GEYSA CAMARA

DO RECONHECIMENTO FACIAL

ESTUDO EXPLORATÓRIO E ANÁLISE COMPARATIVA ENTRE BRASIL E PORTUGAL

Dissertação com vista à obtenção do grau de
Mestre em Direito e Segurança.

Orientador:
Professor Doutor José Fontes

Julho 2021

GEYSA CAMARA

DO RECONHECIMENTO FACIAL

ESTUDO EXPLORATÓRIO E ANÁLISE COMPARATIVA ENTRE BRASIL E PORTUGAL

Dissertação com vista à obtenção do grau de
Mestre em Direito e Segurança.

Orientador:
Professor Doutor José Fontes

Julho 2021

DO RECONHECIMENTO FACIAL

ESTUDO EXPLORATÓRIO E ANÁLISE COMPARATIVA ENTRE BRASIL E PORTUGAL

GEYSA CAMARA

JULHO 2021

DECLARAÇÃO ANTIPLÁGIO

Declaro por minha honra que o trabalho que apresento é original e que todas as citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui grave falta ética e disciplinar.

Lisboa, 09 de Julho de 2021.

DECLARAÇÃO DE CONFORMIDADE DE NÚMERO DE CARACTERES

O corpo da dissertação, incluindo espaços e notas, ocupa um total de 277.548 caracteres.

DEDICATÓRIA

Dedico este trabalho a quem me ensinou a ser forte como a raiz de uma árvore, a quem, devido às circunstâncias do último ano, não foi possível me despedir.

Dedico este trabalho a minha mãe, Leda Camara, *in memoriam.*

AGRADECIMENTOS

Agradeço primeiramente a Universidade Nova de Lisboa por todo acolhimento e atenção durante o percurso acadêmico.

Agradeço ao meu orientador Professor Doutor José Fontes, pela paciência e disponibilidade durante o período difícil de estudos e pesquisa.

Por fim, ao meu esposo e minha irmã, meus maiores incentivadores, minha gratidão.

LISTA DE ABREVIATURAS

ABIS	*Automated Biometric Identification System* - Sistema Automatizado de Identificação Biométrica
AFIS	*Automated Finge Print Identification System* - Sistema de Identificação de Impressões Digitais
AIPD	Avaliação de Impacto sobre Proteção de Dados
ART	Artigo
CCVT	*Closed Circuit Television*
CHS	Comissão de Segurança Humana
CNPD	Comissão Nacional de Proteção de Dados
CRFB	Constituição da República Federativa do Brasil
CRP	Constituição da República Portuguesa
EU	União Europeia
IA	Inteligência Artificial
LDN	Lei de Defesa Nacional
LGPD	Lei Geral de Proteção de Dados
ONU	Organização das Nações Unidas
PSP	Polícia de Segurança Pública
RGPD	Regulamento Geral de Proteção de Dados
RIPD	Relatório de Impacto e Proteção de Dados
STF	Supremo Tribunal Federal

LISTA DE FIGURAS

RESUMO

Esta dissertação empenha-se em realizar um estudo exploratório com dimensões e componentes comparativas sobre a regulação do reconhecimento facial e o grau de maturidade dos ordenamentos jurídicos de Brasil e Portugal, considerando sua utilização para fins de segurança e o binômio da segurança e privacidade. Como é notória a utilização do reconhecimento facial cresce a cada dia e já está entranhado nos mais variados setores da sociedade e não é diferente na área de segurança, onde se consolida como importante aliado. Contudo, considerando os riscos e reflexos diretos a direitos fundamentais e que sua utilização tem por base o tratamento de dados biométricos e estes, via de regra, são proibidos ou mesmo condicionados por exceções legais previstas nas legislações de proteção de dados, esta investigação terá por base analisar conceitos e enquadramentos basilares em cada ordenamento jurídico, assim como explorar e verificar se há instrumentos legais sobre o assunto, tendo em conta que toda a temática que envolve a utilização da tecnologia de reconhecimento facial é extremante mutável e não comporta uma perspectiva exaustiva.

Palavras-chave: Reconhecimento Facial. Segurança. Privacidade. Brasil. Portugal.

ABSTRACT

This dissertation endeavors to carry out an exploratory study with dimensions and comparative components on the regulation of facial recognition and the degree of maturity of the legal systems of Brazil and Portugal, considering it is use for security purposes and the binomial of security and privacy. As it is popular, the use of facial recognition grows every day and is already ingrained in the most varied sectors of society and it is not different in security area, where is consolidated as an important ally. However, considering the risks and direct reflexes to fundamental rights and that their use is based on the processing of biometric data and these, as a rule, are prohibited or even conditioned by legal exceptions provided for in data protection legislation, this investigation will be based on basic concepts and frameworks in each legal system, as well as exploring and checking if there area legal instruments on the subject, taking into account that the whole theme that involves the use of facial recognition technology is extremely changeable and does not include an exhaustive perspective.

Keywords: Facial Recognition. Security. Privacy. Brazil. Portugal

SUMÁRIO

INTRODUÇÃO

É notório que a tecnologia de reconhecimento facial vem sendo utilizada cada vez mais. Em um curto espaço de tempo, como tudo nesta nova sociedade de informação, se desenvolveu rapidamente.

O mais intrigante desta tecnologia é o seu alcance. Os cenários de atuação são vastos e, apesar dos desafios que o cercam, não é possível imaginar seu desuso em face do tempo, pelo contrário, a gama de possibilidades, inovações e aplicações, seja na esfera privada ou pública aumentam exponencialmente a cada dia.

Em uma sociedade cujo problema da segurança aflora em larga escala, sendo o tema do século, o reconhecimento facial vem se consolidando como importante ferramenta na área de segurança. Contudo, há problemas reais como, por exemplo, contaminação de algoritmos, perfilhamentos, monitoramento massivo da população e muitas outras controvérsias sobre o real impacto desta tecnologia em direitos fundamentais.

Soma-se a isto o fato da tecnologia ter por base a utilização de dados biométricos, que via de regra tem o tratamento proibido ou condicionado a certas exceções legais que deverão por sua vez observar a finalidade estrita, proporcionalidade e adequação.

Ocorre que as leis de proteção de dados, apesar de se constituírem como instrumentos regulatórios importantes não se aplicam para fins de segurança, devendo esta área ser necessariamente regida por atos e leis específicos[1].

Assim, considerando o avanço da utilização de ferramentas de reconhecimento facial surgem as indagações que subsidiaram esta investigação: Como se dá a regulação do reconhecimento facial para fins de segurança no Brasil e em Portugal, há legislação específica? Em caso positivo, é eficaz? Em caso negativo, se inexistir legislação específica, qual o grau de maturidade dos ordenamentos jurídicos em questão para permitir a utilização da tecnologia de reconhecimento facial?

Portanto, buscando responder a estas indagações este trabalho visa, de modo exploratório e através de componentes comparativos, analisar a regulação do reconhecimento facial para fins de segurança, tendo por base as premissas básicas de segurança e privacidade.

Para tanto iremos concentrar esforços no ordenamento jurídico português e, consequentemente, por ser Estado-Membro da União Europeia, em alguns instrumentos regulatórios que são comunitários para os fins de proteção de dados e segurança, como por

[1] Conforme Art. 4º da LGPD e Art. 9º do RGPD.

exemplo o Regulamento Geral de Proteção de Dados e a Diretiva UE 2016/680, pois como veremos mais adiante são fontes relevantes no cenário brasileiro.

Analisaremos também o ordenamento jurídico brasileiro, buscando verificar a existência de leis específicas cuja intenção, validade e eficácia serão verificadas no decorrer deste trabalho.

De forma geral o objetivo desse trabalho é desenvolver um modelo exploratório, sob um viés comparativo acerca dos instrumentos de regulação do reconhecimento facial, tendo por base o binômio segurança e privacidade no ordenamento luso brasileiro, bem como tentará auferir o grau de maturidade destes ordenamentos jurídicos para lidar com esta temática.

A escolha do tema se justifica pela atualidade do mesmo e sua projeção para o futuro, bem como seu impacto nos direitos fundamentais e riscos envolvidos. Cumpre salientar que o presente trabalho não tem intenção de delimitar ou por fim a discussão, até mesmo porque seria impossível, visto que o tema está em constante mutação.

Diante disto, a delimitação deste estudo exploratório será realizada em três capítulos: Segurança, Privacidade e Reconhecimento Facial.

No 1º capítulo iremos observar como o conceito de segurança se tornou amplo e complexo e apesar de ser holístico ainda é a função primeira do Estado. Conjugamos também a este capítulo a importante abordagem das novas aceções da segurança e segurança humana, bem como discorreremos sobre a segurança como direito fundamental. Ao longo dos tópicos será possível verificar como a segurança se apresenta em cada ordenamento jurídico objeto deste estudo face às menções legais e comparativas realizadas.

Com o 2º capítulo adentramos na ceara da privacidade, buscando clarificar este conceito que é elástico, bem como sua evolução até a sociedade de informação. Abordaremos novamente do ponto de vista exploratório e com alguns componentes comparativos, a sua apresentação em cada ordenamento jurídico. Dedicaremos especial atenção à proteção de dados, uma vez que está se consagrou como direito fundamental e também por ser o dado biométrico ponto fulcral para as tecnologias de reconhecimento facial.

No 3º capítulo buscamos desmistificar o reconhecimento facial através de suas finalidades, assim como de forma não exaustiva buscaremos uma melhor percepção sobre os riscos envolvidos e os mais diversos cenários de utilização. Iremos também de forma exploratória levantar e analisar os instrumentos regulatórios, caso existam, com vistas a responder os questionamentos realizados.

Por fim, aspiramos que este estudo exploratório possibilite novas perspectivas e sirva de inspiração para continuar a investigação, afinal sendo um tema extremamente novo e mutável e, à medida que se projeta na sociedade, se faz necessário seu acompanhamento.

1. SEGURANÇA

1.1- UMA VISÃO HOLÍSTICA

Desmistificar o conceito de segurança é uma tarefa que hoje exige uma visão múltipla de Estado, indivíduo, ameaças, sociedade internacional, globalização e bem estar social, por isso, a visão da segurança apresentada neste trabalho foi constituída com base nos brilhantes ensinamentos do Professor Bacelar Gouveia, através de suas aulas ministradas no curso de Mestrado em Direito Segurança, bem como em sua obra, Direito da Segurança, Cidadania, Soberania e Cosmopolitismo.

Pois bem. Muito embora o significado de segurança seja hoje complexo e multiconceitual é correto afirmar que advém de premissas básicas de proteção contra uma ameaça, de se fazer seguro. "O próprio sentido etimológico da palavra segurança, do latim *sine cure*, segurança implica proteção." (GOUVEIA, 2018, p. 89)

Desde os primórdios da civilização a segurança esteve relacionada ao poderio de um sobre outro, poderio bélico de um Estado para frear ameaças e valorizar seu território e soberania, entretanto, esta visão está ultrapassada. Podemos dizer, sem sombra de dúvidas, que segurança, "a partir da ótica de um meio de ação, convoca instrumentos, comportamentos e instituições de índole diversas" mantendo sua aceção mais pura, de segurança como atividade de estar seguro. (SICUREZA, 2011 apud GOUVEIA, 2018, p. 89-90)

A visão estatocentrica da segurança foi evoluindo com o passar do tempo e acontecimentos globais como, por exemplo, as duas grandes Guerras Mundiais, a Guerra Fria e o Atentado de 11 de Setembro. A evolução da própria sociedade deu lugar a um conceito muito mais abrangente e multidisciplinar como nunca antes visto.

Sua polissemia, como assevera Gouveia em sua obra, é tão extensa que vai além do próprio sentido natural da palavra e, apesar do consenso de que assegura a ideia de estar ou sentir-se seguro perante ameaças ou perigos, atualmente apresenta-se como um conceito muito mais robusto e abrangente, contemplando diversas acepções que vem ganhando notoriedade com o próprio desenvolvimento das relações humanas dentro da sociedade pós-moderna. (GOUVEIA, 2018)

Como refere Bacelar Gouveia (2018, p.93), atualmente a "polissemia da palavra segurança extravasa seu ambiente natural e assume múltiplas outras formas, tornando-se um conceito muito mais denso e alargado".

No cenário atual, a absorção do conceito da sociedade de risco mundial difundido por Urick Beck trás a tona novas tipologias de riscos globais, como terrorismo, crime organizado, alterações climáticas, fenômenos econômicos e ecológicos, proliferação de armas de destruição em massa, ciberterrorismo dentre outros, cuja resposta exige uma verdadeira cooperação transacional onde a autonomia nacional dá lugar a uma soberania conjunta e cosmopolita. (URICK BECK, 2015 apud GOUVEIA 2018, p.77-82)

Somam-se a isto os Estados falhados que elevam cada vez mais as preocupações, evidenciando um espectro extremamente mutável que envolve a segurança e novas aceções.

O conceito de segurança passou, portanto, a abarcar diversas aceções, dentre elas o *safety e security*. Ou seja, foi necessário responder aos novos desafios da sociedade que vão além de um sentimento iminente de ameaça física, e que engloba a proteção social e individual como, por exemplo, a segurança humana.

Sobre a mutação do conceito da segurança e de acordo com Carvalho em sua dissertação:

> "Apesar do senso comum e da mídia apontar para um conceito de segurança onde se tenta evitar a violência urbana e o terrorismo, atualmente, entende-se a segurança de maneira muito mais ampla. Limitar a segurança ao receio de ser roubado ou de ter sua integridade física ameaçada é discriminatório, uma vez que se observa apenas o lado daqueles destinatários da segurança que pertencem a grupos sociais mais privilegiados, que tendem a ter esse tipo de preocupação com seu patrimônio e sua vida. Contudo, esse ponto de vista não aborda aqueles grupos mais sensíveis da sociedade que tendem a não se preocupar prioritariamente com patrimônio, mas com outros aspectos de satisfação de suas necessidades humanas, como o desemprego, falta de saneamento básico, doenças, má alimentação e etc." (LUNARDI, [s.d.]) apud CARVALHO, 2020, p. 47)

Cumpre ressaltar que um dos estágios alcançados dentro deste novo horizonte evidenciou-se com o aparecimento de legislações e cooperações internacionais contra as novas ameaças e também com novas formas de prevenção e proteção da sociedade, tendo por base a utilização de novas tecnologias, como por exemplo, o reconhecimento facial. Neste novo cenário podemos perceber que já existe uma discussão sobre aceção digital ou cibernética, afinal a hiperconectividade hoje possibilita bilhões de interações globais por segundo e expõe na mesma medida indivíduos e Estados.

Pois bem. Principalmente no contexto da globalização pós-Guerra Fria e apesar do núcleo manter-se inalterado, é incontestável que houve um alargamento no conceito de segurança e suas dimensões, com inclusão de novos atores e novas ameaças.

A segurança deixou de ser apenas segurança contra ato criminoso, ou como prevenção contra a ameaça direta, sendo alargada tal como apontado por Bacelar Gouveia (2018) em sua obra, quando menciona a existência de um rol exemplificativo que compõe este alargamento e as diversas aceções possíveis: "Segurança econômica, segurança alimentar, segurança ambiental, segurança sanitária, desportiva, segurança do trabalho, segurança do emprego, segurança da escola, segurança no consumo, segurança energética, segurança marítima, segurança aérea, segurança urbanística, segurança bancária, segurança financeira." (GOUVEIA, 2018, p.93-94)

Ainda neste tocante, Gouveia (2018, p.94-95) elenca outras duas importantes aceções: a segurança jurídica, que sob o prisma da proteção da confiança se consolidou como princípio derivado do Estado de Direito, e a segurança social, relacionada à proteção do cidadão enquanto sujeito de direitos diante de riscos sociais oriundos do próprio cotidiano do Estado.

Nesta conjuntura, imperioso destacar também a segurança humana.

A segurança humana passou a ser discutida como uma questão de segurança internacional que é multidisciplinar por natureza, o direito das pessoas tornou-se mais importantes que o direito dos Estados, a segurança humana nasceu, portanto, centrada no ser humano e nos direitos humanos.

As Nações Unidas introduziram este conceito em seu relatório de 1994, do PNDU – Programa das Nações Unidas para o Desenvolvimento, com isto o tradicional conceito centralizado no Estado, a segurança político-estadual foi substituída pela segurança humana, com foco no indivíduo. A discussão central dirigiu-se a para os impactos diretos no dia a dia do ser humano, questões como ter o que comer, desemprego, ameaças sociais, políticas ou econômicas, bem como o tráfico de drogas, degradação ambiental, terrorismo, conflitos étnicos passaram a ter impactos e consequências globais. (HDR, 1994 apud ALENCAR, 2016, p.6)

Bacelar Gouveia (2018) aduz que a Segurança Humana apresenta as seguintes características fundamentais:

> 1) Universalidade: é uma preocupação universal, um valor que deve ser alcançado por todas as pessoas;
> 2) Interdependência: é um propósito que depende das ações individuais de cada país, contudo, ferir a segurança humana em algum local ou região, afeta o direito em termos globais;
> 3) Prevenção: é um propósito que é melhor alcançado através da prevenção, sendo a repressão um método menos eficiente;
> 4) Humanidade: o ser humano é o elemento central desse propósito, assim, todas as ações tomadas no intuito de sua consecução devem objetivar o bem maior ao indivíduo. (GOUVEIA, 2018, p.76)

Este novo conceito de segurança humana como diz Bacelar Gouveia (2018, p.76) é "holístico, quer em termos de *safety*, quer em termos de *security* e representa proteção dos valores fundamentais da Comunidade Internacional e suas novas exigências:"

> "A emergência de direitos humanos determinam que os Estados estão a serviço do seu elemento humano e não o contrário, impondo-se nesta realidade que os verdadeiros bens a proteger, além dos comunitários, possam ser os bens individuais mais relevantes. (...) a sociedade atual caracteriza-se pela necessidade de responder a todos os novos riscos que uma sociedade tecnológica tem vindo a potenciar, protegendo os bens não só sobre a ótica do *security*, mas também do *safety*." (GOUVEIA, 2018, p.76-77)

Concordamos também com Maria Gisélia Castro e Silva (2019) quando aponta em sua dissertação intitulada Segurança Humana, Responsabilidade de Proteger e Direito Internacional, que:

> "Não obstante a sua centralidade no indivíduo, numa dimensão mais estreita (*freedom from fear*) ou mais ampla (*freedom from fear; freedom from want*), a figura do Estado não é relegada nesta forma contemporânea de pensar as questões de segurança. O papel que desempenha é hoje diferente, mas de grande importância. É, de certa forma, mais relevante até neste quadro da Segurança Humana, uma vez que lhe é exigido que sejam os seus maiores promotores, sob pena de serem responsabilizados e penalizados, desde logo pelos seus pares. (SILVA M. G., 2019, p.10)

Bacelar Gouveia (2018, p.96) afirma ainda que o conceito de segurança, ao abarcar o conceito de *safety (freedom from want) e security (freedom from fear),* passou a ter uma dimensão que é supraestadual.

Insta salientar que, sendo a segurança humana o maior e mais importante expoente desta evolução multiconceitual e supraestadual da segurança ela centraliza cada vez mais os debates internacionais.

Nesta ótica, o conceito de segurança busca responder aos novos desafios da sociedade, sob um prisma de proteção estatal, social, humana e também, a nosso sentir, sob um mais novo prisma, o digital e tecnológico, tema este que incendeia as discussões ao redor do globo, principalmente no que pertine ao tema deste trabalho, o binômio segurança e privacidade e a regulação de novas tecnologias, nomeadamente o reconhecimento facial.

Contudo, equilibrar a equação entre os fatores de segurança, liberdades fundamentais e privacidade é cada vez mais difícil no modelo de sociedade atual onde o indivíduo e Estados são cada vez mais dependentes de novas tecnologias; há novas preocupações filiadas a

vertente do ciberespaço, da informação, de dados pessoais e abre-se caminho para novas aceções.

Assim, no que toca a este estudo e, paralelamente ao surgimento destas novas aceções e dos novos riscos, identificamos também novas formas de prevenção, proteção e desenvolvimento da sociedade e do ser humano. Isto inclui, por óbvio, a utilização de novas tecnologias, como, por exemplo, a utilização sistemas de videovigilância e reconhecimento facial, que possibilitam a prevenção de atos criminosos, o combate ao terrorismo e crime organizado transnacional, tornando-se assim importante ferramenta para as forças de segurança.

Fato é que a evolução do conceito de segurança, a concretização da segurança humana e as novas aceções evidenciam que inexiste um conceito universal e globalmente aceito. Contudo, ainda que a segurança sempre esteja relacionada à construção de políticas internas e proteção de uma ameaça, ela se consolida no cenário internacional como mecanismo de maior relevância para o bem estar global, social e humano e, por isto, sempre será holística.

1.2- A SEGURANÇA COMO FUNÇÃO PRIMEIRA

Desde os primórdios, quando a segurança era entendida como uma questão físico-estatal, de poderio militar, até os novos contornos de uma sociedade pós-moderna e de risco, nota-se a intrínseca e poderosa relação entre Estado e Segurança.

