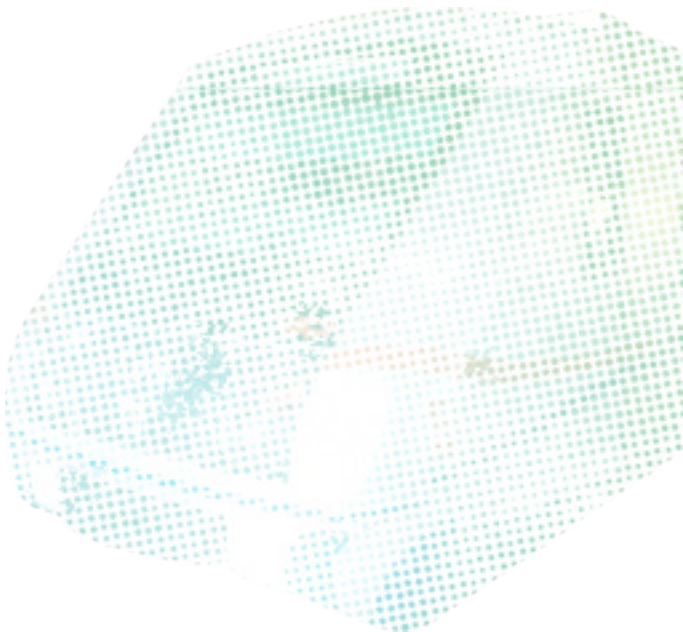
Aqui é necessário fazer um adendo, pois conforme a análise da proporcionalidade, vê-se que o metrô é um serviço público essencial, na medida em que, o transporte público é um direito social inerente ao cidadão. Assim, é essencial dar ao usuário a capacidade de fornecer seu consentimento sobre sua privacidade: ou ele se sujeita à tecnologia para utilizar o metrô ou, ao escolher não abrir mão de sua privacidade, fica impedido de andar no transporte público. Ou seja, condiciona um anula o outro.

D. (BEATRIZ BACCARO)

Continuando, a segurança da informação garante que o tratamento de dados pessoais seja feito conforme padrões de segurança e confidencialidade de modo a evitar a perda, destruição e vazamento de dados. Faz-se necessário criar um conjunto de medidas técnicas capazes de garantir a proteção dos dados coletados pelos sistemas de reconhecimento facial. É preciso que haja disposições expressas acerca de como ocorre a coleta, o tratamento e sobre o período de retenção dos dados pelo sistema.

E. (BEATRIZ BACCARO)

Ademais, o princípio da não-discriminação visa garantir que nenhum tratamento de dados seja realizado com fins discriminatórios segundo critérios de gêreno, origem racial, orientação sexual, posicionamento político e religioso etc. Os sistemas de reconhecimento facial devem criar mecanismos capazes de evitar qualquer viés social no tratamento de dados pessoais e de criar avaliações de impacto social desses sistemas.



2.3. DIREITOS DOS USUÁRIOS

43. (ANTONIO PIVA)

Dentre toda essa complexidade, será que alguém já se questionou sobre quais são seus direitos não simplesmente como cidadão, mas especificamente como usuário do transporte público? Isso implica em alguma coisa no projeto?

44. (PAULA RODOVALHO)

Por se tratar de um projeto no metrô, ainda restam alguns obstáculos para implantação do sistema de reconhecimento facial nesse ambiente, principalmente por ser a relação usuário e Companhia Metropolitana, uma relação de consumo. 3 questões podem ser levantadas nesse sentido

45. (PAULA RODOVALHO)

A primeira delas seria em relação à proteção do usuário frente à tecnologia de reconhecimento facial.

46. (PAULA RODOVALHO)

Tanto a lei Federal, quanto a Estadual garantem a proteção e defesa de direitos dos usuários de serviços públicos e prevêem, que a qualidade da prestação do serviço público deve observar adequação entre meios e fins, sendo vedada a imposição de obrigações ou restrições não previstas em lei, como existe no sistema de vigilância proposto.

47. (PAULA RODOVALHO)

Ainda, apesar de não existir um Código de Usuário do Metrô, por exemplo, que unifique tudo, tendo cada estação de seu próprio ato normativo de criação, quando falamos em seguridade toda política pública de segurança tem duas finalidades: a segurança do usuário e o zelo pelo patrimônio público. Para além dessa regulação "interna" ao serviço público, ainda há a Lei 13.460/17 e a Lei 12.527/11. Em ambas, há uma constelação de direitos e princípios que o usuário de serviços públicos - o direito de acesso à informação e demais direitos.