Nesta linha de pensamento é possível constatar que existe uma íntima ligação entre Estado e Segurança. A necessidade de o homem sair do seu estado de natureza e se organizar socialmente em prol da sua própria sobrevivência faz do Estado uma estrutura complexa e ao mesmo tempo indispensável para sobrevivência humana. Podemos dizer que a razão de ser do Estado firmou-se ao longo da história como a necessidade de garantia de segurança em si e da própria continuação da vida.

E justamente por isso o conceito de Estado como conhecemos sofreu desde época antiga muitas mutações. Atualmente podemos afirmar, em concordância com o exposto por Gouveia em sua obra, que o Estado depende da forma como está organizado: “o Estado é a estrutura que dá vida ao poder político. É no Estado que se concentra a organização política e social, e é constituído do elemento humano, funcional e espacial, sendo estes respectivamente o povo, a soberania externa e interna e o território onde o Estado se projeta”, ou seja, é uma “estrutura juridicamente personalizada, que num dado território exerce um poder político

soberano, em nome de uma comunidade de cidadãos que ao mesmo se vincula." (GOUVEIA, 2018, p.26)

Muitas são as vertentes da segurança, contudo dentre as diversas óticas, a que mais interessa é a classificação ilustrada por Bacelar Gouveia em sua obra, por representar a nosso sentir, a visão mais atual e apropriada ao estudo aqui proposto. Sendo assim, a segurança sobre o ponto de vista do sujeito protegido, dos bens, do âmbito espacial e das estruturas que o asseguram, bem como a intensidade da perturbação (riscos e danos) nos levam a concluir ser do Estado a função máxima e primeira da segurança. (GOUVEIA, 2018, p.26)

Ainda no que tange a Segurança como função do Estado e como aduz Jorge Miranda (1992) em sua obra, "são dois os sentidos possíveis de função do Estado: tarefa ou incumbência, correspondente a certa necessidade coletiva ou a certa zona da vida social; e atividade com características próprias, modo de o poder político se projetar em ação." (MIRANDA, 1992, p. 85)

No primeiro sentido, é complexa a função assumida pelo Estado no que toca a garantia da segurança perante o exterior e da paz civil, à promoção do bem-estar e da justiça social, que segundo o autor, decorre do "alargamento das necessidades humanas, das pretensões de intervenção dos governantes e dos meios de que se podem dotar; mas é também uma maneira de o Estado ou os governantes em concreto justificarem a sua existência ou a sua permanência no poder". (MIRANDA, 1992, p. 86)

No segundo sentido, a função destacada por Miranda "define-se através das estruturas e das formas desses atos e atividades: e revela-se indissociável da pluralidade de processos, de sujeitos e de resultados de toda a dinâmica jurídico-pública." (MIRANDA, 1992, p.86)

Certo é que "manifesta-se um elemento finalístico: diretamente, na função como tarefa; indiretamente, na função como atividade." (MIRANDA, 1992, p.86)

Citando Helder Valente em sua obra Gouveia pondera que a "segurança como fim do Estado será porventura a mais elementar explicação para o poder político que se exerce, valendo-se como proposito fundamental de proteção da comunidade política, através dos seus organismos e da sua normatividade" (DIAS, 212 apud GOUVEIA, 2018, p.100) e vai além, aduz que apesar de não ser a única finalidade é uma das mais fundamentais tarefas na conjuntura estatal, seja do ponto de vista interno como externo e, justamente por isto, sempre foi e continuará sendo a função menos contestada. (GOUVEIA, 2018, p.101)

Logo, igualando o Estado aos seres vivos, cuja finalidade é a sobrevivência, é necessário conjugar meios, critérios, normas e instrumentos para garantir a segurança, interna

e externa e, sendo esta a função primeira, é a que servirá de base a quaisquer outras dentro do Estado Democrático de Direito.

Assim, não obstante a evolução do conceito de segurança e a convergência para uma Segurança Internacional centrada no indivíduo e que abarca não só as novas ameaças como também a segurança humana em si, a segurança pode ser entendida como função primeira do Estado.

Isto porque é justamente a segurança que garante proteção aos direitos e bens jurídicos fundamentais dos cidadãos e das comunidades políticas, bem como a sobrevivência do próprio Estado e sociedade.

Neste tocante a Constituição Portuguesa em seu artigo 9º elenca as tarefas fundamentais do Estado e dentre elas destacam-se: "Garantir a independência nacional e criar as condições políticas, económicas, sociais e culturais que a promovam, garantir os direitos e liberdades fundamentais e o respeito pelos princípios do Estado de direito democrático".[2]

A estas tarefas e funções do Estado português se acresce a segurança, muito embora esteja localizada no Título II do Capítulo I - Direitos liberdades e garantias pessoais, mas precisamente no art. 27.1: "Todos têm direito à liberdade e à segurança." [3]

Já a Constituição Brasileira menciona a segurança em seu preâmbulo quando institui um Estado Democrático destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, e o bem-estar. Em seu Título II trata dos direitos e garantias fundamentais, elencando em seu art. 5º a segurança como direito fundamental, no art.6º como direito social, e em seu art. 144 explícita de forma objetiva ser a segurança pública um dever do Estado.[4]

Por todo ângulo que se analise a estrutura do Estado e evolução da Segurança fato é que esta sempre será sua função primeira, e embora seja condição para exercício dos direitos fundamentais e democráticos é autônoma e, como vimos, holística.

1.3- SEGURANÇA COMO DIREITO FUNDAMENTAL

[2] Disponível em: https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx Acesso em: 20 nov. 2020.
[3] Disponível em: https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx Acesso em: 20 nov. 2020.
[4] Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm acesso em: 20 nov. 2020.

1.3.1- Direitos Fundamentais e Dignidade da Pessoa Humana

Inicialmente cumpre delimitar o Direito Fundamental e também esclarecer a diferenciação entre direitos fundamentais e direitos do homem visto que ambas as expressões são frequentemente utilizadas. Posteriormente abordaremos neste tópico a relação entre direitos fundamentais e dignidade da pessoa humana, assim como suas características e funções.

Pois bem. Podemos dizer que os direitos fundamentais decorrem, como assevera Canotilho em sua obra, de uma teoria jurídico-positiva. Os direitos fundamentais são direitos objetivamente vigentes numa ordem jurídica concreta, um princípio democrático. (CANOTILHO, 1993)

Canotilho (1993) diferencia ainda as expressões direitos do homem e direitos fundamentais uma vez que são frequentemente utilizadas como sinónimas:

> *"*Direitos do homem são direitos válidos para todos os povos e em todos os tempos (dimensão jusnaturalista-universalista); direitos fundamentais são os direitos do homem, jurídico-institucionalmente garantidos e limitados espacio-temporalmente. Os direitos do homem arrancariam da própria natureza humana e daí o seu carácter inviolável, intemporal e universal; os direitos fundamentais seriam os direitos objectivamente vigentes numa ordem jurídica concreta." (CANOTILHO, 1993, p.517)

No tocante aos direitos do homem, Norberto Bobbio (2004) em sua obra ensina que há uma deslocação relevante do Estado para os indivíduos:

> "A afirmação dos direitos do homem derivam de uma inversão de perspectiva, característica da formação do Estado moderno, na representação da relação política, ou seja, na relação estado-cidadão ou soberano súditos: relação que encarada, cada vez mais, do ponto de vista dos direitos do cidadãos, não mais súditos" (BOBBIO, 2004, p.8)

Portanto, os direitos fundamentais assumiram uma real e inquestionável posição na sociedade, fruto da inversão da tradicional e histórica relação entre Estado e indivíduo, onde este último passa a ter primeiro direitos e depois deveres para com o Estado.

Neste diapasão, Bacelar Gouveia assevera que os direitos fundamentais tem uma vertente positiva, vez que estão constitucionalizados e, portanto, tem a finalidade de proteger a pessoa humana. (GOUVEIA, 2018)

Ainda segundo este ilustre professor, o conceito de direitos fundamentais tem uma perspectiva específica inerente ao direito constitucional, pois este como nível supremo da ordem jurídica incumbe a proteção da pessoa humana e, justamente por isso, ocupam a posição cimeira da pirâmide jurídico-estadual. Constitui-se, portanto, como posição jurídica

ativa das pessoas integradas ao Estado Sociedade, e são exercidas por contraposição ao Estado Poder, positivadas na constituição. (GOUVEIA, 2018)

No que tange a dignidade da pessoa humana, é necessário mencionar que este princípio consta dos mais evoluídos ordenamentos jurídicos e está presente na ordem internacional, é o primeiro e principal denominador comum dos estudos dos direitos fundamentais e do direito fundamental a segurança; "o princípio da dignidade humana, como manifestação do princípio do Estado de Direito, significa que a pessoa é colocada como o desígnio supremo do Estado e do Direito." (GOUVEIA, 2018)

Neste contexto podemos dizer que a dignidade da pessoa humana é inerente a todo ser humano. Não é o ordenamento jurídico que atribui ao indivíduo a dignidade, mas sim o faz valer mediante a consagração dos direitos fundamentais e estrita observância de suas funções. Por tais considerações concluímos que a Dignidade da Pessoa Humana é o núcleo em torno do qual gravitam não só os direitos fundamentais como todos os outros.

Noutro giro, cumpre salientar a visão apresentada na obra Hermenêutica Constitucional e Direitos Fundamentais, a qual citando a crítica de Canotilho, elucida de forma objetiva questões relativas a existência de direitos fundamentais fora de catálogos específicos, mas implícitos ou presentes no ordenamento restante, que com fundamento material na dignidade da pessoa humana são ditos direitos fundamentais, ou, ainda, que não pressupõe a ideia princípio de dignidade da pessoa humana "num exemplo típico de uma teoria de direitos fundamentais não constitucionalmente adequada". (CANOTILHO, 1998 apud MENDES, COELHO, & BRANCO, 2000).

> "De toda forma, embora haja direitos formalmente consagrados como fundamentais que não apresentam ligação direta com o príncipio da dignidade humana, é esse principio que inspira os tipicos direitos fundamentais, atendendo a exigência de respeito a vida, a integridade fisíca e íntima de cada ser humano e a segurança.É o principio da dignidade humana que justifica o postulado da isonomia e que demanda fórmulas de limitação do poder prevenindo o arbíitrio e a injustiça. (...) Os direitos e garantias fundamentais, em sentido material, são, pois, pretensões que, em cada momento histórico, se descobrem a partir do valor da dignidade humana." (MENDES, COELHO & BRANCO, p.116).

Ainda nesta mesma obra, se reconhece também como assertiva a visão de José Afonso da Silva:

> "quem os direitos fundamentais designam no nível do direito positivo, aquelas prerrogativas e instituições que o [ordenamento jurídico] concretiza em garantia de uma convivência digna, livre e igual de todas as pessoas . Nos qualificativos fundamentais acha se a indicação de que se trata de situações jurídicas sem as quais a pessoa humana não se realiza, não convive

> e, às vezes, nem mesmo sobrevive". (SILVA, J. A, 1992, p. 163-164 apud MENDES, COELHO, & BRANCO, 2000, p. 117)

Na Constituição Brasileira a dignidade humana é o princípio norteador, estando consagrada no art. 1º inciso III, como princípio fundamental. Destaque também para o fato da Constituição Brasileira dispor primeiro sobre os direitos fundamentais antes de tratar da organização do Estado.[5]

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
> III - a dignidade da pessoa humana.

Os direitos fundamentais também estão expressos de forma cristalina no art. 5º e constituem as chamadas cláusulas pétreas, portanto, não podem ser suprimidos ou alterados por emendas constitucionais, eis que os direitos fundamentais são elemento integrantes da identidade e da continuidade da Constituição. (MENDES, COELHO, & BRANCO, 2000)

O ordenamento jurídico português, de igual modo trás a dignidade da pessoa humana também em seu art. 1º da CRP[6]:

> Princípios fundamentais
> Artigo 1.º
> República Portuguesa
> Portugal é uma República soberana, baseada na dignidade da pessoa humana e na vontade popular e empenhada na construção de uma sociedade livre, justa e solidária.

Com vistas a sua própria sobrevivência e, consequentemente, a garantia suprema da dignidade humana, os direitos fundamentais se apresentam, portanto, como concretizadores desta e, para tanto, são várias as características e funções como veremos a seguir.

1.3.2- Das Características, Funções e Dimensões dos Direitos Fundamentais

Sobre este ponto é necessário salientar que nos deparamos com imensa e valiosa bibliografia sobre o tema, que culminou em certa dificuldade em elencar todas as características dos direitos fundamentais projetadas por diversos Estados, vez que, por óbvio, não são uniformes. Diante disto, sem menosprezar quaisquer características, mas com fim de melhor delimitar iremos apontar brevemente apenas aquelas que, sob o prisma do estudo aqui proposto, são mais importantes e que proporcionam uma visão mais abrangente do tema.

[5] Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 21 mai. 2020
[6] Disponível em https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx acesso em: 21 mai. 2020

Sendo assim podemos dizer que da doutrina analisada as características mais importantes percebidas foram: Universalidade; Historicidade; Inalienabilidade; Imprescritibilidade; Irrenunciabilidade; Relatividade/Limitabilidade.

Segundo José Afonso da Silva (2005) a Historicidade se deve ao fato de que os direitos nascem se modificam e desaparecem com o decorrer do tempo, rechaçando assim a teoria do direito natural. A Inalienabilidade se deve ao fato de serem intrasferíveis, indisponíveis e inegociáveis, vez que não tem conteúdo patrimonial. No que tange a imprescritibilidade, os mesmos nunca deixam de ser exigíveis, daí decorre a ausência de requisitos que importem em prescrição. Já a irrenunciabilidade se exprime no fato de que o direito até pode não ser exercido, mas jamais renunciado. Quanto à relatividade e limitabilidade, segundo o autor não existem direitos fundamentais absolutos, pois todos encontram limites em outros direitos. Logo, para que os direitos fundamentais possam conviver entre si não podem ser considerados absolutos; o autor ainda menciona que isto não pode ser aceito desde que se reconheça a historicidade. Justamente por isso rechaça também o posicionamento de Pontes de Miranda de que "há direitos fundamentais absolutos e relativos (SILVA, J. A, 1992, p. 181)

Ainda sobre este enfoque, a universalidade apesar de não supor uniformidade é uma das características mais marcantes, pois é de se reconhecer suas semelhanças em diversos ordenamentos jurídicos e também em legislações internacionais. (MENDES, COELHO, & BRANCO, 2000)

Igualmente, a questão dos direitos absolutos se coloca como inaceitável, do ponto de vista interno e externo, eis que podem ser objeto de limitações:

> "Em sistemas aparentados ao nosso, tornou-se pacífico que os direitos fundamentais podem sofrer limitações, quando enfrentam outros valores de ordem constitucional, inclusive outros direitos fundamentais. Igualmente no âmbito internacional, as declarações de direitos humanos admitem expressamente limitações que sejam necessárias para proteger a segurança, a ordem, a saúde ou a moral pública ou os direitos e liberdades fundamentais de outro(art.18 da Convenção de Direitos Civis e Politicos de 1966 da ONU). (MENDES, COELHO, & BRANCO, 2000)

No que toca as funções, Canotilho (1993) assevera que os direitos fundamentais cumprem a função de direitos de defesa dos cidadãos sob uma dupla perspectiva:

> "constituem, num plano jurídico-objectivo, normas de competência negativa para os poderes públicos, proibindo fundamentalmente as ingerências destes na esfera jurídica individual; implicam, num plano jurídico-subjectivo, o poder de exercer positivamente direitos fundamentais (liberdade positiva) e de exigir omissões dos poderes públicos, de forma a evitar agressões lesivas por parte dos mesmos (liberdade negativa). (CANOTILHO, 1993, p.541)"

Noutra visão, o direito de defesa faz o Estado "abster-se de praticar o ato incompatível com os direitos fundamentais ou a anular o que já praticou." (MENDES, COELHO, & BRANCO, 2000, p.147)

Os direitos fundamentais também podem ser considerados como direito a prestações, ou seja, como direitos ao acesso e utilização de prestações estaduais, visto que ao poder público, ao Estado em si, incumbe à responsabilidade de por a disposição dos cidadãos as mais variadas prestações existenciais e dignas, garantindo assim, nomeadamente a dignidade da pessoal humana. (CANOTILHO, 1993)

Ou seja, enquanto os direitos de defesa representam uma "abstenção que resulta na manutenção do *status quo* do indivíduo" visando proteção contra atos de opressão Estadual, a função de prestação se traduz num *status* positivo, no dever de agir do Estado para garantir a promoção dos direitos. Assim, "os direitos de defesa asseguram as liberdades e os direitos prestacionais buscam favorecer as condições materiais indispensáveis ao desfrute efetivo destas liberdades." (MENDES, COELHO, & BRANCO, 2000, p.142-143)

Por fim, necessário ainda mencionar a existência de uma dimensão subjetiva e objetiva dos direitos fundamentais. "A dimensão subjetiva no que concerne a finalidade dos direitos fundamentais, pode ser expressa numa função positiva ou negativa como vimos acima, já a dimensão objetiva resulta do significado dos direitos fundamentais como princípios básicos da ordem constitucional". (MENDES, COELHO, & BRANCO, 2000, p.152-153)

1.3.3- Segurança como Direito Fundamental e sua relação com outros Direitos

Como vimos os direitos fundamentais, com todas as suas características, funções e dimensões são a essência do Estado Democrático de Direito, operando como limite do poder e como diretriz para sua ação.

A segurança, contudo, tem contornos especiais, pois além de ser um direito fundamental positivado nos ordenamentos jurídicos objetos deste estudo, tem também sua relevância positivada historicamente nas mais diversas legislações e diplomas internacionais dentre os quais se destacam o sistemas da Organização das Nações Unidas, o Conselho da Europa e União Europeia e o Mercosul.

Em todos estes sistemas a segurança se apresenta como direito fundamental porque conjuga as características e funções já mencionadas e que por sua vez são inerentes aos

direitos fundamentais, sendo ainda essencial para concretização da dignidade humana e bem estar coletivo.

No cenário português, a Constituição é vista como a Constituição da Segurança. A relevância da Segurança aflora em diversas partes da constituição, desde o preâmbulo faz alusão à preocupação com a instauração do Estado Democrático de Direito com base em princípios fundamentais, cuja orientação interna e externa rege-se pela afirmação da segurança como tarefa fundamental do Estado.

Dentre as diversas menções constitucionais a segurança destacamos a disposta no art.27 da CRP, que está localizado no Título II- direitos, liberdades e garantias:

> Artigo 27.º
> (Direito à liberdade e à segurança)
> 1. Todos têm direito à liberdade e à segurança.

Entretanto, tendo por base a obra do professor Bacelar Gouveia (2018), em que esmiunça a posição da segurança no respectivo ordenamento jurídico, tem-se a segurança como um direito fundamental constitucional, cuja dimensão é ampla, representando um acréscimo de proteção jurídico constitucional, ainda que sua posição sistemática esteja equivocada:

> "Há um erro na localização sistemática deste direito á segurança no contexto do direito a liberdade, que pode levar o interprete ao equívoco de pensar que este direito a segurança se limita a segurança física perante a prisão ou a detenção ilegal, o que não é verdade, pois é muito mais do que isso. Trata-se de uma segurança com o significado de proteção de outros bens jurídicos que venham beneficiar o titular do direito, proteção que se dirige a muitos âmbitos." (GOUVEIA, 2018, p.299)

Como assevera Bacelar Gouveia o conteúdo do direito a segurança o transforma em um "meta-direito, através do qual o mesmo se constitui como um " largo portal de proteção" de cada um dos direitos fundamentais" (...) Nestas condições, o direito da segurança assume-se como um direito fundamental sobreposto, com um conteúdo que é somatório dos conteúdos específicos de cada um dos outros tipos de direitos fundamentais." (GOUVEIA, 2018, p.299)

Na Constituição Brasileira, a segurança está enquadrada como direito fundamental e social, localizada no capítulo I e II respectivamente, além de diversas outras menções espalhadas ao longo do texto constitucional.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes.

> Art. 6º São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição.

É necessário ressaltar ainda que, muito embora a ideia da segurança ser condição para exercício de outros direitos fundamentais, não se resume a isto, pelo contrário, trata-se de um direito fundamental autônomo, assumindo-se também como bem coletivo. Fato é que não é legítima sua degradação como mero 'auxiliar', a segurança é um direito complexo o qual podemos afirmar ser um direito fundamental e também um direito a liberdade e garantias.

Importa mencionar também, no que tange a Segurança como limitadora de direitos fundamentais que há uma percepção de que os direitos fundamentais são absolutos, pois detém uma posição superior no quadro jurídico constitucional. Tal percepção é oriunda da visão jusnaturalista de que o Estado existe para proteger direitos naturais, logo não haveria lugar para conflitos de direitos e restrições.

Porém, a doutrina majoritária converge no sentido de que não há direitos fundamentais absolutos de forma que, sendo o direito a segurança um direito fundamental subjetivo e autônomo pode entrar em colisão com outros direitos e até mesmo com o próprio direito à segurança de outrem. A segurança poderá, portanto, se apresentar como limite a outros direitos fundamentais, posto que não são ilimitados.

A resolução não é fácil e tampouco pacífica na doutrina, porém sempre deverá ter como critério de análise a proporcionalidade.

Isto porque é impossível cogitar uma fixação, simples, rígida e hierárquica entre os ditos direitos, sem antes apreciar o caso concreto e ponderar uma possível prevalência. "Essa prevalência somente é possível em função das peculiaridades do caso concreto e desde que se revele através de um juízo de ponderação e proporcionalidade, haja vista não existir um critério de solução de conflitos válido em termos abstratos". (MENDES, COELHO, & BRANCO, 2000, p.183)

Neste tocante é imperioso mencionar a análise de Bacelar Gouveia (2018) sobre a possibilidade dos direitos fundamentais absolutos como limite ao exercício dos direitos fundamentais:

> "Se é verdade que muitos conflitos se solucionam diminuindo, no plano concreto, equitativamente, o alcance dos direitos conflitantes, não é menos verdade que, noutras situações tal tarefa não é possível e a concordância prática tem de ser complementada ou substituída por uma ideia de prevalência, tal a gravidade da colisão na lesão dos direitos em questão. É nesse cruzamento metodológico que os direitos fundamentais absolutos se

> podem constituir como auxiliar precioso na resolução dos conflitos entre direitos fundamentais, enquanto exprimam um critério geral de ordem ética, como é, no caso o da dignidade da pessoa humana, que se afigura particularmente presente na tipificação daqueles direitos fundamentais absolutos." (GOUVEIA, 2018, p.358)

E ainda, a segurança fundamenta certas restrições a direitos fundamentais, o que incluiu por óbvio o direito a segurança de cada um. Vale frisar que invocar a segurança como cláusula geral para impor restrições e limitações aos direitos fundamentais é medida que deve conter específica autorização constitucional e proporcionalidade, a exemplo de conformidade com esta regra temos o disposto no art. 18.2 da CRP:

> Art. 18.2. A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos.

Neste cenário de restrições e limitações de direitos fundamentais é necessário observar também as relações especiais de sujeição, como por exemplo, os militares portugueses, cujos direitos fundamentais sofrem restrições em decorrência do exercício das funções de segurança e tem de forma objetiva tanto na CRP quanto na LDN "autorização" para restrição.[7]

Pois bem. Após desmistificar o conceito de segurança e verificar que hoje é um conceito holístico foi possível perceber, seu desenvolvimento e relacionamento com a estrutura do Estado, suas características, funções e dimensões. Além disto, o percebemos como direito fundamental consagrado na ordem interna dos Estados objeto deste estudo e também na esfera internacional. Verificamos ainda sua contribuição na garantia de outros direitos fundamentais inerentes ao ser humano e a concretização da segurança humana.

Foi possível perceber também a possibilidade de limitações, restrições e colidências entre os direitos fundamentais, cuja resolução deverá atender critérios de proporcionalidade e uma eximia análise do caso concreto que não deverá suprimir os valores inerentes a cada dos direitos fundamentais, posto que não há uma hierarquia entre os mesmos.

[7] Conforme Art. 270º da CRP - Restrições ao exercício de direitos. A lei pode estabelecer, na estrita medida das exigências próprias das respetivas funções, restrições ao exercício dos direitos de expressão, reunião, manifestação, associação e petição coletiva e à capacidade eleitoral passiva por militares e agentes militarizados dos quadros permanentes em serviço efetivo, bem como por agentes dos serviços e das forças de segurança e, no caso destas, a não admissão do direito à greve, mesmo quando reconhecido o direito de associação sindical.
Art. 26º da LDN - Direitos fundamentais. Os militares na efetividade de serviço, dos quadros permanentes e em regime de voluntariado e de contrato, gozam dos direitos, liberdades e garantias constitucionalmente previstos, com as restrições ao exercício dos direitos de expressão, reunião, manifestação, associação e petição colectiva e a capacidade eleitoral passiva constantes da presente lei, nos termos da Constituição.

Por fim cumpre destacar relativamente à questão trazida neste trabalho, segurança e privacidade, que eventual colisão de direitos deverá ter em pauta de resolução o equilíbrio máximo, cujo vetor de análise e ponderação será a proporcionalidade que deverá ter por base o núcleo essencial de todos os direitos fundamentais, qual seja a dignidade humana e também o bem coletivo, permitindo ao Estado e seus indivíduos a vida em sociedade ao mesmo tempo em que permitirá o exercício de outros direitos tidos como fundamentais ou não.

2- PRIVACIDADE

2.1- CONCEITO ELÁSTICO

Historicamente a privacidade sempre foi difícil de conceituar. As diferentes terminologias foram ganhando a seu tempo diversos contornos. Vida privada, intimidade, o sigilo, individualidade, são diferentes vocábulos, mas que gravitam em torno do núcleo privacidade, mas afinal o que é privacidade e em que consiste o direito a privacidade?

O conceito Privacidade advém de privado "do latim *privatus*, significa separado de". (CORREIA, 2016, p.63).

Apesar das inúmeras tentativas de conceituação e vasta doutrina sobre o tema podemos dizer, de forma geral, que a privacidade abarca tudo aquilo que o indivíduo não quer compartilhar, ou seja, que não quer ver exposto a domínio público, tudo aquilo que lhe é privado, particular, pessoal.

Partindo desta premissa decorre a necessidade de diferenciar o público do privado com vistas a garantir uma melhor compreensão da privacidade.

A dicotomia entre o público e privado, para Victor Correia, encontra fundamento já na antiguidade, e são expressos nos pensamentos de Aristóteles quando distingue a esfera privada (*oikos*) das esfera pública (*polis*). "Quando por ocasião da *polis*, espaço onde se estabelece a igualdade entre cidadãos, e o privado que se restringe ao universo doméstico". (ARISTÓTELES, 2003 p 30, apud CORREIA, 2016, p. 42)

Os pensamentos de John Locke, segundo Correia, expressa que a dicotomia público privada, traduzia-se na necessidade de regular as relações entre Estado, economia, e população, e serviu de base ao que hoje chamamos de privacidade, "a dicotomia público privada constitui o início do termo chave do liberalismo, fora durante este período que se consagrou o direito dos indivíduo de se resguardar da ingerência do poder público" (JONH LOCKE, 2006, apud CORREIA, 2016, p. 64).

Conforme assevera o referido autor a dicotomia público-privado é algo sempre a "redefinir, é circunstancial, pois advém de uma construção social e histórica, não constituindo um dualismo rígido, é um conceito aberto, no fundo, o público e o privado são duas faces da mesma moeda: cada um deles é enquanto tal, dada a existência do outro". (CORREIA, 2016)

A doutrina jurídica aponta como marcos inicial do estudo da privacidade o *Bill of Rights* (Carta dos Direitos), surgida em 1792 nos Estado Unidos, que garantiu pela primeira vez o direito à inviolabilidade das pessoas, casas, papéis e posses contra busca e apreensão arbitrárias. (CARVALHO, 2020)

Em 1890 outro marco surgiu nos Estados Unidos, o primeiro estudo jurídico sobre a privacidade. O artigo escrito por Samuel D. Warren e Louis Brandeis, *The Right to Privacy* (O Direito à Privacidade), consagrou o direito "*right to be let alone*" (o direito de ser deixado sozinho).[8]

O referido artigo foi um contributo significativo na construção do direito a privacidade. O conceito de privacidade elaborado por Samuel Warren e Louis Brandeis buscava respostas a problemática da invasão na esfera privada experimentada após a utilização de uma nova ferramenta tecnológica, nomeadamente a câmera fotográfica, que passou a ser utilizada pela impressa da época.

O autor Alexandre Sousa Pinheiro (2015) dedica parte de sua obra em analisar os aspectos do artigo e suas consequências históricas e jurídicas visando determinar se o *right to privacy* se traduz numa referência discursiva de um novo direito ou se é um embrião deste.

Para o Autor a construção de Warrenn e Bradeis não pode deixar de ser avaliada como um contributo original para fundar um novo direito: *the right to privacy*, muito embora "Warren e Bradeis declarem não existir uma ampliação da proteção *do right to be let alone*, mas uma extensão do seu conteúdo. (PINHEIRO, 2015, p.294)

Interessante destacar, ainda sob a ótica de Alexandre Pinheiro, que apesar da motivação fática e momento histórico do artigo, "a *privacy* não constitui, no pensamento dos autores de Harvard, um direito absoluto, isento de limitações. O *right to privacy* não impede publicações que se revistam de interesse geral ou público. As limitações do *Right to privacy* deviam ser adequadas ao sujeito titular do direito." (PINHEIRO, 2015, p.294)

O *Right to privacy* foi desenhado para corresponder a um universo elitista de pessoas, de forma que os autores pretendiam proteção das pessoas para que a imprensa não atuasse

[8] O artigo original está disponível em *JSTOR*, www.jstor.org/stable/1321160 Acesso em 08 fev. 2021.

com recolha de imagens em acontecimentos privados ou protegidos do conhecimento social. (PINHEIRO, 2015, p.294)

Conforme ainda assevera o referido autor, apesar do contexto fático é notável que o referido artigo foi integrado a uma revista científica, o que representou sem sombra de dúvida, um avanço na discussão e consolidação da privacidade, tanto que diversas decisões nos anos seguintes tiveram respaldo na discussão posta em causa no artigo, também as diversas críticas e reanalises que o artigo sofreu contribuíram para difusão e transformação da privacidade, sendo necessário reconhecer o importante alcance e legado deixado pelo artigo. (PINHEIRO, 2015)

A partir daí a definição de privacidade passou a comportar diversas terminologias e a abarcar uma variedade de conceitos, por isso, em concordância com a visão de Victor Correia exposta em sua obra "Sobre a Privacidade", podemos dizer que privacidade é um "conceito elástico". (CORREIA, 2016, p. 42)

A privacidade no cenário internacional se concretizou principalmente após a Segunda Guerra Mundial, com a Declaração Universal dos Direitos do Homem, em 1948, sendo atualmente considerada direito fundamental e positivada em várias constituições democráticas e em vários diplomas internacionais que reafirmam sua proteção enquanto direito de personalidade, cujo fundamento é a dignidade humana.

Portanto, a privacidade enquanto direito humano é um direito universal e imprescritível, é um verdadeiro direito de personalidade e implica numa liberdade reconhecida juridicamente a cada indivíduo e encontra fundamento na dignidade da pessoa humana.

O Direito a privacidade constitui, nas palavras de Victor Correia, a afirmação de um direito subjetivo, significa ter um determinado poder, "poder de exigir que sua privacidade não seja invadida," o que implica o direito de cada indivíduo não sofrer interferência do Estado, e dos outros indivíduos, na sua vida privada.

Ao contrário dos direitos sociais e econômicos, este não depende do Estado, mas busca nele sua proteção, a privacidade aliada a democracia constitui importante base de concretização de outros direitos. (CORREIA, 2016, p. 78)

Sendo certo que o conteúdo da privacidade evolui conforme o desenvolvimento do tecido social, o tema vem se reposicionando conforme a multiplicidade de envolvidos e novas tecnologias; na sociedade atual, hiperconectada, digital e informacional, há quem diga que a

privacidade está fragilizada e por um fio e que a exposição individual na internet, consentida ou não, é irreversível.

Muito embora o redesenho da privacidade tenha sofrido na prática um fragilização já que é notório o aumento de violações, principalmente através da internet e outras ferramentas tecnológicas, é indissolúvel o entendimento nuclear: o conceito complexo e elástico de privacidade vai muito além do indivíduo, além de ser base para o desenvolvimento da personalidade e dignidade humana, ela se torna essencial para garantia de liberdades, igualdade, democracia, assegurando, assim como a segurança, o bem estar da vida em sociedade.

> "O direito a privacidade deve ser encarado também com base na sua importância para a própria sociedade, e não em termos de um direito meramente individual. O direito à privacidade não é apenas essencial para autonomia individual, mas também para o bem estra da própria sociedade como um todo. Sem o direito à privacidade muitos outros direitos como a liberdade pessoal e a igualdade ficariam mais vulneráveis. É necessária uma concessão democrática de privacidade, conforme defende Anabelle Lever. Por conseguinte, a privacidade tem também valor no âmbito político. Por um lado o direito à privacidade é importante para a democracia, e por outro lado a democracia é importante para o direito à privacidade, e só assim entendida, a privacidade e a democracia constituem um compromisso em relação a outros Direitos Humanos como por exemplo à liberdade, e o direito à igualdade." (CORREIA, 2016, p. 130)

Assim, apesar da grande variedade de termos como "vida privada" e "intimidade" dentre outros, é imperioso perceber que a utilização do termo privacidade mostra-se uma opção mais razoável e eficaz para especificar seu conteúdo, pois permite uma melhor abrangência e elasticidade no que toca ao seu raio de proteção.

2.2- CONSOLIDAÇÃO DA PRIVACIDADE NO CENÁRIO GLOBAL

Com vistas a resguardar a privacidade e com isto conferir o status de direito fundamental correlato à dignidade humana diversos diplomas internacionais positivaram o reconhecimento não só da sua essencialidade no desenvolvimento dos direitos de personalidade do indivíduo, mas também como da sociedade democrática como um todo.

Foi assim que, considerando o reconhecimento da dignidade humana, a ONU em 1948 proclamou pela primeira vez o direito a privacidade em seu artigo 12 da Declaração Universal dos Direitos do Homem ao dispor: "Ninguém sofrerá intromissões arbitrárias na sua vida

privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei."[9]

Posteriormente, em 1950, com base nos subsídios de proteção ao indivíduo fornecido pela ONU foi elaborada a Convenção Europeia de Salvaguarda dos Direitos do Homem e das Liberdades Fundamentais, que no contexto da privacidade determinou em seu art. 8º não só o Direito ao respeito pela vida privada e familiar como também a possibilidade de limitação com fulcro na segurança.[10]

Em 1966, o Pacto Internacional relativo aos Direitos Civis e Políticos da ONU trouxe em ser artigo 17.1 e 2: "ninguém será objeto de intromissões arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio, ou na sua correspondência, nem de ataques ilegais à sua honra e à sua reputação. Toda a pessoa tem direito à proteção da lei contra tais intromissões ou tais atentados". [11]

Em 1969 a Convenção Americana sobre os Direitos Humanos, reconhece a proteção da honra e da dignidade ao dispor em seu artigo 11.2 e 3: "ninguém pode ser objeto de ingerências arbitrárias ou abusivas na sua vida privada, na vida da sua família, no seu domicílio ou na sua correspondência, nem de ataques ilegais à sua honra e à sua reputação. Toda a pessoa tem o direito à proteção da lei contra tais ingerências ou tais ataques". [12]

Em 1990, Convenção sobre os Direitos da Criança da ONU, artigo 16.1 e 2: "1 - Nenhuma criança pode ser sujeita a intromissões arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou correspondência, nem a ofensas ilegais à sua honra e reputação. A criança tem direito à protecção da lei contra tais intromissões ou ofensas." [13]

Em 2000 a Carta dos Direitos fundamentais da União Europeia, tendo por base valores indivisíveis e universais da dignidade do ser humano, da liberdade, da igualdade e da solidariedade assente nos princípios da democracia e do Estado de Direito para criar um espaço de liberdade, segurança e justiça e coloca o ser humano no cerne da sua ação e, para tanto, dispõe em seu artigo 7° sobre o respeito pela vida privada e familiar: "Todas as pessoas

[9] Disponível em: https://unric.org/pt/declaracao-universal-dos-direitos-humanos/ Acesso em: 03 fev. 2021.
[10] Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/convention_por.pdf Acesso em: 03 fev. de 2021.
[11] Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/pacto_internacional_sobre_os_direitos_civis_e_politicos.pdf Acesso em: 03 fev. 2021.
[12] Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm Acesso em: 03 fev. 2021.
[13] Disponível em: https://www.unicef.pt/media/2766/unicef_convenc-a-o_dos_direitos_da_crianca.pdf Acesso em: 03 fev. 2021.

têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações."[14]

Em 2003, a ONU novamente atua com elaboração da Convenção Internacional sobre a proteção de todos os trabalhadores migrantes e dos membros da sua família, que prevê no artigo 14: "nenhum trabalhador migrante ou membro da sua família será objeto de intromissões arbitrárias ou ilegais na sua vida privada".[15]

Em 2013, a OCDE revisou as diretrizes de 1980 relativas à política internacional sobre a proteção da privacidade. Ciente da introdução da tecnologia de informação em várias áreas da vida econômica e social e da importância e poder crescentes do processamento automatizado de dados, propôs esta revisão com foco na implementação prática da proteção da privacidade por meio de uma abordagem baseada na gestão de riscos, e na necessidade de abordar a dimensão global da privacidade por meio de uma interoperabilidade aprimorada e, reconhecendo a importância estratégica da privacidade, requer uma estratégia nacional multifacetada, coordenada nos mais altos níveis de governo.[16]

Em 2016, um novo marco e grande avanço do debate da privacidade mundial se concretiza na União Europeia com aprovação do Regulamento Geral de Proteção de Dados Regulamento (UE) 2016/679. Embora este regulamento contemple mais adiante alguns aspectos comparativos é imperioso dizer que foi definitivamente um marco para o tratamento da privacidade, que sob a ótica da proteção de dados pessoais, contextualiza um novo perfil a ser seguido mundialmente, revelando um direito a ter controle sobre as próprias informações e dados pessoais, cujo tratamento deve ser realizado seguindo as diretrizes de licitude e adequação, dentre outras mais.[17]

2.3- PRIVACIDADE NO CENÁRIO LUSO BRASILEIRO

No que tange a positivação e interpretação da privacidade no direito luso brasileiro, cumpre destacar suas divergências e convergências, haja vista que este trabalho além de ser exploratório busca trazer alguns aspectos comparativos que são importantes para melhor compreensão das temáticas enunciadas com prioritárias.

[14]Disponível em: https://op.europa.eu/webpub/com/carta-dos-direitos-fundamentais/pt/ Acesso em: 03 fev. 2021.
[15]Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/convencaomigrantes.pdf Acesso em: 03 fev. 2021.
[16] Disponível em https://www.oecd.org/digital/ieconomy/privacy-guidelines.htm acesso em: 09 de fev. de 2021
[17]Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679 Acesso em: 09 fev. 2021.

Assim sendo, considerando inicialmente o ordenamento jurídico brasileiro verifica-se que o Direito a Privacidade no Brasil tem proteção constitucional e infraconstitucional, sendo também considerado Direito de Personalidade.

A Constituição Federal de 1988 insere a privacidade no rol dos direitos fundamentais no Título II - Dos direitos e garantias fundamentais. O inciso X do artigo 5º da Constituição Brasileira de 1988 dispõe que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".[18]

Nota-se, que embora ausente o termo "privacidade" a Constituição confere a ela um desenho mais genérico e amplo. Assim, a luz do ordenamento jurídico brasileiro, o direito e o conceito de privacidade compreende vários aspectos de proteção, como a honra, a imagem, a vida privada e a intimidade.

Neste aspecto, Carvalho (2019) espelha em sua dissertação os estudos de Sampaio:

> "o termo 'intimidade' advém do latim *intimu*s, que significa "íntimo, mais recôndito, interior, relacionado, ainda, com a noção de confiança e segredo, como pode ser visto nos Aduz ainda que a intimidade, ou ter intimidade diz respeito a um terceiro que tem acesso a um espaço de reserva de um indivíduo". Assim, seria uma situação ou qualidade que se usufrui perante o outro: ser próximo o suficiente para lhe expressar sentimentos, emitir opiniões, ser confidente ou fazer algum tipo de pedido, sem formalidades. Dessa forma, "invadir a intimidade" implica em tomar conhecimento de segredos e assuntos pessoais de outro, estar em um âmbito restrito a poucos ou a ninguém." (SAMPAIO, 1998 p. 268 apud CARVALHO, 2019, p. 56)

No que diz respeito ao termo vida privada o autor afirma ainda que há uma pequena diferença no sentido, "pois se refere ao próprio titular da oração, e não uma qualidade que se possuiu em relação a outro. E mais, o significado também é distinto, pois expressa o sentido de ter vida própria, autônoma, independente." (SAMPAIO 1998 p.269 apud CARVALHO, 2019, p.56)

Em verdade, a complexidade e dificuldade de conceituar privacidade e distinguir intimidade e vida privada fez com que o legislador optasse por esta pluralidade de vocábulos na tentativa de abarcar os mais diversos níveis de proteção à intrusão no espaço de autonomia ou de independência do indivíduo. Entretanto, apesar de ter menção expressa à vida privada e intimidade, a expressão direito a privacidade é a mais utilizada, pois tem um sentido amplo e genérico e consegue abranger todas as manifestações da esfera íntima, da vida privada e da personalidade a que a CRFB/88 se refere.