48. (PAULA RODOVALHO)

A dúvida que fica é: o uso da tecnologia de reconhecimento facial protege a quem, se aparentemente viola, ou no mínimo não assegura, todos os interesses do usuário das normas legais existentes sobre o metrô?

49. (ANTONIO PIVA)

E tem também a questão a respeito da transparência.

50. (ANTONIO PIVA)

Você sabe quais são os dispositivos que coletam sua imagem? Quais os dados que são coletados? Como eles fazem o rastreamento de identificação? Como e onde que estes dados são armazenados - nuvem? Como que estes dados são protegidos? Quem tem a propriedade destes dados? Quem tem acesso e com quem eles são compartilhados? Quais são seus riscos?

51. (ANTONIO PIVA)

Se você ouvinte, no começo deste PodCast, sequer sabia que seu rosto poderia ser escaneado, provavelmente não têm a mínima ideia das respostas. E, ao que parece, nem as autoridades. Em nenhum site, em documento algum são divulgadas as informações acima.

52. (ANTONIO PIVA)

Como visto, um dos maiores princípios da LGDP é a transparência, e só com o que foi descrito agora já percebemos que a política pública não se adequa. O poder público deve informar o usuário, disponibilizando todos os dados acima. Mas saiba que, depois de tudo que trabalhamos aqui, existem meios para tentar adquirir todas essas informações, como por exemplo, realizar pedidos junto ao sistema de Acesso à Informação, utilizar as ferramentas de feedback que o próprio metrô disponibiliza para mostrar insatisfação...o caminho é, sem dúvidas, a união do todo, pensando enquanto coletividade.

53. (BEATRIZ BACCARO)

E ainda tem um último ponto nessa relação metrô e usuário que pode ser levantada. Accountability, já ouviu falar? Não há uma tradução literal, talvez a mais próxima seja: prestar contas, mas é a necessidade de o Estado prestar conta para você, cidadão. Não é opção, é dever. Cada um que nos ouve deve terminar esse PodCast, essencialmente, com uma certeza: o Estado não é superior ao cidadão, ele presta, apenas, um serviço a todos e deve prestar contas, sim. Não há que temer o Estado, há que se questionar - pelos meios legítimos - suas ações e coibir abusos. A coibição começa com pequenas ações, como, por exemplo, questionar-se: o Estado tem a permissão de vigiar? Você tem o direito de não ser controlado?

54. (BEATRIZ BACCARO)

O papel do Estado, em segurança, perpassa dois objetos centrais: a prevenção e punição

- antes e depois do delito. A legislação vigente é muito clara em estabelecer limites para o Estado, seja pela garantia de direitos, seja por vedações expressas.

55. (BEATRIZ BACCARO)

Pergunte-se: o uso do reconhecimento facial está em que campo? Ele, na plataforma da estação, vai coibir o delito? Em teoria, não. O sistema é nutrido por fotografias e o processo de machine learning irá reconhecer, buscar nos rostos em multidão, àqueles pontos específicos, de poucas pessoas. Os dados de todos são coletados, mas imagine revisitar todos os dados de todas as pessoas que passam pela estação da Sé em horário de pico - em virtude de um roubo ou furto? Inviável. E mesmo em viabilidade, como já abordamos no tópico sobre proporcionalidade, o uso e armazenamento dos dados faciais não pode se justificar por argumento tão simples, ainda mais, se considerado que há outros meios para exercer este controle e rastreamento de delituosos - como o uso das câmeras convencionais.

56. (BEATRIZ BACCARO)

Então chegamos no ponto correto: o uso do reconhecimento auxilia a punição. Fotografias de investigados, réus e condenados abastecem o sistema, para serem identificados. O Estado tem o poder de punir, mas pode ele invadir a privacidade dos dados de milhões de pessoas diariamente? Seu rosto, sua rota, quem lhe acompanha, seu horário - tudo na mão do Estado, sem qualquer certeza de conformidade com a LGPD. Qual a diferença de um sistema que controla sua localização pelo seu tornozelo para um sistema que controla sua localização no metrô por meio do seu rosto? Lembrando que um é entendido juridicamente enquanto cautelar penal e outro como política pública.

57. (BEATRIZ BACCARO)

Percebe o desequilíbrio?