[18] Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 10 fev. 2021.

Neste sentido:

> "Esse termo parece a opção mais razoável, pois é específico o suficiente para se diferenciar de outras expressões como imagem, honra ou identidade pessoal, bem como é claro o suficiente para especificar o seu conteúdo, resultado da sua atualidade. Tal escolha não deriva somente da fragilidade das demais opções, mas principalmente por unificar adequadamente os valores expressos pelos termos intimidade e vida privada". (DONEDA, 2006 apud CARVALHO, 2019, p. 57)

Além disto, a privacidade comporta outras menções e âmbitos de proteção no ordenamento jurídico brasileiro. Podemos citar, por exemplo, o Código Civil que em seu artigo art. 21 dispõe que "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma". [19]

Há também no ordenamento jurídico brasileiro a figura do Habeas Data, remédio constitucional para proteção da esfera íntima dos indivíduos no que concerne ao direito a informações e retificações de dados, previsto no art. 5 º, LXXII, da CF/88; há ainda proteção da vida privada e intimidade no que tange ao domicílio, a correspondência, as comunicações, a invasão dos dispositivos informáticos e os dados pessoais.

No direito português identificamos que igualmente houve dificuldade de conceituar o direito a privacidade o que culminou na utilização da expressão reserva da intimidade e vida privada no texto constitucional.

O direito a privacidade é também considerado um direito de personalidade, inclusive situa-se Capítulo I- Direitos, liberdades e garantias pessoais, Título II - Direitos, liberdades e garantias – outros direitos pessoais mas, igualmente ao texto brasileiro, não menciona expressamente a expressão " direito a privacidade" em seu texto.

O artigo 26.º n.º1 da CRP dispõe que "a todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação."[20]

Para além do texto constitucional e semelhante ao que acontece no ordenamento jurídico brasileiro, é possível verificar a esfera de proteção da privacidade disposta em outras normas como, por exemplo, no Código Civil português que em seu art. 80 - Direito à reserva

[19] Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm Acesso em: 10 fev. de 2021.

[20] Disponível em: https://dre.pt/web/guest/legislacao-consolidada/- lc/337/202103181925/73938545/diploma/indice Acesso em 10 fev. 2021.

sobre a intimidade da vida, dispõe que "todos devem guardar reserva quanto à intimidade da vida privada de outrem e que a extensão da reserva é definida conforme a natureza do caso e a condição das pessoas." [21]

O Código Penal português trás ainda importante capítulo sobre crimes contra a reserva da vida privada, ao elencar do art. 190 até 196 os tipos penais de violação de domicílio ou perturbação da vida privada, introdução em lugar vedado ao público, devassa da vida privada, devassa por meio de informática, violação de correspondência ou de telecomunicações a violação de segredo e aproveitamento indevido de segredo.[22]

Destaque para o artigo 192 do código penal português que trata mais detalhadamente da vida privada, sendo aqui a privacidade o bem jurídico tutelado:

> Artigo 192.º
> Devassa da vida privada
> 1 - Quem, sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual:
> a) Interceptar, gravar, registar, utilizar, transmitir ou divulgar conversa, comunicação telefónica, mensagens de correio electrónico ou facturação detalhada; b) Captar, fotografar, filmar, registar ou divulgar imagem das pessoas ou de objectos ou espaços íntimos;c) Observar ou escutar às ocultas pessoas que se encontrem em lugar privado; ou d) Divulgar factos relativos à vida privada ou a doença grave de outra pessoa;é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.
> 2 - O facto previsto na alínea d) do número anterior não é punível quando for praticado como meio adequado para realizar um interesse público legítimo e relevante.[23]

Cabe ressaltar ainda que o cenário português comporta outras normas mais específicas no que tange a privacidade em sua visão mais extensiva e atual, como por exemplo, o RGPD, bem como a Lei de execução deste regulamento e outras normas comunitárias, as quais serão melhor abordadas nos tópicos a seguir.

2.4- PRIVACIDADE E SOCIEDADE DE INFORMAÇÃO

A privacidade ao longo da história vem sendo moldada pelo próprio tecido social, este hoje muito mais do que antes, dependente da tecnologia e das informações dela resultantes.

[21] Disponível em: https://dre.pt/web/guest/legislacao-consolidada/-/lc/147103599/202103181928/73905514/diploma/indice acesso em 10 fev. 2021.
[22] Disponível em: https://dre.pt/legislacao-consolidada/-/lc/107981223/201708230100/indice Acesso em 10 de fev. de 2021.
[23] Disponível em: https://dre.pt/web/guest/legislacao-consolidada/lc/107981223/201708230200/73474106/diploma/indice Acesso em 10 fev. 2021.

Podemos dizer que na sociedade da informação que atualmente estamos moldando com base no mundo digital, os conceitos iniciais do *right to be let alone* estão dando lugar a uma nova configuração, muito mais sensível e direcionada a proteção de dados e a autodeterminação informativa.

Após a valorização da terra, dos bens de produção na revolução industrial, e da chamada de atenção para a sociedade de risco mundial de Urick Beck, evidencia-se a supervalorização da informação. Podemos afirmar que hoje a informação é um pilar para o desenvolvimento social, econômico e cultural da sociedade. (GOMES, et al, 2020, p.452)

Nesta sociedade de informação há uma legítima expectativa de privacidade conquanto observa-se sua fragilidade. A privacidade assume uma feição, onde o principal ativo é a informação e os dados pessoais. O fluxo deles decorrente representa hoje a própria funcionalidade da sociedade em si.

Como assevera Ghisi, (2014), a informação é o pressuposto de existência e sustentação desta nova sociedade e as tecnologias permitem conservar o conhecimento e empregá-lo na transformação do mundo e na geração e outros conhecimentos.

Contudo, de forma muito mais acentuada que noutros momentos da história, a sociedade anseia cada vez mais por informações, serviços e compartilhamentos ao mesmo tempo em que busca de forma efetiva a proteção dos dados pessoais e exercício do direito à autodeterminação informativa.

Estes são expoentes desta nova realidade e, a nosso sentir, corroboram esta fase de expansão da privacidade e refletem o molde atual de uma sociedade hiperconectada e altamente dependente de tecnologia, onde o dado pessoal é matéria prima.

Na sociedade de hoje, como assevera Victor Correia (2016), a Globalização acabou por produzir efeitos nunca antes vistos ou imaginados, “os meios de comunicação de massa e as alterações produzidas pelas novas tecnologias, nomeadamente através da internet, deram lugar a um mundo virtual e universal, onde todas as pessoas podem ter acesso as mesmas informações.” (CORREIA, 2016, p.94)

Isto não quer dizer que o conceito de privacidade esteja esvaziado no todo, mas é de se ponderar os efeitos da velocidade da informação e os avanços das tecnologias. Há uma maior diversidade de ferramentas tecnológicas que nos obrigam a uma maior exposição para obtenção de determinado serviço, ou, mesmo que o intuito seja uma exposição ‘consentida’, como no caso das redes sociais, nos faz questionar se a privacidade ainda é regra ou exceção.

Fato é que o fluxo de informações e dados pessoais tornou-se um fenômeno de escala global e as novas tecnologias impulsionam cada vez mais esta troca e este fluxo, que por sua vez, consolidam-se como base estruturante da sociedade e dos Estados.

A auto exposição do indivíduo, assim como a vigilância pelos poderes estatais com fulcro na garantia da segurança conferem ainda uma nova dimensão às preocupações em torno do direito à privacidade, a proteção de dados pessoais e a autodeterminação informativa nesta nova era.

Neste contexto alguns autores defendem que esses conceitos são distintos do direito à privacidade. Contudo, as definições de "proteção de dados, ou de autodeterminação informativa, nada mais são do que uma nova forma de aplicar o direito à privacidade." (OLGA, 1985, p.81 apud, CORREIA, 2014, p.72).

Noutra perspectiva, o direito à privacidade na sociedade da informação é um alargamento conceitual para uns e, para outros, uma redefinição do conceito, isto porque todo e qualquer cenário individual pode traduzir-se num potencial quadro de informações que necessitam, portanto, de maior proteção. (DONEDA, 2006)

O universo virtual surgido com a expansão das redes de internet e, posteriormente das redes sociais, proporciona a tempo real, um maior e mais fácil compartilhamento de dados, imagens e sons. Verifica-se com isso um paradoxo na sociedade de informação que temos hoje, pois ao passo que ela requer maior proteção da informação há também uma redução no controle das mesmas, isto porque outro marco desta nova era é o fluxo contínuo e desmedido de dados, este fluxo é também sustentáculo da sociedade de informação.

Isto por óbvio repercute na esfera de proteção do indivíduo enquanto ser uno, mas também enquanto pertencente a uma coletividade global.

Justamente por isso a privacidade na sociedade da informação comporta uma dimensão coletiva como afirma Doneda (2006). Nesta dimensão a proteção não se manifesta exclusivamente na proteção de dados pessoais, mas sim em "vários interesses ligados à personalidade e às liberdades fundamentais da pessoa humana, fazendo com que a disciplina da privacidade passe a se definir como um estatuto que perpassa as relações da própria personalidade com o mundo exterior." (DONEDA, 2006)

Nesta era informacional a discussão concentra-se, portanto, numa vertente voltada a nova formatação da proteção da privacidade que está relacionada à que dados o indivíduo decide compartilhar e também uma proteção coletiva.

Contudo, necessário salientar que ainda encontram-se positivados a reserva da vida privada, da intimidade, sigilo de correspondências e etc., o que houve foi um acréscimo com a introdução da proteção de dados e da autodeterminação informativa, com vistas a acompanhar os novos anseios de uma sociedade que se transforma a cada instante.

A rapidez e facilidade dos meios de comunicação, a forma como as pessoas trocam informações e interagem entre si, somadas a diversidade e constante evolução das ferramentas tecnológicas e de informação proporcionam a expansão da participação e interação dos indivíduos ao mesmo tempo em que acarreta riscos de violação aos direitos fundamentais, como por exemplo, o risco de novos métodos de vigilância e controle da liberdade individual pelos órgãos estatais.

Apesar de não se centrar apenas na proteção dos dados pessoais esta somada a autodeterminação informativa são os marcos legais desta nova era, sua importância não se resume as bases positivadas, mas demandam também uma mudança de comportamento cultural e social. Em verdade, a privacidade na era informacional se expande e ganha um novo capítulo.

Assim, na sociedade de informação, podemos perceber que a privacidade engloba ainda os contornos iniciais e para além destes, se materializa como direito de manter o controle sobre as próprias informações, tendo para isto um aparato legal mais abrangente e rico, que fornece meios de conhecer, controlar, endereçar e interromper o fluxo destas informações pessoais.

2.5- A TUTELA DA PROTEÇÃO DE DADOS - O CONTRIBUTO EUROPEU

Apesar de ter trazido até aqui alguns componentes comparativos do direito luso brasileiro no que tange a segurança e privacidade, bem como algumas considerações sobre o alargamento da privacidade na sociedade de informação, necessário abordar também o contributo europeu para evolução da tutela da proteção de dados.

Diferentemente de Portugal e da União Europeia, o Brasil não dispunha de uma cultura sólida de proteção de dados. Podemos dizer que o ponto de partida para consolidação da legislação de proteção de dados no Brasil foi sem dúvida alguma a necessidade de regulação do assunto no Brasil, mas também a aprovação e entrada em vigor do Regulamento Geral de Proteção de Dados - RGPD.

O efeito gerado por sua extraterritoriedade, o respeito pela conformidade e segurança jurídica que este trás para os cidadãos europeus no que tange a proteção dos seus dados enquanto direito fundamental, bem como o impacto em negócios que se dá em larga escala, já que a conformidade com esta legislação é critério de investimentos e competitividade no mercado global, trouxe impactos e reflexos não só no Brasil, mas no mundo todo.

No que tange a tutela da proteção de dados, é notório que a evolução histórica da cultura jurídica de proteção de dados europeia é muito mais rica e madura se comparada ao Brasil.

No cenário europeu, se voltarmos ao tempo, perceberemos que após a Segunda Guerra Mundial, especificamente com a criação do Conselho da Europa e, posteriormente, com adoção da Convenção Europeia dos Direitos do Homem, já se discutia o direito a proteção de certos dados pessoais, como apontado no artigo 8º daquela Convenção.[24]

Mais tarde, em 1981, com base neste artigo 8° foi estabelecida a Convenção 108[25], já vislumbrando a necessidade de tratamento dos dados pessoais com respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal, foram também estabelecidas, pela primeira vez, as premissas de que os dados pessoais deveriam ser tratados de forma legal, ou seja, desde a recolha e armazenamento até a utilização os dados pessoais deveriam ser usados de forma proporcional, adequada e pertinente, sendo ainda passíveis de retificação.

Já em 1995 nasce a Diretiva n° 95/46/CE[26] do Parlamento Europeu e do Conselho, cujo intuito foi estabelecer equilíbrio entre os Estados membros que regulavam a matéria, garantindo à proteção das pessoas singulares e à livre circulação desses dados pessoais.

Com advento da CDFUE - Carta Dos Direitos Fundamentais da União Europeia em 2000[27], e posteriormente, em 2009, o Tratado de Lisboa, em especial o artigo 16º, n.º 1, do

[24] Artigo 8° da Convenção Europeia dos Direitos do Homem: Direito ao respeito pela vida privada e familiar.
1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros. Disponível emhttps://gddc.ministeriopublico.pt/sites/default/files/convention_por.pdf Acesso em: 26 mai. 2020.

[25] Convenção 108 do Conselho da Europa. Disponível em: http://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/convencao_protecao_pessoas_tratamento_automatizado_dados_caracter_pessoal.pdf Acesso em: 26 mai. 2020

[26] Diretiva n° 95/46/CE .Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT Acesso em :26 mai. 2020

[27] Artigo 8° Protecção de dados pessoais 1. Todas as pessoas tem direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e

Tratado sobre o Funcionamento da União Europeia (TFUE)[28] consagraram de vez o direito a proteção de dados como direito fundamental na União Europeia.

Neste seguimento, e considerando a evolução do direito comunitário de uma Europa de Liberdade, Segurança e Justiça chegou-se o tempo do Regulamento Geral de Proteção de Dados – RGPD, Regulamento n.º 679/2016 que entrou em vigor em 25 de maio de 2018.

A uniformização quanto à proteção dos dados pessoais não só revogou a Diretiva n.° 95/46/CE com o foi de aplicação obrigatória a todos os Estados Membros. Mas não só isto. Devido as suas características, especificidades e seu efeito aterritorial, o Regulamento Europeu serviu de inspiração ao modelo brasileiro.

Seus reflexos e impactos alcançaram empresas em diversas partes do globo, inclusive as brasileiras, o que somado ao fato de não haver no Brasil uma cultura sólida de proteção de dados, mas sim legislações esparsas, alavancou a consolidação de uma cultura de proteção de dados no Brasil.

No que tange as tais legislações esparsas brasileiras, podemos citar, por exemplo, a Lei nº 8.078 de 1990, mais conhecida como Código de Defesa do Consumidor que em sua secção VI, dispõe do banco de dados e cadastro de consumidores, que embora não previsse o apagamento já possibilitava retificação de dados, Lei 12.737/2012 - Crime de invasão de dispositivos informáticos (Lei Carolina Dieckmann); Lei 12.527/2011: Lei de acesso à informação (Art. 4º IV e Art. 31) e a própria Constituição, que como vimos prevê em seu art. 5° a inviabilidade da vida privada, do sigilo das correspondências e comunicações telefônicas e a inviabilidade de dados.

Pondera-se ainda que em 1988 o legislador brasileiro não dispunha de uma *mens legis* referente à proteção de dados como hoje, isto somente foi possível com os avanços tecnológicos, com advento da sociedade de informação e de uma cultura da conectividade e da internet.

Neste contexto não podemos deixar de mencionar também a Lei Brasileira n° 12.965 de 2014, mas conhecida como Marco Civil da Internet[29], que foi de extrema importância no

---

com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas tem o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR Acesso em: 26 mai. 2020

[28] Art. 16 n.º 1. do TFUE : Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF Acesso em: 26 mai. 2020

[29] Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm acesso em 21 mai. 2020.

cenário brasileiro, pois estimulou o pensamento social a respeito do tema das novas tecnologias e agregou impulso a mudança no curso na legislação brasileira no que se refere ao direito digital propriamente dito, ao expandir a discussão das questões atinentes a garantias, direitos e deveres para o uso da Internet no Brasil.

Contudo, ao passo que disciplinava o uso da internet no Brasil, assegurando a liberdade de expressão, os direitos e garantias do usuário, a responsabilidade dos provedores, neutralidade da rede, a guarda de registros de acesso a aplicações de internet na provisão de aplicações, guarda de registros de conexão, não tratava especificamente dos dados pessoais, ficando neste aspecto um grande ponto omisso na legislação brasileira, enquanto despontava na Europa o RGPD com seus reflexos globais para uma cultura eficaz e sólida de proteção de dados.

Diante disto, o cenário brasileiro, por óbvio, carecia de uma legislação própria sobre proteção de dados, que regulasse de forma direta esta temática, promovendo uniformização e garantindo segurança jurídica.

Assim, tendo como inspiração o cenário europeu e sendo o RGPD o contributo mais importante na tutela de proteção de dados, a Lei n.º 13.709 de 2018 foi aprovada em 10 de julho de 2018, consolidando-se como a primeira Lei Brasileira a tratar da proteção de dados de forma específica. [30]

O contributo europeu para tutela da proteção de dados, portanto, torna-se evidente com a consolidação de uma cultura em torno da proteção de dados e da materialização do RGPD.

Ainda neste aspecto, podemos dizer que o contributo europeu se manifesta, como assevera Filipa Calvão, num contexto onde "afirma a proteção de uma dimensão humana como garantia de autonomia pessoal, a qual passa pela proteção da informação relativa ás pessoas (singulares)." (CALVÃO, 2018, p.14)

Muito embora a sociedade hoje esteja vivenciando constantes desafios trazidos pelo desenvolvimento de novas soluções tecnológicas "há uma consciência da importância da proteção e controlo da informação pessoal pelo próprio titular" (CALVÃO, 2018, p.14)

O surgimento de novas ferramentas tecnológicas possibilita, por óbvio, o aumento dos riscos associados a recolha e tratamento de dados pessoais para além dos métodos tradicionais. A criação de perfis discriminatórios, análises de comportamento, sistemas de videovigilância combinados com inteligência artificial, captura de emoções, a exposição em

[30]Lei Geral de Proteção de Dados disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm acesso em 01 out. 2020.

redes sociais, dados de navegação na internet, dentre outros tantos métodos de recolha de informação reclamam, na visão de Filipa Calvão "especiais ponderações entre a recolha da informação e as dimensões humanas assim ameaçadas: a identidade pessoal, a privacidade, e, por sua via, as liberdades pessoais, e em consequência, a democracia". (CALVÃO, 2018, p.17)

Assim sendo, "a proteção de dados se afigura como instrumento de garantia da privacidade e também como meio de garantia da igualdade, da liberdade e de desenvolvimento da personalidade de cada um e da livre participação na sociedade, assegurando a democracia, no sentido de aí ser reconhecido um espaço próprio de pensamento e de escolhas livres de influências e pressões públicas e privadas". (RODOTÁ (2014) apud CALVÃO, 2018, p.17)

Por fim, percebemos ainda, que todo este contributo europeu é gradativo e vem ganhando espaço no cenário brasileiro, ou seja, vem se consolidando ao longo do tempo, a exemplo podemos citar o recente reconhecimento pelo Supremo Tribunal Federal do status da proteção de dados a direito fundamental[31] seguindo mais uma vez o modelo europeu. Além disto, há no horizonte outros marcos legais específicos como, por exemplo, a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, que está contribuindo para estruturação de projetos que visam por fim a carência regulatória brasileira no que tange ao tratamento de dados para fins de segurança, como veremos mais adiante.

2.6- RGPD X LGPD – BREVES ASPECTOS COMPARADOS

Diante deste panorama e considerando a importância, impacto e reflexos do Regulamento Geral de Proteção de Dados para o ordenamento jurídico brasileiro que culminou na aprovação da Lei Geral de Proteção de Dados, se mostrou necessário o presente tópico que, dentro do escopo deste trabalho visa analisar semelhanças e divergências de uma legislação para outra.

Entretanto, necessário esclarecer que devido à extensão das legislações, suscitaremos apenas os pontos que a nosso sentir são mais importantes e que provocam maior reflexão e,

[31] ADI 6387 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, processo eletrônico. Disponível em https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%206387%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true acesso em 02 fev. 2021.

portanto, poderão agregar conhecimento nesta investigação quando nos deparamos com a reflexão sobre a existência e eficácia de instrumentos regulatórios do reconhecimento facial.

Pois bem. Conforme disposto em seu art. 1º a Lei Geral de Proteção de Dados - LGPD regula o tratamento dos dados pessoais, inclusive por meios digitais, e tem por objetivo estabelecer e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa, tal como previsto na Constituição Brasileira.

O Regulamento Geral de Proteção de Dados – RGPD, de forma similar, estabelece que a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental e, por isso, todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.[32] O RGPD através de seus considerandos, reforça o objetivo de contribuir para a realização de um espaço de liberdade, segurança e justiça.

A LGPD, trás em ser art. 2º as suas bases fundamentais quando especifica o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

É possível notar novamente premissas fundamentais e constitucionais como, por exemplo, o respeito à privacidade e liberdade, os direitos humanos e a dignidade. Ao mencionar fundamentos de livre concorrência, desenvolvimento econômico e defesa do consumidor evidencia que, ao passo que garante ao cidadão o direito de ser soberano enquanto titular de seus dados, através do reconhecimento da autodeterminação informativa, a Lei indica que não prejudicará as empresas que tratam dos dados pessoais, mas sim, regulará a forma de tratamento destes dados, reconhecendo os direitos fundamentais do titular.

Em seu artigo 5° a LGPD elenca suas definições e, a nosso sentir o faz de forma menos detalhada, diferentemente do RGPD, que em seu art. 4º, apresenta um rol de definições muito mais extenso. Por óbvio esta carência de detalhes poderá gerar conflitos e lacunas na interpretação, sendo necessário recorrer em analogia ao Regulamento Europeu.

A título de ilustração, a LGPD define dado pessoal apenas como informação relacionada à pessoa natural identificada ou identificável, enquanto o RGPD em seu art. 4.1

[32] Considerando 1 do RGPD: A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT Acesso em: 10 out. 2020.

fornece maiores parâmetros quando estabelece como Dados pessoais: "informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular."

Mas não é só. A LGPD define ainda em ser art. 5º, II, dados sensíveis todos os tipos dados tidos como especiais na RGPD, mas sem proporcionar uma 'distinção' como faz o regulamento europeu em seu art. 4.12 e 4.13, por exemplo.

Quanto aos princípios do tratamento de dados que regem a LGPD, os mesmos estão dispostos no art. 6º e podemos dizer que são muito semelhantes a vertente europeia do RGPD, são eles: finalidade, adequação, necessidade, livre acesso, qualidade de dados e transparência, segurança, prevenção, não discriminação, responsabilização.

A finalidade como sabemos é um dos mais importantes princípios, pois garante que o dado pessoal seja tratado apenas para finalidade específica, não sendo possível sua coleta sem propósito; logo o tratamento deverá ser adequado à finalidade, sendo ainda efetuado o tratamento dos dados de acordo com a necessidade, ou seja, somente aqueles dados absolutamente essenciais devem ser tratados para aquela finalidade específica. Os dados ainda tem que ter qualidade suficiente, estar corretos e atualizados. [33]

O princípio do livre acesso confere ao titular o direito de saber para que seus dados estão sendo utilizados e o tratamento deverá seguir ainda o princípio da transparência na prestações de informações. A segurança assim como a prevenção visa assegurar critérios e medidas de proteção de dados para prevenir danos e violações. Os dados pessoais devem ser tratados de forma preventiva, com apoio de políticas de privacidade e mecanismos que minimizem riscos a segurança da informação. [34]

O princípio da não discriminação tem como objetivo impedir fins discriminatórios, já à prestação de contas indica ser necessários instrumentos de comprovação de conformidade com os demais princípios que regem a LGPD. [35]

Relativamente aos princípios, o RGPD prevê na al. a do n.º 1 do art. 5.º a licitude, lealdade e transparência como princípios chaves e norteadores e conta ainda com os princípios

[33] Disponível em: https://guialgpd.com.br/lgpd-comentada/ Acesso em: 03 mar. 2021.
[34] Disponível em: https://guialgpd.com.br/lgpd-comentada/ Acesso em: 03 mar. 2021.
[35] Disponível em: https://guialgpd.com.br/lgpd-comentada/ Acesso em: 03 mar. 2021.

de livre circulação, propósito limitado, minimização dos dados, princípio da exatidão, limitação de conservação de dados, principio da segurança dos dados, adequação e da responsabilidade.

As condições de licitude de tratamento do RGPD estão dispostas em seu art. 6º: consentimento, execução de um contrato, cumprimento de uma obrigação jurídica defesa de interesses vitais do titular dos dados ou de outra pessoa, exercício de funções de interesse público ou ao exercício da autoridade pública e interesses legítimos e neste aspecto podemos dizer que a LGPD segue os mesmos critérios em seu art. 7º, quando dispõe sobre os requisitos de tratamentos de dados.

Nota-se até aqui que os princípios norteadores se apresentam de forma bastante similar em ambas as vertentes, tanto a Lei Brasileira como o Regulamento tem por base a mesma matriz principiologica.

Contudo, fragmentando a análise para os pontos que guardam maior proximidade com o tema proposto, chama nossa atenção algumas questões sobre consentimento, dados biométricos, avaliações de impacto de proteção de dados e tratamento para fins de segurança, as quais destacamos a seguir.

Consentimento

Especificamente no que tange ao consentimento, o art. 4º n.º 11 do RGPD define consentimento do titular dos dados como uma "manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".

Tal aceitação não pode ser genérica e, como vimos, deve ser específica e lícita, ou seja, deve ter por base a licitude, lealdade e transparência, conforme al. a, do n.º 1 do art. 5º do RGPD. O consentimento é uma das opções garantidoras da licitude, cujas condições estão previstas no art. 7°.

Nota-se aqui que o RGPD optou por conferir maior destaque às definições e meios de tratamentos do consentimento justamente por reconhecer sua importância. Logo, resta claro que o consentimento dever ser livre, específico, direto, deve ser claro e de fácil acesso, permitindo ainda a retirada pelo titular dos dados.

Neste tocante a legislação brasileira define consentimento em seu artigo 5°**,** XII, como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

O consentimento na legislação brasileira, assim como na europeia, é listado com um dos primeiros requisitos ao tratamento de dados. A LGPD em art. 7º, I aduz que o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular.

Este consentimento deverá ser fornecido por escrito em cláusula destacada das demais ou por outro meio que demonstre a manifestação livre de vontade do titular. A LGPD ainda estipula de forma similar a vertente europeia que cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com a lei, sendo vedado o tratamento de dados baseados em consentimento viciado ou em cláusulas genéricas.

No caso de crianças e adolescentes o RGPD prevê que o consentimento para este tipo de tratamento de dados ocorre quanto à oferta direta de serviços da sociedade da informação. O RGPD estipula faixa etária, conforme artigo 8º do regulamento europeu, permitindo a dispensa do consentimento parental, se a criança tiver mais de 16 anos.

Uma questão bem característica do RGPD nesta ceara é que permite certa margem para os Estados legislarem de acordo com a idade, mas desde que a criança não tenha idade inferior a 13 anos.

Em contrapartida, a LGPD prevê que o tratamento deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, não havendo, portanto, qualquer indicação relacionada à dispensa com faixa etária, muito embora o Estatuto da Criança e do Adolescente faça distinção.[36] Entretanto, prevê a exceção do consentimento no art. 14 § 3°, quando a coleta e tratamentos se faz necessária para contatar os pais ou o responsável legal.

Gera inquietações a ausência de uma faixa etária uma vez que o próprio ECA faz distinção entre criança e adolescente e exige consentimento da criança maior de 12 anos para colocação em família substituta, logo, perspectiva-se que neste tocante a LGPD deverá ser conjugada com o Estatuto da Criança e do Adolescente.

De modo geral, no que tange ao consentimento, percebe-se mais semelhanças principiológicas, notando-se algumas omissões, principalmente no que se refere a indicação da faixa etária relacionada ao consentimento para uso dos dados de crianças e adolescentes no âmbito da LGPD.

[36] Lei n.º 8.069 de 1990 - Estatuto da Criança e do Adolescente - em seu artigo 2° Considera criança, pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm Acesso em 01 jun. 2019.

Dados pessoais e dados biométricos

No âmbito do RGPD dado pessoal é toda a informação relativa a uma pessoa considerada identificável ou que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular, conforme art. 4.1 do RGPD. [37]

Já a LGPD considera dado pessoal como informação relacionada à pessoa natural identificada ou identificável e só, conforme art. 5º inciso I.

Posteriormente define dado sensível como sendo o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, conforme art.5, II da LGPD.

O RGPD enfatiza a categoria especial de dados pessoais em seu artigo 9º, a fim de garantir mais proteção a estes. Vê se aqui que a Lei brasileira diferentemente do regulamento europeu não define, por exemplo, dado genético ou biométrico, ela incorpora todos estes dados numa única categoria sem qualquer distinção.

No âmbito do Regulamento Europeu a sistemática em torno do dado biométrico é muito mais imponente e específica, inclusive considerando que a utilização da tecnologia de reconhecimento facial tem por base a utilização da biometria facial, necessário trazer a definição do RGPD exposta no n° 14 do art. 4°:

> "Dados biométricos, dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópico".

A respeito do tratamento destes dados é possível observar que RGPD apresenta um texto mais rígido, pois proíbe o tratamento conforme n.º 1 do artigo 9º, enquanto a legislação brasileira condiciona o tratamento em seu art.11.

O n.°1 do art. 9º do RGPD dispõe:

> "É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados

[37] Art. 4.1 Regulamento 679/2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679 Acesso em: 03 jun. 2019.

> relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa."

Contudo, há hipóteses de inaplicabilidade previstas no n.º 2 do art. 9º, ou seja, embora o tratamento dos dados biométricos seja em regra proibido, se o tratamento ocorrer para cumprimento de obrigações e direitos específicos e, desde que observados os critérios especiais de tratamento, poderão ser tratados.

Desta forma o tratamento dos dados sensíveis no RGPD pode ser realizado de forma condicionada, se o titular der o seu consentimento explícito para finalidade específica, salvo se o direito da UE previr que essa proibição não pode ser anulada pelo titular; se for necessário para cumprimento e exercício de direitos e obrigações de legislação laboral, segurança social ou proteção social, para proteção de interesses vitais do titular em casos de impossibilidade deste dar seu consentimento; no âmbito de atividades legítimas e com medidas adequadas, ligadas a associações sem fins lucrativos, ou se os dados foram tornados públicos pelo titular, para exercício ou um direito num processo judicial, ou por motivo de interesse ou arquivo público, medicina preventiva ou do trabalho.

A LGPD não proíbe, mas sim condiciona o tratamento destes dados com e sem consentimento.

O inciso I do art. 11 dispõe sobre o critério do consentimento de forma semelhante ao RGPD, no que tange a forma e finalidades específicas. Contudo, o inciso II do art. 11 da LGPD trás hipóteses de tratamento sem consentimento do titular.

Conforme disposto na Lei, o tratamento dos dados sensíveis sem consentimento do titular poderá ocorrer para cumprimento de obrigação legal ou regulatória pelo controlador; tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; realização de estudos por órgão de pesquisa, garantida, exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, interesses vitais do titular e de terceiros, tutela da saúde, e garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Nota-se, tanto na LGPD como no RGPD refletem uma maior preocupação quanto aos dados especiais relativamente aos riscos de tratamento inadequado desta espécie de dados. Entretanto, o RGPD é mais rígido ao proibir o tratamento num primeiro momento, enquanto a

LGPD o condiciona. A LGPD ao estabelecer as opções de tratamento de dados biométricos com e sem consentimento do titular determina como pode e como deve ser feito este tratamento.

Ainda no âmbito do RGPD, o considerando n.º 51 aduz que os dados especiais tido como sensíveis merecem proteção específica dado os riscos a direitos e liberdades fundamentais, logo este tratamento se constitui numa exceção.

Prosseguindo ainda na exposição do considerando n.º 51, o tratamento destes dados não poderá ser realizado, salvo se contiver autorização específica e em conformidade com o regulamento, ou constar em direito dos Estados-Membros que pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento.

Destaca-se ainda que o tratamento somente poderá ser efetuado em conformidade, cumprindo os requisitos de proporcionalidade, respeito da à proteção de dados e prestação de garantias adequadas. Deve haver uma necessidade estrita, uma justificativa autorizada pela legislação nacional ou da UE.

Avaliação de impacto de proteção de dados

No âmbito de tratamento dos dados pessoais, se houver necessidade ou utilização de nova tecnologia, ou ainda o tratamento for suscetível de causar elevado risco para os direitos e garantias fundamentais, ou quando as operações de tratamento forem de grande escala ou existir avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada na definição dos perfis desses dados ou na sequência do tratamento de categorias especiais de dados pessoais, de dados biométricos ou de dados sobre condenações penais e infrações ou medidas de segurança conexas, este tratamento deverá ser precedido de uma avaliação de impacto. [38]

De maneira geral podemos dizer que esta avaliação busca identificar e minimizar os riscos deste tratamento de acordo com a necessidade e proporcionalidade.

A avaliação de impacto em proteção de dados é um procedimento presente em ambas às legislações, mas com algumas diferenças.

[38] Conforme considerandos n.º 89 a 96 do RGPD.

Conforme assevera Saldanha (2018), no âmbito do RGPD constitui em verdadeiro instrumento de responsabilização e de demonstração de conformidade, sendo obrigatório nos termos do art. 35. Na esfera brasileira, contudo, não há obrigatoriedade, mas sim uma recomendação para adoção de medidas e regras que revelem boas práticas, a exceção dos casos de inaplicabilidade da LGPD, previstos no art. 4º inciso III.

Esta exceção brasileira se faz presente § 3º do art. 4º e apenas para tratamento de dados relativos à segurança pública, nacional, segurança do Estado e investigação criminal, quando a autoridade nacional deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

Segundo a definição brasileira exposta no art.5º inciso XVII, o RIDP - Relatório de Impacto à Proteção de Dados Pessoais consiste na documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Observa-se aqui que o texto brasileiro de forma similar ao RGPD indica que os riscos estão voltados não só a proteção de dados ou dados sensíveis, mas abarca também liberdades civis e direitas fundamentais. Porém, a LGPD sugere um modelo genérico de relatório, sendo necessário sua instrução e definição de parâmetros pela autoridade nacional, o que ocorreu recentemente, em dezembro de 2020, no âmbito da oficina dirigida do Governo Federal.[39] Contudo, o relatório de impacto de proteção de dados brasileiro ainda será alvo de discussões técnicas pela ANPD.[40]

Ainda no que tange a recomendação, o art. 38 da LGPD dispõe que a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente à suas operações de tratamento de dados. O referido relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O art. 50 da LGPD dispõe que o controlador poderá estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à

[39]Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/apresentacao-oficina_ripd_v2.pdf Acesso em: 03 abr. 2021.
[40] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-cronograma-completo-de-reunioes-tecnicas-sobre-relatorio-de-impacto-a-protecao-dos-dados-pessoais Acesso em: 21 jun. 2021.

privacidade, sendo competência da Autoridade Nacional de Proteção de Dados- ANPD editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei.

Outro aspecto que merece destaque refere-se ao prazo de comunicação de incidentes; a LGPD não tem prazo determinado de forma que caberá a ANPD definir este prazo de comunicação enquanto o RGPD estipula em seu art. 33 que em caso de violação de dados pessoais, o responsável pelo tratamento deverá notificar a autoridade de controlo em até 72 horas.

De forma geral, tendo por base o RGPD, compreendemos que a finalidade do relatório é, portanto, apontar qualquer risco que possa surgir do tratamento de dados e mitigá-los, sendo sempre antecedente ao tratamento para servir de base a tomada de decisão, traduzindo-se também num instrumento de prestação de contas e responsabilização.

Nas palavras de Alexandre Sousa Pinheiro e Carlos Jorge Gonçalves, o RGPD indica os casos em que a avaliação de impacto é obrigatória, conforme n.º 3 do art.35. Além disto, informa as competências dadas à autoridade de controlo nos n.ºs 4 e 5 quanto a publicitação ou não de listas de operações de tratamentos sujeitos ou não a avaliação de impacto. Soma-se a isto a aplicação de um controlo da coerência. Ainda nesta perspectiva aduzem que a avaliação de impacto apresenta uma fase descritiva, uma fase avaliativa e uma fase decisória. (Pinheiro, Coelho, Duarte, Gonçalves, & Gonçalves, 2018, pp. 460-461). Evidencia-se assim maior rigidez e preparo da norma europeia para viabilizar a utilização deste importante instrumento.

Em contrapartida, uma fragilidade se revela na Lei brasileira. Gera dúvidas e inquietações a utilização dos termos ‘poderá e deverá’, uma vez que a respectiva Lei aduz, conforme art. 38, que poderá solicitar relatório de impacto, e nos casos de inaplicabilidade da LGPD previstos no art. 4º, III, para os quais ainda não há lei específica, dispõe que deverá solicitar aos responsáveis o RIPD.

Nota-se, mais uma vez, maior rigidez e solidez do RGPD em comparação a LGPD.

Tratamento para fins de segurança

No que tange a segurança importa mencionar que o RGPD e a LGPD não se aplicam para o tratamento de dados pessoais para efeitos de Segurança Pública, Defesa Nacional,

Política Externa e Segurança Comum da EU, e tratamento pelas autoridades competentes para efeitos de prevenção, investigação e repressão criminal.

O tratamento destes dados se dará através de legislação específica que conjugue medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção de dados e os direitos dos titulares, tal como disposto na al. (d) do n° 2 do art. 2° do RGPD e art. 4º inciso III § 1º da LGPD.

Outra importante diferença consiste no fato do RGPD indicar ato jurídico específico, nomeadamente a Diretiva (UE) 2016/680, conforme se verifica no considerando n° 19:

> "A proteção das pessoas singulares em matéria de tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados, é objeto de um ato jurídico da União específico. O presente regulamento não deverá, por isso, ser aplicável às atividades de tratamento para esses efeitos. Todavia, os dados pessoais tratados pelas autoridades competentes ao abrigo do presente regulamento deverão ser regulados, quando forem usados para os efeitos referidos, por um ato jurídico da União mais específico, a saber, a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho (1)." Os Estados-Membros podem confiar às autoridades competentes na aceção da Diretiva (UE) 2016/680 funções não necessariamente a executar para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, de modo a que o tratamento dos dados pessoais para esses outros efeitos, na medida em que se insira na esfera do direito da União, seja abrangido pelo âmbito de aplicação do presente regulamento."

Em contrapartida a LGPD, apenas dispõe em seu art. 4º, inciso III, § 1º:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

A LGPD prevê legislação específica, mas não faz qualquer menção sobre qual ato legislativo irá assegurar o tratamento de dados relacionados à segurança pública, à defesa nacional e/ou à segurança do Estado, de modo que já nasceu com esta lacuna, diferentemente do RGPD.

É neste contexto que surgem os questionamentos que subsidiaram esta investigação, se as leis gerais de proteção de dados não se aplicam ao tratamento de dados para fins de segurança deve haver lei específica que regule a matéria e ainda, considerando o avanço da tecnologia de reconhecimento facial que tem por base o tratamento de dados biométricos, foi necessário explorar ambos os ordenamentos para melhor compreender como se dá esta regulação para fins de segurança, conforme veremos no próximo capítulo.

Pois bem. Diante da exposição destes elementos e considerando uma breve dimensão comparativa, vislumbramos que ambas as legislações são muito semelhantes principalmente no que concerne aos princípios norteadores e não poderia ser diferente vez que a LGPD tem sua inspiração no RGPD.

Verificamos também que o regulamento europeu e a legislação brasileira tem em si o mesmo sustentáculo jurídico, a mesma essência de proteção aos dados pessoais enquanto direitos fundamentais, porém é possível constatar que a legislação brasileira contém algumas lacunas no que tange as definições e formas de tratamento de dados, sendo necessário recorrer em analogia ao regulamento europeu para uma melhor percepção e aplicação da Lei.

3- RECONHECIMENTO FACIAL

3.1- FINALIDADES E CENÁRIOS DE UTILIZAÇÃO

O reconhecimento facial sempre foi uma condição inerente à natureza humana, o homem sempre foi capaz de reconhecer seus semelhantes, contudo o avanço da tecnologia facilita e impulsiona cada vez mais sua utilização, seja pelo setor privado ou público.

A utilização da tecnologia de reconhecimento facial vem sendo rapidamente difundida ao redor do globo, a forma como se insere em nosso cotidiano é rápida e sútil, a possibilidade de desbloquear um simples *smartphone,* a marcação de amigos em redes sociais ou fazer um *check in* no aeroporto são exemplos notórios que estão inseridos em nosso dia- a- dia.

Diante desta expansão e, como veremos mais adiante, vem ganhando espaço uma discussão própria sobre a regulação da tecnologia de reconhecimento facial, visto que a mesma é baseada na captação e tratamento de dados biométricos, que como vimos acima, são dados especiais, sensíveis, e que exigem maior rigidez em seu tratamento.