58. (ANTONIO PIVA)

E mais do que isso: que tipo de Estado estamos tratando? Claramente há vedações normativas, em vários âmbitos e em vários segmentos - seja na CF/88, seja na Lei de Acesso à Informação e LGPD - e mesmo assim este PodCast mostra-se necessário. O que se assiste aqui, de camarote (infelizmente) é uma deturpação da lógica social para com o Estado. O Estado serve ao povo e controlá-lo, como em utopias literárias, ultrapassa o limite daquilo que o pacto social criou em primeiro lugar: o Estado deve garantir a paz social e ela apenas. Enquanto houver meios para garanti-la sem restringir a liberdade dos cidadãos, assim deverá ser. Infelizmente, o Estado brasileiro tem agido como totalitário, apesar de tudo já vivido.

2.4. CAUTELAR

59. (PAULA RODOVALHO)

A respeito de todos esses problemas apresentados no projeto do metrô de São Paulo, foi iniciado um procedimento judicial, como citamos algumas vezes, em formato de cautelar em que requisitou-se pela produção antecipada de provas contra a Companhia Metropolitana de São Paulo (Metrô) a respeito do projeto.

60. (PAULA RODOVALHO)

A ação foi conduzida pelas Defensorias Públicas do Estado de São Paulo e da União, pelo IDEC (instituto brasileiro de defesa do consumidor), pelo INTERVOZES (coletivo Brasil de comunicação social) e pelo ARTIGO 19 BRASIL. As organizações de defesa de direitos pretendiam obter, com a produção de provas, a delimitação do alcance, finalidade, cautela e limites do campo de dados da tecnologia que seria implantada no projeto, obtendo, assim, uma justificativa para uma futura ação judicial.

61. (PAULA RODOVALHO)

O edital da licitação para concepção desse sistema não fornecia um detalhamento técnico da tecnologia, mas apenas demonstrava a intenção de implementação de sistema de reconhecimento facial com capacidade de armazenar dados pessoais.

62. (PAULA RODOVALHO)

O que é evidente é que, atualmente, não há informações suficientes a respeito do uso ou armazenamento dos dados coletados pelas câmeras de reconhecimento facial, dificultando ainda mais o trabalho de quem estuda os impactos dessa tecnologia.

63. (BEATRIZ BACCARO)

Sim, Paula. Ainda, a ação cautelar também identificou o potencial de violação do direito à privacidade de todos os usuários do metrô, já notificado previamente pelo IDEC à Companhia Metropolitana, como falamos agora há pouco,

64. (BEATRIZ BACCARO)

A ação também se atenta ao potencial lesivo na relação usuário e serviço público, sobretudo, considerando o desrespeito ao Código de Proteção e Defesa do Usuário do Serviço Público do Estado de São Paulo (Lei Estadual 10.294/1999); ao Código de Defesa do Usuário dos Serviços Públicos (Lei Federal 13.460/2017); e ao Código de Defesa do Consumidor (Lei Federal n. 8.078/1990).

65. (PAULA RODOVALHO)

Como dito, as leis prevêem que a qualidade da prestação do serviço público deverá observar adequação entre meios e fins, sendo explicitamente vedada a imposição de obrigações ou restrições não previstas em lei - respeitando o princípio da legalidade. O que se observou na ação é que a falta de transparência somada aos abusos da tecnologia pela prestadora de serviço são ofensas diretas aos direitos dos usuários.

66. (PAULA RODOVALHO)

Devemos entender também que apenas o fato de saber que está sendo filmado, sinalizado por placas, não é mais suficiente, sobretudo com o uso dessas tecnologias e a LGPD. O tratamento desses dados pessoais é uma questão extremamente relevante. O potencial lesivo disso foi reconhecido nesta cautelar mas, infelizmente, não se sabe ao certo sua extensão.

67. (ANTONIO PIVA)

Também foi abordado o direito de crianças e adolescentes na ação, não?

68. (BEATRIZ BACCARO)

Sim. O direito à imagem e privacidade são expressamente garantidos pelo Art. 100 do ECA, sendo reforçados pela LGPD - que exige um consentimento expresso para o tratamento de dados de crianças e adolescentes.

69. (BEATRIZ BACCARO)

Por essa e as demais razões, foi levantada como de extrema importância a produção de provas, das quais poderão ser extraídas informações que identifiquem o real alcance do sistema de reconhecimento facial e a extensão de seus potenciais danos. Aqui fica evidente a importância desta cautelar e seu potencial para o futuro das ações contra o uso do reconhecimento facial.