Mas afinal, o que vem a ser o reconhecimento facial? Em que consiste esta tecnologia, em que cenários está inserida? Quais são seus riscos e benefícios?

O reconhecimento facial é uma técnica de probabilística computacional que torna possível reconhecer um indivíduo através da análise de suas características físicas, fisiológicas ou comportamentais. O reconhecimento facial pertence à categoria mais ampla de técnicas biométricas (impressões digitais, rede venosa, íris, etc.) que quando conjugada com o desenvolvimento de processos de inteligência artificial e *machine learnin*g pode ser implementado dentro de sistemas existentes (câmeras, *closed-circuit television* (CCTV), banco de dados de fotos, etc.).[41]

O reconhecimento facial depende de estimativas estatísticas para atingir correspondência entre os elementos comparados, exige também maior acurácia das tecnologias e *softwares* envolvidos para aumentar o percentual de assertividade ou probabilidade. Ainda assim é intrinsecamente falível, intrusivo e controverso, já que tem por base o tratamento dos dados de biometria facial.

Podemos dizer que o reconhecimento facial é uma técnica de identificação biométrica automatizada, utilizada em conjunto com *softwares* de inteligência artificial que permite o mapeamento do rosto humano, através de seus pontos identificadores. Estes pontos chamados nodais são convertidos em algoritmos que, posteriormente, são analisados e introduzidos num banco de dados para que determinados objetivos sejam alcançados.

Os pontos nodais são, portanto, marcos divisórios distintos e característicos do rosto humano. O *software* de reconhecimento facial faz a leitura dos pontos nodais medindo, por exemplo, a distância entre os olhos, a largura do nariz, a profundidade das órbitas oculares, o cumprimento da mandíbula etc. (CARVALHO, 2020, p. 36)

Atualmente o reconhecimento facial é realizado por *softwares* cada vez mais modernos com inteligência artificial, mas como refere Carvalho sobre o artigo escrito por Bonsor e Johnson (2001), inicialmente os softwares de reconhecimento facial tinham por base a utilização de imagem com tecnologia 2D, entretanto, com o passar do tempo e a necessidade de maior eficácia e precisão e a própria evolução das tecnologias fizeram com que os *softwares* de reconhecimento facial passassem a utilizar também um sistema de imagem em 3D. (BONSOR e JOHNSON 2001 apud CARVALHO, 2019)

Fato é que cada vez mais a tecnologia de reconhecimento facial evolui e permite o aperfeiçoamento das técnicas e ferramentas que garantem maior precisão na identificação facial, traduzindo-se numa mais valia para fins de segurança e também em outros campos. O

[41] Disponível em https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf Acesso em: 02 mar. 2021. Tradução livre

software pode, portanto, ser conectado a uma infinidade de sistemas e combinado com outros recursos, o que amplia ainda mais a gama de possibilidades de sua utilização, sendo quase impossível pensar em sua não utilização em face do tempo.

Relativamente ao *modus operandi* da tecnologia de reconhecimento facial adotamos a posição do Guia de Adoção de Boas Práticas - Reconhecimento Facial e o Setor Privado[42] do InternetLab e IDEC, que a nosso sentir exprime de forma bastante clara suas finalidades e a divisão de suas etapas, conforme veremos na figura 1 a seguir:

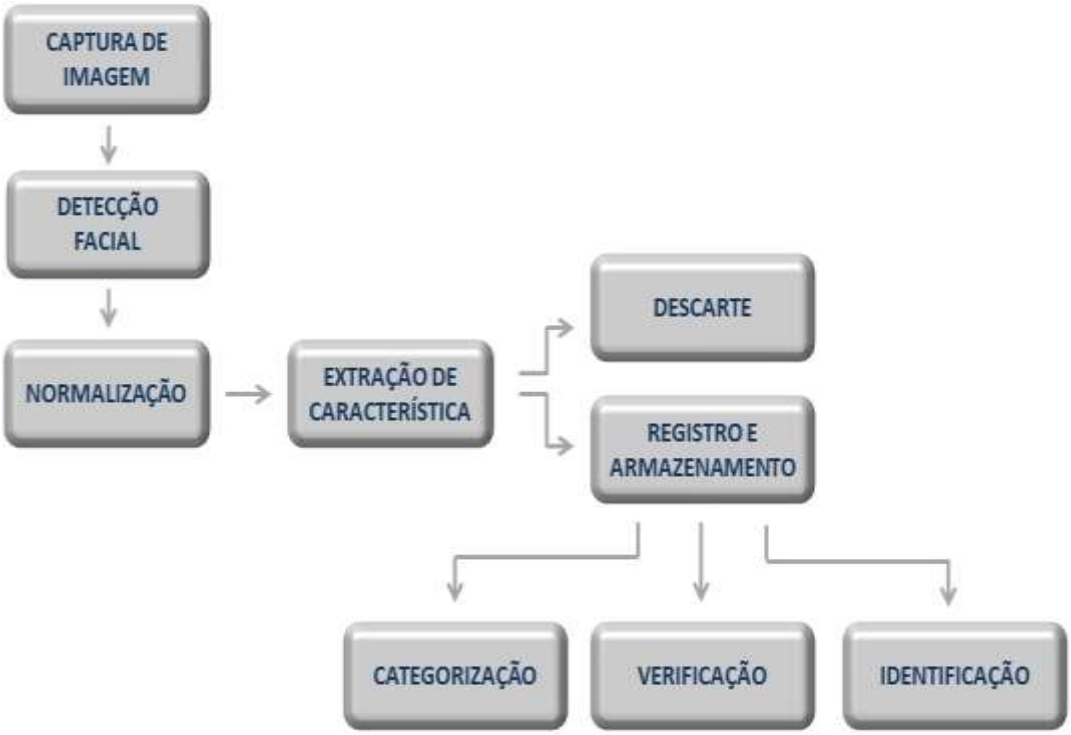

Figura 1 – Etapas do processo de Reconhecimento Facial. Adaptado do Guia de Adoção de Boas Práticas- Reconhecimento Facial e o Setor Privado – InternetLab/IDEC 2020.

Conforme o referido Guia a primeira etapa consiste obviamente na captura da imagem como um todo. Em seguida, detecção facial, onde é enquadrado o rosto humano, ou seja, parte da imagem que contém a face humana é segmentada do restante para possibilitar uma melhor análise da imagem facial, visto que a captura da imagem pode comportar partes não humanas e também ser afetada por outros fatores como, por exemplo, iluminação e posicionamentos da câmera.

[42] Guia de Adoção de Boas Práticas - Reconhecimento Facial e o Setor Privado – Disponível em: https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf Acesso em: 24 fev. 2021.

Após estas duas primeiras etapas tem-se a normalização que permite uma maior uniformização das imagens para que seja possível prosseguir até a etapa seguinte que é a extração de atributos ou características.

Esta quarta etapa por sua vez se concentra nas características geométricas faciais. É nessa parte que se aufere, por exemplo, o distanciamento dos olhos, nariz, ou seja, os pontos nodais, extraindo assim os atributos faciais.

Em casos que não haja o descarte dos atributos passa-se ao registro que permite o armazenamento do dado facial e, por fim, temos a etapa de análise em si, que permite não só a análise propriamente dita, mas a comparação com uma base dados preexistente, podendo ser uma comparação de um para um ou um para todos.

Está fase de análise se subdivide em outras três com base nas finalidades e objetivos de aplicação da ferramenta de reconhecimento facial. São elas: categorização, autenticação/verificação e identificação, podendo ser utilizadas de forma conjugada ou não.

A categorização concentra um dos maiores riscos dessa tecnologia, pois permite enquadrar a imagem biométrica conforme determinadas característica de gênero, idade e cor, por exemplo, e com isto obter determinados perfis que poderão impactar diretamente o direito a privacidade e direitos fundamentais.

A autenticação é a verificação da pessoa, geralmente realizada no contexto de um para um, com nos casos de desbloqueio de *smartphones* e aplicativos de viagens por exemplo, ou seja, dois modelos biométricos são comparados para determinar a probabilidade da pessoa ser quem ela diz ser.

Já a identificação, conforme referido em Reconhecimento Facial e Setor Privado: Guia para adoção de boas práticas de Simão, Fragoso & Roberto (2020), pressupõe uma comparação mais abrangente, ou seja, a imagem da pessoa é comparada em um banco de dados pré-existente para saber a quem pertence numa generalidade.

Insta ressaltar que estes dados são biométricos e, portanto, dados pessoais de categoria especial, sensíveis por natureza, e seu tratamento é proibido ou condicionado a certas exceções, como mencionado no capítulo anterior, frise-se, ainda, o descarte ou anonimização não descaracteriza o tratamento de dados pessoais, pois até a chegada destas etapas pressupõe-se o seu tratamento. Desta forma, é possível concluir que é impossível a utilização desta tecnologia sem tratamento de dados pessoais (Simão, Fragoso, & Roberto, 2020).

É de amplo conhecimento que os avanços tecnológicos permitiram soluções inovadoras, fáceis e mais rápidas indo de encontro aos anseios desta nova sociedade digital e

hiperconectada e informacional. Não é diferente com as ferramentas de reconhecimento facial que cresceram exponencialmente numa escala nunca antes vista e tem se tornado onipresente na atualidade.

Dentre os cenários possíveis de utilização da tecnologia de reconhecimento facial podemos dizer que há forte inclinação para utilização nos campos da segurança dada o alargamento das questões de insegurança, principalmente após o 11 de setembro. Sua utilização é em grande parte conjugada com a videovigilância/CCTV, e tem por objetivo a prevenção e repressão criminal, estando disposta em espaços públicos e privados, contribuindo assim para melhoria da fiscalização e monitoramento pela segurança pública, busca por foragidos, sendo ainda importante ferramenta de persecução penal, busca por desaparecidos e controle migratório.

Além da área de segurança, atualmente são inúmeros os cenários de utilização da tecnologia de reconhecimento facial, entretanto, sendo certa a impossibilidade de citar todos, abordaremos a seguir alguns exemplos variados de *softwares* que utilizam a tecnologia de reconhecimento facial e estão entranhados na sociedade, bem como alguns cenários de utilização que foram veiculados na mídia recentemente.

Seja no cenário econômico, do varejo, da segurança, transportes e até mesmo na educação é certo dizer que a utilização diária e banal pelos cidadãos, como um simples desbloqueio de s*martphone*, por exemplo, ou para uma finalidade mais engajada, trás a teconologia de reconhecimento facial, ao que tudo indica, para domínios globais ilimitados.

Considerando estes domínios ilimitados podemos citar o reconhecimento facial da gigante Amazon, o *Amazon Rekognition*[43], cuja utilização em diversos setores já é uma realidade, permite que os usuários identifiquem a presença de rostos em uma imagem ou vídeo, indicando também quais atributos esses rostos têm. Por exemplo, o *Amazon Rekognition* consegue analisar atributos como olhos abertos ou fechados, humor, cor do cabelo e geometria visual do rosto além de auxiliar outras plataformas, como no caso da *Maarinus Analytics*, por exemplo, que o conjuga com inteligência artificial e fornece ferramentas, como o *Traffic Jam* para agências que auxiliam na identificação e localização de vítimas do tráfico de pessoas. Outro exemplo é a *Aella Credit*, uma empresa de serviços financeiros sediada na África Ocidental que fornece serviços bancários via aplicativo móvel para pessoas com acesso limitado aos serviços bancários dos mercados emergentes. Ao usar o

[43]Disponível em https://aws.amazon.com/pt/rekognition/the-facts-on-facial-recognition-with-artificial-intelligence/ Acesso em: 10 out. 2020.

recurso do *Amazon Rekognition* para detectar e comparar rostos, a *Aella Credit* consegue fazer verificação de identidade sem qualquer intervenção humana. O simples uso do reconhecimento facial permite que mais pessoas tenham acesso aos serviços bancários do que era possível antes.

Já o popular Face ID da Apple[44] fornece uma autenticação através do sistema de câmara de última geração *TrueDepth* com tecnologias avançadas que permitem mapear com precisão a geometria do rosto, assim apenas com o olhar, o Face ID desbloqueia o *iPhone* ou *iPad* podendo ainda autorizar compras na *ITunes Store, App Store* e *Apple Books* e efetuar pagamentos com o *Apple Pay*. O destaque do *Face ID* está em sua alta tecnologia para adaptar-se automaticamente às alterações do rosto, como por exemplo, utilização de maquiagem, chapéus, cachecóis, óculos, lentes de contacto de óculos de sol, ou quando o usuário deixa a barba crescer, incluindo áreas interiores, exteriores e até em situações de escuridão total.

Nesta mesma linha, o *Facebook*[45] utiliza reconhecimento facial para encontrar e analisar as fotos e os vídeos em que o usuário aparece na rede social, sugerir marcações e fornecer recomendações mais relevantes de conteúdo e recursos, pode assim avisar quando o usuário da rede social aparece em fotos ou vídeos, mas não foi marcado, sugerir a marcação de pessoas em fotos ou vídeos publicados por um amigo, e ainda prevê a possibilidade de proteger o usuário contra o uso indevido de identidade, detectando, por exemplo, se a pessoa aparece na foto do perfil de outra pessoa, permitindo a denúncia e exclusão do perfil.

Outro exemplo é o aplicativo de *Selfie Payment* que foi o desenvolvido pela MasterCard[46], o *MasterCard Identity Check*, onde os clientes durante o *check out* em uma loja virtual recebem um *pop-up* em seu celular, por meio do qual poderá autorizar o pagamento com facilidade via reconhecimento facial.

Na educação, por exemplo, seu uso já vem sendo disseminado. Escolas do Espiríto Santo, no Brasil, usam reconhecimento facial para controlar frequência e desperdício de merenda. A tecnologia está sendo testada em cinco escolas municipais e tem como objetivo controlar a frequência escolar, ter maior comunicação com as famílias dos alunos e até diminuir o desperdício de merenda.[47]

[44]Disponível em: https://support.apple.com/pt-pt/HT208108 , Acesso em: 10 out. 2020.
[45] Disponível em: https://www.facebook.com/help/122175507864081 acesso em 10 de out. 2020.
[46]Disponível em: https://newsroom.mastercard.com/videos/mastercard-identity-check-facial-recognition-biometrics/ Acesso em: 10 out.2020.
[47] Disponível em: https://g1.globo.com/es/espirito-santo/noticia/escolas-de-nova-venecia-usam-reconhecimento-facial-para-controlar-frequencia-e-desperdicio-de-merenda.ghtml acesso em: Acesso em: 11 out. 2020

Outro aplicativo de reconhecimento facial vem sendo utilizado também no Espírito Santo, onde professores realizam as chamadas dos alunos através do aplicativo *IAmHere*, que utiliza reconhecimento facial e inteligencia artificial para realizar o controle de presença com mais rigidez e reduzir o tempo para verificar quais alunos assistiram ou não a aula.[48]

Na China escolas usam reconhecimento facial para avaliar atenção dos alunos durante as aulas. Um sistema foi instalado em uma escola em Hangzhou, onde câmeras nas salas de aula trabalham com reconhecimento facial permitindo assim avaliar o nível de atenção dos alunos. O objetivo é auxiliar o trabalho dos professores, facilitando o processo de registro de presenças e avaliando o grau de interesse dos alunos em tempo real (e, em caso de desinteresse dos alunos, identificar se esse é um padrão recorrente).[49]

O cenário de utilização do reconecimento facial no varejo também tem chamado a atenção, a possíbilidade de reconhecer um cliente "VIP" ao entrar na loja ou captar reações sobre determinada oferta vem sendo utilizado por diversas lojas.

A famosa loja Hering, por exemplo, conseguia captar as reações dos consumidores e traçar um perfil de seus visitantes, com isso conseguia determinar qual o conjunto de roupas em exposição era mais aceito ou não despertava tanto interesse.[50]

Outro cenário em que se vislumbra cada vez mais a utilização da tecnologia de reconhecimento facial geralmente alinhada a área de segurança, seja ela pública ou privada, é o cenário dos grandes eventos.

A cidade do Rio de Janeiro e Salvador, por exemplo, colocaram em teste o sistema de reconhecimento facial no carnaval de 2019, com objetivo de monitorar a população durante o evento e identificar pessoas com mandado de prisão em aberto, com passagens pela polícia e desaparecidos.[51]

O sistema de reconhecimento facial usado na cidade do Rio de Janeiro durante o Carnaval identificou 8 mil pessoas foragidas, suspeitas ou desaparecidas. De acordo com o porta-voz da Polícia Militar do Rio de Janeiro, coronel Mauro Fliess, a partir das 8 mil pessoas identificadas, foram realizadas 10 prisões.[52]

[48] Disponível em https://olhardigital.com.br/2019/10/24/noticias/professores-brasileiros-realizam-chamada-por-reconhecimento-facial/ Acesso em: 11 out. 2020.
[49] Disponível em: https://www.targethd.net/escolas-na-china-usam-reconhecimento-facial-para-avaliar-atencao-dos-alunos-durante-as-aulas/ Acesso em: 11 out. 2020.
[50] Disponível em: https://www.leiaja.com/tecnologia/2019/09/03/hering-responde-por-uso-indevido-de-reconhecimento-facial/ Acesso em: 10 out. 2020.
[51] Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/02/rio-e-salvador-terao-sistema-de-reconhecimento-facial-no-carnaval.shtml acesso em 11 out. 2020.
[52] Disponível em: https://tecnoblog.net/289696/rio-de-janeiro-identificou-8-mil-reconhecimento-facial/ Acesso em: 11 out. 2020.

Noutro grande evento ocorrido no Brasil em 2019, onze pessoas foram presas através da tecnologia de reconhecimento facial. A festa de São João de Campina Grande, um dos maiores eventos de São João do Mundo, utilizou o reconhecimento facial como ferramenta de monitorização do evento. Ao todo onze pessoas foram presas por conta da tecnologia de reconhecimento facial utilizada pelos órgãos de segurança na Central de Monitoramento instalada no Parque do Povo. Todos eram foragidos do Sistema Prisional ou tinham mandados de prisão em aberto. Ainda segundo a Polícia Militar, houve mais de 200 reconhecimentos de pessoas, cujas imagens constam nos bancos de dados dos órgãos de segurança.[53]

Considerando ainda grandes eventos desportivos, o monitoramento através do reconhecimento facial nos estádios de futebol em dias de jogos, como já acontece no Estádio do Maracanã, no Rio de Janeiro ou como foi aplicada na final da Liga Europa em 2019 passam a ser cada vez mais utilizados e incentivados. Neste cenário a utilização novamente vem relacionada a questões de segurança, sendo justificada pela prevenção da violência, que permite identificar, por exemplo, os adeptos com antecedentes criminais, possibilitando com isto um melhor monitoramento e medidas necessárias pelas autoridades policiais. [54]

Cumpre destacar também que após a pandemia do COVID-19 as soluções de biometria facial serão ainda mais inseridas no cotidiano, seja com fim de controle pandêmico ou de abstenção de contato físico, o que torna os cenários de utilização ainda mais abrangentes e inovador. A exemplo, o governo do Japão que pretende colocar um sistema de reconhecimento facial em uso para prevenir novas infecções por Coronavírus em eventos de grande escala, incluindo os Jogos Olímpicos e Paraolímpicos de Tóquio.[55]

Neste cenário, conforme apontado no estudo apresentado pelo Instituto Igarapé e Data Privacy Brasil Research - Regulação do Reconhecimento Facial no Setor Público: Avaliação de Experiências Internacionais[56], a medida que o COVID-19 se espalha os governos do mundo inteiro vêm buscando soluções tecnológicas para ajudar no combate à pandemia.

[53] Disponível em: https://www.pbhoje.com.br/noticias/65563/onze-pessoas-foram-presas-atraves-da-tecnologia-de-reconhecimento-facial-no-sao-joao-de-campina-grande.html acesso em 11 de out. 2020.
[54] Disponível em: https://adcecija.pt/reconhecimento-facial-nos-estadios-de-futebol-inteligencia-artificial-banida-da-uniao-europeia/ Acesso em: 11 out. 2020.
[55] Disponível em: https://tododia.jp/japao-considera-usar-reconhecimento-facial-para-rastreamento-em-grandes-eventos/ Acesso em: 10 out. 2020.
[56] Disponível em https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf Acesso em: 10 out. 2020.

Segundo o estudo, dentre as soluções, está à utilização pela Rússia e China dos sistemas de reconhecimento facial que através do emprego desta tecnologia podem monitorar pessoas infectadas no cumprimento do regime de isolamento. Assim, caso a pessoa infectada descumprir a quarentena seu rosto será identificado na via pública e estará sujeita as penalidades locais.

O cenário dos transportes também é um dos mais atraídos pela utilização de tecnologia de reconhecimento facial. Os aeroportos, portos marítimos, estações de metrô, buscam cada vez mais garantir a implantação de sistemas modernos com fito de garantia da segurança já que concentram um número elevado de pessoas em circulação e, por isso, se tornam alvos de ataques, havendo neste cenário uma maior relação com a utilização para fins de segurança, naturalmente.

Fato é que, independente do cenário, é evidente a facilidade e rapidez com que as ferramentas de tecnologia de reconhecimento facial se inserem em nosso cotidiano. Esta percepção deve nos direcionar na mesma proporção à questão da privacidade, pois apesar das inúmeras facilidades trazidas pela tecnologia, principalmente na área de segurança, há inúmeros riscos associados a privacidade das pessoas e direitos fundamentais, que como vimos são os pilares para desenvolvimento da personalidade e da dignidade humana, princípios estes norteadores das sociedades democráticas.

3.2- RISCOS ENVOLVIDOS

São muitos os benefícios trazidos pela inovação tecnológica, isto é um fato incontestável. Dentre os principais benefícios reconhecemos a automatização e rapidez no cumprimento de tarefas tanto de âmbito público como privado.

A biometria facial contribui, por exemplo, para redução de fraudes de identidade, principalmente no setor bancário e de pagamentos, também pode ser utilizado para controlar entrada e saída de funcionários em grandes empresas, entradas e saídas de moradores de condomínios, de alunos em escolas e transportes públicos, redes sociais, são inúmeros os benefícios e cenários de atuação, conforme observado através dos exemplos já citados.

Para fins de segurança contribui para melhoria da prestação de serviço e fiscalização. Amplia o monitoramento pela segurança pública, busca por foragidos, sendo importante ferramenta de persecução penal, busca por desaparecidos e controle migratório.

Contudo, às regras de proteção de dados proíbem, em princípio, o tratamento de dados biométricos para efeitos de identificação de uma pessoa singular, exceto em condições específicas.

Especificamente, nos termos do RGPD, esse tratamento só pode ter lugar com base num número limitado de motivos, sendo o principal por razões de interesse e segurança pública. Logo, considerando a utilização do reconhecimento facial em lugares públicos há riscos específicos para os direitos fundamentais, tanto para o indivíduo em si como para sociedade enquanto coletividade.

No que se refere aos riscos envolvidos e considerando que não há tecnologia de reconhecimento facial sem tratamento de dados pessoais, ainda que a utilização seja realizada em atendimento aos critérios legais, a utilização de reconhecimento facial representa risco aos direitos fundamentais.

Seja pela violação dos dados em si ou através da criação de perfis discriminatórios e viés, seja pelas consequências de falsos positivos e falsos negativos, ou até mesmo o monitoramento e controle massivo da população, há inúmeros riscos associados à utilização da tecnologia de reconhecimento facial.

Sendo assim, podemos afirmar que sempre haverá riscos a sua utilização, assim como conflito entre direitos. É justamente por isto que esta discussão está no topo da agenda mundial.

Tanto o setor privado como os Estados utilizam o reconhecimento facial e aqui não estão em causa apenas a forma de coleta e armazenamento dos dados biométricos e a transparência da utilização da tecnologia, mas também a criação de perfis discriminatórios e monitoramento do cidadão que esbarra diretamente em liberdades e garantias fundamentais, direitos individuais e desenvolvimento de uma sociedade livre e democrática.

Nesta ótica, o Guia para adoção de boas práticas da InternetLab e IDEC expõe que:

> "O reconhecimento facial é uma tecnologia com implicações potenciais sobre o exercício de direitos, dada sua capacidade de identificar e fornecer informações sensíveis sobre indivíduos. Se mal utilizadas – seja pela má intenção de quem detém os dados, seja pela negligência em mitigar riscos –, podem alimentar práticas de vigilância, além de viabilizar práticas abusivas, discriminação e invasão de privacidade." (SIMÃO, FRAGOSO & ROBERTO, 2020, p.44)

Ainda neste tocante afirma Ghisi (2014):

> "Com a correta aplicação de tecnologias, o indivíduo pode ser incessantemente vigiado, não somente por poderes ou autoridades estatais, mas também por particulares, tendo em vista a popularização e fácil acesso a

> sistemas e mecanismos tecnológicos que permitem observação das vidas alheias a partir das informações pessoais, sobressaindo-se controles visuais e auditivos pela captação de imagens, movimentos e sons. Não é exagero cogitar, portanto, que na Sociedade da Informação os indivíduos possam se tornar fáceis objetos de observação, o que pode pôr em risco direitos humanos de extrema importância, com destaque para o direito à privacidade." (GHISI, 2014, p.10)

Assim, podemos dizer que a velocidade da inovação tecnológica e do fluxo de dados nesta sociedade hiperconectada, somados as ferramentas de reconhecimento facial possibilitaram uma nova forma de vigilância e controle, uma nova espécie de Panoptismo.

Os sistemas de vigilância atuais, principalmente em Estados totalitários ou falhados, evidenciam um dos maiores riscos da utilização desenfreada da tecnologia de reconhecimento facial, o controle massivo da população.

Neste contexto de vigilância e controle cumpre relembrar a ideia do Panóptico de Bentham que tinha por base uma arquitetura circular que "elimina a privacidade dos indivíduos", "a construção de um estabelecimento prisional, em forma de circunferência, que permitisse a um único ponto de controlo abranger toda a população criminal, sem que esta se apercebesse do facto de estar, ou não, a ser objeto de observação a cada momento." (BENTHAM, BOZOVIC, 1995 p.35 apud PINHEIRO, 2015, p.186-191)

Esta construção circular idealizada por Bentham permitiria um controle e vigilância baseada em uma onipresença do inspetor que em tese se localiza no centro de uma torre central, assim a ideia de ver sem ser visto permite maior vigilância e controle, como consequência disto, alterações de padrões comportamentais. Assim, conforme aduz Pinheiro, o Panóptico de Bentham e a visão posterior de Focucault sobre o assunto aproxima–se da realidade atual, qual seja, uma sociedade vigiada. "Uma sociedade onde o medo impera e o terrorismo é uma ameaça invisível torna-se difícil limitar as políticas de segurança, ainda que tais limitações tenham por base a proteção da privacidade e dados pessoais." (BENTHAM, BOZOVIC, 1995, p.35 & FOCAULT, 1975 p.233 apud PINHEIRO, 2015, p.186-191)

Fato é que a ideia do Panóptico vem servindo de inspiração aos modelos atuais de fiscalização e monitoramento, o que somados a evolução social, das ameaças e da tecnologia geram a possibilidade/necessidade de videovigilância.

É necessário ressaltar, entretanto, a crítica realizada por Pinheiro a qual concordamos e que diz respeito à relação concreta e específica que fora objeto do modelo inspirador:

> "O Panóptico foi concebido para racionalizar o sistema de controlo pessoal, garantindo um mecanismo simples e eficaz de fiscalização de espaços fechados, onde se presume a inexistência de relações sociais (...)destinava-se

> originalmente aguardar pessoas concretas, não a proceder a buscas difusas em espaços públicos ou privados" (PINHEIRO, 2015, p.191).

O cenário que se tem hoje é um controle baseado na existência, em verdade os avanços tecnológicos, o aprimoramento da videovigilância e ferramentas de reconhecimento facial com *IA* evidenciam a dicotomia segurança x privacidade e tem permitido a exceção tornar-se a regra.

Esta nova configuração do panóptico apoioado nos avanços tecnológicos tem por base, portanto, o desconhecimento do inimigo e da ameaça, formando uma verdadeira sociedade vigiada, numa premissa geral de que mais vale vigiar o todo para garantir a prevenção do crime, a manutenção da ordem pública e a segurança coletiva.

> "Apesar da finalidade fundamental da videovigilância ser a proteção das pessoas e bens, a expansão deste controle permite a capacidade de ver e condicionar o comportamento de quem se desloca no espaço público revelando uma manifestação residual, mas efectiva: apesar de não se traduzir na finalidade do tratamento de dados, apresenta-se como uma consequencia necessária". (PINHEIRO, 2015, p.197-198)

Neste aspecto Pinheiro (2015) destaca ainda que os princípios da dignidade humana e Estado de Direito estaria ivertido, assumido-se como uma espécie de subproduto de um princípio inominado com função de prevenção geral.

Fato é que, guardadas as devidas proporções, a sociedade vigiada que hoje vivemos pode ser interpretada ou equiparada a uma nova forma de panoptismo, que tem como principal motor as informações recolhidas e transmitidas, de forma consentidas ou não, através dos novos e mais modernas meios tecnológicos, nomeadamente a videovigilância e o reconhecimento facial, dentre outros.

Assim, como exposto no artigo Controle e Vigilância na Sociedade da Informação: Novas Formas de Panoptismo "esta nova forma de vigilância influência desde padrões de delinquência até a construção de uma nova forma de garantia de mansidão dos indivíduos, o que se dá através das informações pessoais transmitidas pela world wide web." (GOMES et al, 2020, p.451).

O exemplo mais notório desta nova forma de controle social baseado na videovigilância e ferramentas de reconhecimento facial é a China, que possui uma extensa e sólida rede CCTV e base de dados que permitem a videovigilância em tempo real. As mais de

170 milhões de câmeras e a utilização massiva de reconhecimento facial, somada a outras tecnologias de monitoramento online aprofundam a vigilância sobre os cidadãos locais.[57]

Outro exemplo utilizado na China são os óculos de policiais chineses que já permitem a identificação em tempo real. Com os óculos de reconhecimento facial um policial chinês pode tirar uma foto ou ter acesso imediato a uma base de dados sobre suspeitos.[58]

O reconhecimento facial passou a ser obrigatório até mesmo para aquisição de um cartão SIM, como refere a matéria publicada no jornal *The Guardian*. Com esta nova política todos os usuários de telefones celulares na China que registrarem novos cartões SIM devem se submeter a exames de reconhecimento facial. Segundo a matéria jornalística, as diretrizes exigem que as empresas de telecomunicações implantem inteligência artificial e outros métodos técnicos para verificar a identidade das pessoas que registram cartões SIM, de forma que todas as lojas físicas do país têm prazos para iniciar a implantação deste novo padrão".[59]

Ainda na China a vigilância massiva sobre a população desencadeou o sistema de pontuação mais conhecido como *score social* que fez com que a vigilância online atingisse novas perspectivas, permitindo pontuar os cidadãos conforme as sua condutas.[60] Desta forma, sob o pretexto da pontuação, cujas consequências poderão ser "boas ou más" com recompensas ou sanções, o governo consegue controlar a população.

Além da vigilância massiva mais presente em regimes totalitários ou estados falhados, mas não só restrita a estes, ainda há outros riscos oriundos da prática de *profiling,* vieses e discriminação algorítmica, além dos casos de falso positivos e negativos.

A utilização do reconhecimento facial utilizada no varejo, por exemplo, tem reflexos na identificação e relacionamento com consumidores. A possíbilidade de reconhecer um cliente "VIP" ao entrar na loja e com isto prestar "atendimento especial", apresentar promoções e ofertas personalizadas de acordo com seu perfil e histórico de compras atrai inúmeros varejistas, pois permite mapear o perfil do cliente, registrar fluxo e montar estratégias de vendas especiais. Contudo, tais práticas não atraem interesse apenas dos varejistas, talvez o varejo seja um dos cenários em que gere mais questionamentos do público em geral sobre a utilização do reconhecimento facial para criação de perfis, pois seus efeitos são sentidos instantaneamente pelo consumidor, já que afetam sua liberdade de escolha e

[57]Disponível em: https://www.bbc.com/portuguese/geral-43011505 Acesso em: 02 mar. 2021.
[58]Disponível em: https://www.bbc.com/portuguese/geral-43011505 Acesso em: 02 mar. 2021.
[59]Disponível em: https://www.theguardian.com/world/2019/dec/02/china-brings-in-mandatory-facial-recognition-for-mobile-phone-users Acesso em: 02 mar. 2021.
[60]Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/01/19/a-sociedade-mais-vigiada-do-mundo-como-a-china-usa-o-reconhecimento-facial.htm Acesso em: 02 mar. 2021.

compra. Neste cenário a Secretaria Nacional do Consumidor (Senacon), órgão ligado ao Ministério da Justiça do Brasil, multou a famosa empresa de vestuário Hering em R$ 58.767,00 reais devido à prática abusiva ligada à utilização de reconhecimento facial sem consentimento dos consumidores.[61]

Outro risco associado ao reconhecimento facial que tem tido repercussão social e incendiado as discussões diz respeito à exclusão ou preconceitos causadas pela discriminação algorítmica.

Este problema ocorre quando o algoritmo ou base de dados projetada por ele ou para ele tem certos preconceitos enraizados ou não possui níveis de diversidade suficientes e aptos a possibilitar um correto enquadramento quanto a etnia, gênero, cor e demais características humanas. Infelizmente quando isto acontece tem-se a concretização de exclusão e fomento de desigualdades e preconceito. Uma outra importante causa de discriminação é a qualidade dos dados usados para desenvolver algoritmos e *softwares*. Além disto, para ser eficaz e preciso, o *software* de reconhecimento facial precisa ser alimentado com grandes quantidades de imagens faciais. (AGENCY FOR FUNDAMENTAL RIGHTS, 2019)

Quem não se lembra do famoso caso do Google que repercutiu mundialmente quando amigos foram identificados como gorilas?[62] Outros erros semelhantes ganharam notoriedade na mídia, como por exemplo, o *software* da câmera da Nikon, que interpretou erroneamente as imagens de asiáticos como piscando, o s*oftware* da câmera da *web* da *Hewlett-Packard*, que teve dificuldade em reconhecer pessoas com tons de pele escuros. Outro exemplo muito sério faz referências a um *software* amplamente utilizado para avaliar o risco de reincidência em criminosos, que de acordo com a investigação tinha duas vezes mais probabilidade de sinalizar erroneamente réus negros como tendo um risco maior de cometer crimes futuros enquanto sinalizava os réus brancos como de baixo risco.[63]

Neste cenário no Brasil, a Rede de Observatórios da Segurança lançou um relatório com dados sobre as prisões baseadas em reconhecimento facial. O relatório 'Retratos da Violência – Cinco meses de monitoramento, análises e descobertas', reúne dados e artigos inéditos sobre a utilização do reconhecimento facial no País.[64]

[61]Disponível em: https://olhardigital.com.br/2020/08/27/noticias/senacon-multa-hering-em-r-58-mil-por-uso-indevido-de-reconhecimento-facial/ Acesso em: 10 out. 2020.
[62] Disponível em: https://www.theguardian.com/technology/2015/jul/01/google-sorry-racist-auto-tag-photo-app Acesso em: 02 mar. 2021.
[63]Disponível em: https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html Acesso em: 02 mar. 2021
[64] Disponível em: https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf Acesso em: 01 mar. 2021.

O objetivo do relatório foi entender o impacto da aplicação destas tecnologias no trabalho de policiamento no Brasil e para isto monitorou os casos de prisões e abordagem com o uso de reconhecimento facial, bem como projetos e planos de implementação deste tipo de tecnologia em quatro estados: Bahia, Rio de Janeiro, Santa Catarina e Paraíba, ainda segundo o relatório, entre março e outubro de 2019 foram presas 151 pessoas.

Conforme aponta o relatório, foi difícil encontrar informações completas sobre o perfil da pessoa presa ou abordada onde o reconhecimento foi realizado, bem como os motivos da eventual prisão. No conjunto, em 66 casos havia informações sobre sexo: 87,9% dos suspeitos foram homens e 12,1%, mulheres. A idade média do grupo foi de 35 anos. Em relação aos casos em que havia informações sobre raça e cor, ou quando havia imagens dos abordados (42 casos), 90,5% das pessoas eram negras e 9,5% eram brancas. (NUNES, 2019, p.69)

Ou seja, como aborda o relatório, ainda que para alguns a tecnologia de reconhecimento facial possa parecer uma novidade misteriosa e incerta, "para os rapazes jovens e negros ela tem representado a certeza de que continuarão a ser abordados de forma preferencial". Após um ano de experiências em alguns estados do Brasil o relatório ainda salienta como única certeza " que essas tecnologias podem agravar o encarceramento em massa, principalmente de jovens e negros das periferias brasileiras." (NUNES, 2019, p.67)

Outro ponto que merece destaque são os falsos positivos e falsos negativos, que geram uma identificação errônea. Por óbvio que as tecnologias de reconhecimento facial, como todas as inovações tecnológicas não estão livres de erros. Soma-se a isto que a tecnologia trabalha com probabilidades e não com um resultado definitivo, de modo que existe uma possibilidade real de falsos positivos/negativos.

Diversos fatores podem desencadear um processo de falso positivo/negativo, seja a baixa qualidade de imagens coletadas, modificações estéticas, luminosidade, ângulos e posicionamento das câmeras e o comprometimento da base de dados. Todos estes fatores representam risco aos direitos fundamentais, a liberdade e privacidade, pois a não a identificação da pessoa com precisão pode levar até mesmo a prisão de inocentes.

O falso negativo se traduz na falha do *software* ao combinar duas fotos da mesma pessoa, aqui há também risco para o detentor da tecnologia que tem em verdade uma ineficiência da ferramenta uma vez que a mesma não encontra correspondência e, portanto, não atinge o fim que se destina. Já o falso positivo, refere-se à situação em que uma imagem é combinada com outra imagem em um banco de dados resultando em uma pessoa identificada erroneamente como estando na lista de observação, logo, para fins de segurança e aplicação

da lei tem consequências severas sobre direitos fundamentais desta pessoa, pois significa dizer que ela estava inserida erroneamente na lista de observação / base dados. (AGENCY FOR FUNDAMENTAL RIGHTS, 2019)

Como exemplo desta falha gravíssima podemos citar o caso ocorrido na cidade do Rio de Janeiro, onde o sistema de reconhecimento facial utilizado pela Polícia Militar apresentou falha e uma mulher acabou sendo detida por engano. Após ter sido reconhecida pela câmera de reconhecimento facial instaladas em Copacabana a mulher foi levada para a delegacia, onde foi confirmado que não se tratava da criminosa procurada. Os policiais foram até o local e abordaram a mulher acreditando estar prendendo uma foragida da Justiça, acusada pelos crimes de homicídio e ocultação de cadáver. Contudo, após ter sido conduzida a 12ª delegacia de Copacabana a mulher detida por engano teve sua identidade checada e os agentes confirmaram que não se tratava da pessoa que eles procuravam, evidenciando o grau de falhas e perigos da utilização desta tecnologia.[65]

Fato é que estes riscos e resultados gerados por erros de identificação das ferramentas de reconhecimento facial e, diferentemente de outras tecnologias, representam um risco real e gravíssimo, com enorme potencial ofensivo a direitos fundamentais e impacto direto na liberdade e privacidade dos indivíduos.

Assim, com vistas a equilibrar ou evitar uma possível colisão entre estes direitos fundamentais ao passo que garantimos o progresso e desenvolvimento tecnológico e os benefícios trazidos pela utilização das ferramentas de reconhecimento facial, é necessário minimizar ao máximo os riscos envolvidos na utilização desta tecnologia. Com apoio de condutas que, desde o seu desenvolvimento, revelem boas práticas e conformidade com a proteção de dados e outros direitos fundamentais, que garantam transparência e uma maior assertividade e qualidade de dados, mas não só isto, é importante ter por base legislações claras e eficazes para garantir equilíbrio e mitigação dos riscos de proteção dos direitos fundamentais de segurança, liberdade, privacidade e proteção de dados.

3.3- INSTRUMENTOS DE REGULAÇÃO PARA FINS DE SEGURANÇA BRASIL E PORTUGAL

[65] Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml Acesso em: 11 out. 2020.

3.3.1- Brasil

No Brasil a utilização do reconhecimento facial vem ganhando força mesmo antes de uma legislação consolidada sobre proteção de dados. Frise-se aqui, a legislação de proteção de dados somente entrou em vigor em setembro de 2020 e não trata do assunto de forma específica, apenas indica ser o dado biométrico dado sensível, ao passo que exclui sua aplicação para fins de segurança e faz recomendação sobre relatório de impacto de proteção de dados.

Por óbvio devemos considerar que, *a priori,* qualquer emprego de sistemas de reconhecimento facial deverá respeitar a Constituição no que tange a preservação dos direitos fundamentais, assim como as leis ordinárias e a própria LGPD.

Contudo, conforme disposto na própria LGPD o tratamento de dados pessoais para fins de segurança será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal e os princípios gerais de proteção expresso na LGPD,[66] porém até o momento não há, a nível nacional, regulação específica da proteção de dados para fins de segurança. Neste tocante observa-se que Portugal e União Europeia contam com a Diretiva (UE) 2016/680.

Cumpre destacar que em 2018 houve uma série de iniciativas e debates na Câmara de Deputados e Ministério Público sobre o emprego do reconhecimento facial no Brasil, especialmente na área da segurança, onde ficou clara uma abertura à discussão sobre a regulamentação do reconhecimento facial. Os debates centraram-se na "necessidade de uma regulação equilibrada, com respeito a direitos fundamentais, dentre os quais à privacidade e o direito à informação, bem como a possibilidade de sistemas auditáveis e propostas com colaboração entre os setores público e privado". (FRANCISCO, 2019)

Assim, considerando a inexistência de regulação a nível nacional para fins de segurança e visando analisar o cenário brasileiro tomaremos por base o estudo "Regulação do Reconhecimento Facial no Setor Público: Avaliação de experiências internacionais"[67] desenvolvido pelo Instituto Igarapé e Data Privacy Brasil, através do qual foi possível notar que, ao mesmo tempo que há um aumento da utilização da tecnologia de reconhecimento facial há também uma verdadeira arena regulatória. (FRANCISCO, 2019)

[66] Conforme art. 4º da LGPD.