70. (ANTONIO PIVA)

Fora do âmbito do direito, em que ações judiciais são o meio para atingir o objetivo de impedir o uso de sistemas de reconhecimento facial em massa, além da própria lei que orienta a conduta de atores privados e públicos, também existem ideias criativas sendo colocadas em prática para mostrar a indignação da população com o sistema, como a utilização de máscaras e óculos nos transportes, a fim de evitar o reconhecimento, ou manifestações, como aconteceram recorrentemente em Hong Kong onde quebraram câmeras de vigilância.

3. CONCLUSÃO

71. (ANTONIO PIVA)
No final das contas, o que devemos fazer? Pode ou não usar o reconhecimento facial?

72. (PAULA RODOVALHO)
Existem 2 caminhos possíveis para a questão do reconhecimento facial: (i) garantir procedimentos, que seria o que se tem sido exigido da Companhia Metropolitana até agora no que tange à produção de provas, documentos, entre outros que detalham todo o uso da tecnologia, como bem fizeram os agentes responsáveis pela ação; ou (ii) explorar banimentos.

73. (ANTONIO PIVA)
Qual é a melhor alternativa?

74. (PAULA RODOVALHO)
Tendo em vista a crescente tendência internacional ao banimento dessa tecnologia, como em São Francisco, na Califórnia, onde agências do governo baniram o uso de sistemas de reconhecimento facial por considerarem essa tecnologia consideravelmente violadora de direitos e liberdades individuais, vê-se que a melhor e mais eficaz forma de proteger os indivíduos contra essas violações é o banimento.

75. (PAULA RODOVALHO)
É necessário entender que mesmo tendo bons procedimentos e seguindo todas as recomendações de boas práticas, os sistemas de reconhecimento facial vão sempre ser uma tecnologia de alto risco, justamente por utilizarem de dados extremamente sensíveis dos indivíduos.

76. (PAULA RODOVALHO)
Dessa forma, há de se considerar que os benefícios trazidos por esse mecanismo de reconhecimento facial, poucas vezes superam os riscos iminentes de violação a direitos fundamentais, como a privacidade e a proteção de dados pessoais. Além disso, a liberdade dos cidadãos é colocada em xeque principalmente quando se trata do uso de reconhecimento facial pelo setor público em serviços de caráter essencial, como no metrô, onde o poder de escolha do indivíduo é posto de lado.

77. (ANTONIO PIVA)
E o que o usuário, pensando nos nossos ouvintes, pode fazer? Para além do que está ao

alcance dos juristas, como podem contribuir para impedir esse tipo de violação à privacidade a qual querem sujeitá-lo?

78. (BEATRIZ BACCARO)
Além de manifestações, existem outros caminhos que podem ser seguidos que tanto amenizem os efeitos colaterais de uma possível implantação, como também auxiliem na luta pelo banimento.

79. (BEATRIZ BACCARO)
Como já mencionado, um primeiro caminho a ser seguido é a de requerer que o metrô e a empresa responsável pela tecnologia, no presente caso a Engie Ineo Johnson, prestem informações relativas aos dados coletados, seguindo os princípios da LGPD. Mesmo se tratando de segurança pública, na qual haveria uma excepcionalidade à mencionada lei, o direito à privacidade não pode ser totalmente tolido em nome de segurança pública, existindo, portanto, essa possibilidade de exigência.

80. (BEATRIZ BACCARO)
Outra alternativa, e talvez a que realmente acarrete em um banimento desses sistemas de reconhecimento facial, ainda mais no setor público, é a de propor uma ação individual requerendo que sua face seja preservada do alcance da tecnologia de reconhecimento. Em outras palavras, dizer que não quer ser filmado, por todos os argumentos aqui já expostos. Como não há como deixar de filmar uma só pessoa, a Companhia Metropolitana e a Engie Ineo Johnson teriam um problema, principalmente técnico, que acabaria impedindo que fosse filmada qualquer pessoa. Assim, preferível será a discussão no sentido de banimento dessa tecnologia, sob risco de adentrarmos uma era de fim do direito à privacidade, na qual ao contrário de segurança, encontremos abuso de poder, espionagem e, principalmente, medo.

81. (ANTONIO PIVA)
Excelente. Chegamos ao final do podcast. Mas se você, ouvinte, quiser saber mais sobre reconhecimento facial, proteção de dados e direitos do consumidor, acesse as plataformas do IDEC e do Data Privacy Brasil. Agradecemos pela atenção e até a próxima!