[67] Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf Acesso em: 10 out. 2020.

O referido estudo foi utilizado parcialmente para o desenvolvimento deste tópico, que tem por objetivo fazer uma análise das principais iniciativas e tendências regulatórias do reconhecimento facial no Brasil. Contudo, devido à "arena regulatória'' estar em constante discussão e mutação e ter este trabalho um viés exploratório, para além deste estudo alargamos a pesquisa e localizamos outros projetos e leis que, como veremos adiante, fomentam ainda mais a discussão sobre o assunto.

Pois bem. Conforme demonstra o estudo a implementação dos sistemas de reconhecimento facial pelo setor público tem sido realizada por iniciativas de regulação esparsas e que não atendem as premissas básicas para garantia de direitos, o que a nosso sentir representa, num primeiro momento, um desafio no cenário brasileiro. (FRANCISCO, 2019)

No referido estudo, a procura por projetos de lei teve como critério o levantamento propostas baseadas especificamente em reconhecimento facial e atuação do poder público, onde foram localizadas três propostas legislativas: PL 9.414/2017, PL 9.736/2018 e PL 4.612/2019.

O PL 9.414/2017[68] cuja ementa é: "Obriga a instalação da leitura de impressão digital e facial nos meios de transportes públicos coletivos", destina-se a fim específico de implementação do reconhecimento facial nos transportes públicos coletivos, sob a justificativa de inibição de fraudes dos benefícios concedidos pelo setor público.

O PL 9.736/2018[69] tem por objetivo tornar obrigatória a identificação biométrica de custodiados pelo Estado pelo método do reconhecimento facial. A justificativa deste projeto de lei tem por base a necessidade do aumento da segurança nos estabelecimentos penais.

Relativamente a estes dois projetos verifica-se que são voltados para setores específicos, um para controle de fluxos no transporte público e outro para identificação em estabelecimentos penais. Além disto, têm como finalidade a autenticação, e não a identificação. Entretanto, não há nenhuma previsão ou menção a princípios e direitos, medidas de transparência, prestação de contas, documentação, ou qualquer elemento de análise de risco. (FRANCISCO, 2019)

Já no que diz respeito à projeto de Lei n.º 4.612/2019[70] e, em concordância com o estudo, esta nos parece mais abrangente e, guardada as devidas proporções, mais próxima da

[68] Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1634793 Acesso em: 03 mar. 2021.
[69] Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1643053 Acesso em: 02 mar. 2021.
[70] Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2216455 Acesso em: 03 mar. 2021.

necessidade nacional de uma regulação específica sobre o tema. O referido projeto tem por objetivo "o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos".

Segundo o Estudo do Instituto Igarapé e *Data Privacy*, o PL n.º 4.612/2019 poderá ser um marco regulatório sobre o tema no Brasil "porque ele parte do pressuposto de que o emprego dos sistemas de reconhecimento facial, seja pelo setor privado ou público, impõe riscos que devem ser levados em consideração".

Diante do reconhecimento destes riscos elenca direitos e boas práticas, como por exemplo, a definição multissetorial de boas práticas quando consequências do uso do reconhecimento facial sejam desconhecidas, obrigações específicas para desenvolvedores e utilizadores de reconhecimento facial e restrições ao uso compartilhado de dados provenientes de reconhecimento facial e, inclui ainda, o envolvimento da ANPD - Autoridade Nacional de Proteção de Dados. (FRANCISCO, 2019)

O Estudo trouxe ainda outras propostas, mas a nível estadual[71], contudo afirma que esta configuração é preocupante, pois os projetos não consideram os riscos inerentes e não incorporam as medidas de prevenção mais básicas, como o estabelecimento de princípios e direitos dos cidadãos.

Ainda no cenário estadual foram localizados pelo estudo do Instituto Igarapé e Data Privacy instrumentos regulatórios que permitem a utilização do reconhecimento facial: Lei n.º 7.123/2015 do Estado do Rio de Janeiro; Lei n.º 21.737/2015 do Estado de Minas Gerais; Lei n.º 16.873/2019 do Estado do Ceará e Lei n.º 8.113/2019 do Estado de Alagoas.

Dentre estas, destaca-se a Lei n.º 7.123/2015[72] do Estado do Rio de Janeiro, que visa a implantação da biometria facial como forma de controle do transporte público coletivo. Diferentemente das outras leis estaduais é interessante notar que mesmo a legislação carioca sendo anterior a LGPD contempla previsão expressa de respeito aos direitos fundamentais de

[71]Conforme Estudo Regulação do Reconhecimento Facial no Setor Público: Avaliação de Experiências Internacionais: PL 1893/19, PL 391/2019-MG, PL 148/2019-PR, PL 342/2019-RJ, PL 607/2019-RJ, PL 318/2019-RJ, PL 341/2019-RJ, PL 853/2019-RJ, PL 665/2019-RJ, PL 1101/2019-RJ, PL 1033/2019-RJ, PL 865/2019-SP.

[72]Disponível em: http://www3.alerj.rj.gov.br/lotus_notes/default.asp?id=53&url=L2NvbnRsZWkubnNmL2IyNGEyZGE1YTA3Nzg0N2MwMzI1NjRmNDAwNWQ0YmYyL2VhODExNDg5YmY3MmY4YjI4MzI1N2YxODAwNTg0M2E4P09wZW5Eb2N1bWVudA==# Acesso em: 05 mar. 2021.

liberdade e privacidade, bem como a responsabilização civil e criminal pelo uso indevido dos dados em ser art.9 § 6° e §7º[73].

Já as demais, como a Lei n.º 21.737/2015[74] do Estado de Minas Gerais, Lei n.º 16.873/2019[75] do Estado do Ceará e Lei n.º 8.113/2019 [76] do Estado de Alagoas, tem por objetivo regular o consumo de bebida alcoólica em estádios de futebol e contém permissão para utilização do reconhecimento facial. Contudo, estas Leis apenas autorizam o uso do reconhecimento facial nos estádios, sem especificar mecanismos de coleta, tratamento, guarda e garantias dos titulares dos dados utilizados pela tecnologia.

Pois bem. Conforme mencionado sentimos a necessidade de alargar a pesquisa visto que o tema está em constante mutação. Com isto, para além destas legislações analisadas pelo estudo do Instituto Igarapé e Data Privacy Brasil, localizamos a Lei n.º 9.167 de 06 de janeiro de 2021[77] que dispõe sobre o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos no Estado do Rio de Janeiro.

Esta Lei estadual é recente e posterior à entrada em vigor da LGPD e, por isto, já prevê que armazenamento e o compartilhamento de dados será realizado em conformidade com ela, estipulando ainda a competência da Secretaria de Polícia Civil para inserção imediata de todos os dados referentes ao Banco de Dados de Reconhecimento Facial e Digital de Crianças Desaparecidas no Sistema de Cercamento Eletrônico e Vídeo monitoramento do Estado do Rio de Janeiro.

A referida Lei permite ainda comparações analíticas de projeção de envelhecimento do indivíduo e veda a utilização do banco de dados para qualquer outro fim, sob pena de responsabilização do agente público.

---

[73]Art. 9 § 6° - A utilização dos dados biométricos pelas concessionárias e permissionárias, que respeitará os direitos fundamentais de liberdade e privacidade, a inviolabilidade da intimidade e o livre desenvolvimento da personalidade da pessoa natural, dependerá de prévia regulamentação pelo Poder Executivo.
§ 7° - As empresas concessionárias e permissionárias de serviços públicos, a operadora do Sistema de Bilhetagem Eletrônica, bem como suas respectivas diretorias, responderão civil e criminalmente pelo uso indevido de dados dos usuários a que tiverem acesso."

[74]Disponível em: https://www.almg.gov.br/consulte/legislacao/completa/completa.html?tipo=LEI&num=21737&comp=&ano=2015 Acesso em: 05 mar. 2021.

[75]Disponível em https://belt.al.ce.gov.br/index.php/legislacao-do-ceara/organizacao-tematica/cultura-e-esportes/item/6638-lei-n-16-873-de-10-05-19-d-o-10-05-19 Acesso em: 05 mar. 2021.

[76]Disponível em https://sapl.al.al.leg.br/media/sapl/public/normajuridica/2019/1594/lei_no_8.113_de_29.05.2019.pdf Acesso em: 05 mar. 2021.

[77]Disponível em: http://alerjln1.alerj.rj.gov.br/contlei.nsf/f25edae7e64db53b032564fe005262ef/017e439b81aa5b700325865700640e38?OpenDocument&Highlight=0,reconhecimento,facial%20 Acesso em: 05 mar. 2021.

Alargando ainda mais a pesquisa realizada pelo Instituto Iguaripé e Data Privacy, localizamos também a Lei n.º 6.712 do Distrito Federal, sancionada em novembro de 2020[78] e o anteprojeto da Lei de Proteção de Dados para Segurança Pública e Persecução Penal[79]. Ambas posteriores ao estudo e de suma importância no cenário brasileiro.

A Lei n.º 6.712 do Distrito Federal visa especificamente o uso de tecnologia de reconhecimento facial – TRF na segurança pública do Distrito Federal e trás diversos elementos e mecanismos mais próximos do que se espera de uma legislação tão importante.

> Art. 1º Esta Lei dispõe sobre o uso de tecnologia de reconhecimento facial – TRF na segurança pública do Distrito Federal.
> Art. 2º Para os efeitos desta Lei, considera-se:
> I – Tecnologia de reconhecimento facial: a tecnologia que analisa as características faciais usada para a identificação pessoal exclusiva de indivíduos em imagens estáticas ou em vídeos;
> II – Vigilância contínua: a utilização de TRF para envolver-se em um esforço contínuo de rastreamento dos movimentos físicos de um indivíduo identificado em um ou mais locais públicos onde esses movimentos ocorrem, durante um período de tempo superior a 72 horas, seja em tempo real, seja por meio da aplicação dessa tecnologia para registros históricos.

Apesar de conter, a nosso sentir, uma definição frágil sobre o que é reconhecimento facial e vigilância continua, ela dispõe sobre a limitação do uso de tecnologia de reconhecimento facial ao vedar de forma expressa em seu art. 3º o uso de TRF para vigilância contínua de um indivíduo ou grupo de indivíduos, além de assegurar em seu art. 5º a revisão de informações por elemento humano.

> Art. 3º Fica vedado o uso de TRF para vigilância contínua de um indivíduo ou grupo de indivíduos, em qualquer hipótese.
> Art. 5º Toda e qualquer sinalização de identificação positiva gerada por sistema de reconhecimento facial deve ser revisada por um agente público antes de qualquer ação decorrente. Parágrafo único. A identificação positiva gerada pelo sistema deve ser validada em campo próprio pelo agente público responsável.

Ela aborda ainda de forma especifica a custódia das informações, assegurando o cumprimento da LGPD, assim como permite o compartilhamento de informações do sistema de reconhecimento facial com órgãos de segurança pública de outros entes da Federação, no estrito limite da Lei, bem como define o prazo de guarda de 5 anos.

[78]Disponível em: https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf Acesso em: 05 mar. 2021.
[79]Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf Acesso em: 08 mar. 2021.

Num primeiro momento, ainda que contenha definições frágeis sobre o reconhecimento facial e mesmo sendo uma Lei Distrital representa um verdadeiro avanço e inovação no cenário legal, pois é a primeira que de fato busca tratar da utilização da tecnologia de reconhecimento facial no âmbito da segurança.

Da leitura do texto legal, contudo é possível constatar a fraqueza de detalhes que comportam diversas críticas, sendo necessário convergir com a Nota Técnica do Laboratório de Políticas Públicas e Internet - LAPIN[80] que afirma que "apesar da inovação em regulamentar o uso dessas tecnologias de reconhecimento facial para segurança pública a referida Lei apresenta pontos preocupantes, por meio de ambiguidades e omissões."

Dentre eles destaca- se a reflexão realizada sobre a clareza da vedação da vigilância em larga escala. Isto porque conforme a nota técnica a vedação do inciso II do parágrafo 2º deveria ser melhor especificada já que a leitura conjunta com o art. 3º deixa dúvidas se a vigilância contínua é ou não proibida pela Lei. Conforme a nota técnica a "vedação do inciso II deveria ser melhor especificada, de modo que se permita somente a vigilância contínua de indivíduos especificados, por até 72h, e não em larga escala, como pretende a norma." (REIS, 2021)

Estaríamos diante de uma divergência interpretativa, cujo impacto social é severo, de modo que será necessário sanar tais contradições e omissões, através de um decreto regulamentador que deverá, segundo a nota técnica, "vedar, de forma explícita, a utilização de TRF em desfavor de grupos de indivíduos indeterminados em qualquer contexto em que não houver autorização judicial para tanto." (REIS, 2019)

Merece atenção também a restrição do uso de TRF para segurança pública em espaços e equipamentos públicos, muito embora não forneça definições de quais espaços são estes. A nota técnica afirma que se bem determinados os conceitos de espaços e equipamentos públicos será possível "reduzir a coleta de dados pessoais sensíveis como os de convicção religiosa, opinião política, filiação sindical ou a organização de caráter religioso, filosófico ou político, ou, ainda, referente à saúde ou à vida sexual." (REIS, 2019)

Outro ponto omisso refere-se ao art. 6°, como aduz a nota técnica, não traz informações acerca dos critérios para o tratamento e uso dos dados, o que pode se traduzir em incertezas sobre como deverão ser as restrições de acesso. A nota vai além ao afirmar que,

[80] A nota técnica tem por objetivo discutir os aspectos positivos e negativos da Lei Distrital nº 6.712 de 2020 e propor medidas que a adequem às exigências do sistema jurídico brasileiro, em especial ao exercício do direito à proteção de dados. Disponível em: https://lapin.org.br/wp-content/uploads/2021/02/NT_LD_67122020_reconhecimento_facial_DF_LAPIN-1.pdf Acesso em: 05 mar. 2021.

"considerando a inexistência de uma Lei Federal específica sobre o uso de TRF para fins penais, não há critérios específicos quanto a quais tipos de investigação criminal podem ser objeto da tecnologia ou às bases de dados utilizadas. (REIS, 2019)

Por fim, a nota técnica faz um alerta de que as imagens coletadas de outras pessoas devem ser imediata e automaticamente apagadas, além disto, afirma que o prazo de 5 anos é excessivo e que a Lei Distrital não traz qualquer previsão a respeito da elaboração de um Relatório de Impacto de Proteção de Dados, critérios de cibersegurança ou direito dos titulares de dados, muito embora sejam este imperativos da LGPD. (REIS, 2019)

Considerando a inexistência de uma Lei nacional de proteção de dados para fins de segurança ou que vise à regulação do reconhecimento facial é inegável a inovação e contributo desta Lei Distrital. Entretanto, após esta breve análise das leis e projetos de lei aqui mencionados verifica-se que do ponto de vista legal são todos insatisfatórios, eis que não contém regras mínimas adequadas para garantir a proteção de dados e demais direitos fundamentais, quiçá metodologia de tratamento adequada e mecanismos de avaliação de impacto e transparência, evidenciando assim a necessidade de uma Lei Nacional que uniformize e regule o tema no País.

Necessário destacar também, no âmbito da investigação criminal, a Lei n.º 13.964/2019, conhecida como pacote anticrime, muito embora seja fonte de discussões quanto a sua constitucionalidade, ela visa aperfeiçoar a legislação penal e processual penal com a criação, no âmbito do Ministério da Justiça e Segurança Pública, do Banco Nacional Multibiometrico de Impressões Digitais que terá por objetivo armazenar não só dados de registros biométricos de impressões digitais mas também de íris, face e voz para subsidiar investigações criminais, devendo sua formação, gestão e acesso ser ainda regulamentado pelo Poder Executivo Federal.[81]

Insta frisar que, apesar da inexistência de uma legislação nacional que uniformize padrões mínimos para utilização de reconhecimento facial percebe-se um importante movimento das agências e órgãos, assim como representantes da sociedade civil, brasileira priorizando a discussão desta temática no País.

A própria Agência Brasileira de Inteligência - ABIN defendeu em discussão pública na câmara dos deputados para a regulação da utilização do reconhecimento facial. Segundo a ABIN é necessário diferenciar vigilância pública e privada e traçar requisitos legais com

[81] Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13964.htm Acesso em: 05 mar. 2021.

limites para a atuação do Estado, uma vez que uso da tecnologia de reconhecimento facial é importantíssimo para suprir necessidades táticas e melhorar a segurança pública do Brasil.[82]

Igualmente merece relevo a existência do Plano Nacional de Segurança Pública e Defesa Social 2018-2028, que ciente da necessidade de fortalecer o aparato de segurança estimula a presença de profissionais de segurança pública, e a fiscalização por reconhecimento facial nas fronteiras, divisas interestaduais, portos, aeroportos, rodoviárias e ferroviárias.[83]

Do Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal

No que toca ao anteprojeto da Lei de Proteção de Dados para Segurança Pública e Persecução Penal84, nota-se, sem sombra de dúvidas, ser este o passo mais importante para consolidação de uma regulamentação da utilização dos dados pessoais para fins de segurança.

Em verdade trata-se ainda de um anteprojeto elaborado por uma comissão de especialistas e juristas com coordenação do ministro do Superior Tribunal de Justiça, Nefi Cordeiro. O referido anteprojeto apelidado como 'LGPD Penal' foi entregue em novembro de 2020 à Camara de Deputados e caminha para os trâmites de aprovação, que inclui a definição de um deputado para assumir a relatoria do projeto.

O anteprojeto da "LGPD Penal" é extenso, composto 12 capítulos e 68 artigos. De forma geral ele busca além de preencher a lacuna normativa quanto à lei específica mencionada no art. 4º da LGPD, dar segurança jurídica para as autoridades que necessitam usar dados pessoais em sua atividade.

Por tratar-se apenas de minuta que certamente desencadeará revisões, modificações e até mesmo vetos caso aprovada, não se mostra necessário uma análise extensiva de forma que iremos sintetizar a proposta, apresentando os pontos que a nosso sentir mais interagem com a temática proposta neste trabalho, afinal, apesar de sua recente divulgação é com toda certeza um projeto de extrema importância no cenário regulatório brasileiro e que contribuirá para um maior amadurecimento do ordenamento jurídico de proteção de dados como um todo e,

[82] Disponível em: https://www.gov.br/abin/pt-br/assuntos/noticias/abin-apoia-regulacao-de-reconhecimento-facial Acesso em: 05 mar. 2021.
[83] Disponível em: https://www.justica.gov.br/sua-seguranca/seguranca-publica/plano-e-politica-nacional-de-seguranca-publica-e-defesa-social.pdf acesso em: 05 mar. 2021.
[84] Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf Acesso em: 08 mar. 2021.

consequentemente, para a utilização e regulação do reconhecimento facial para fins de segurança no Brasil.

Pois bem. Inicialmente cumpre destacar que o anteprojeto tem como matriz principiológica a LGPD, com especial relevo para os direitos dos titulares, para as obrigações dos agentes de tratamento, compartilhamento de dados, e para transferência internacional de dados. Além disto, conforme consta em sua exposição de motivos sua influência vem da Diretiva EU 2016/680.

Em consonância ao cenário legal mais moderno a minuta do anteprojeto propõe regular em seu art. 1º o tratamento de dados pessoais realizado por autoridades competentes para atividades de segurança pública e de persecução penal, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O referido anteprojeto visa disciplinar a proteção de dados pessoais em atividades de segurança pública, aplicando-se a qualquer operação de tratamento realizada por autoridades competentes em atividades de segurança pública e de persecução penal e tem por base os fundamentos elencados abaixo, com vistas também a alcançar ideais de uma sociedade democrática e não sujeita à vigilância:

- ✓ Direito fundamental à proteção de dados pessoais;
- ✓ Exercício da cidadania pelas pessoas naturais, com respeito à dignidade, aos direitos humanos, o livre desenvolvimento da personalidade;
- ✓ Liberdade de comunicação, informação, expressão e pensamento;
- ✓ Autodeterminação informativa;
- ✓ Respeito à vida privada e à intimidade;
- ✓ Confidencialidade e integridade dos sistemas informáticos pessoais
- ✓ Presunção de inocência;
- ✓ Garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal.

Se aprovado será um dos mais importantes marcos regulatórios brasileiros eis que disciplinará a proteção de dados pessoais em atividades de segurança pública e de persecução penal e trará melhores definições de mecanismos, instrumentos e finalidades.

Inclusive neste ponto o anteprojeto buscou trazer em seu artigo 5°, XXI e XXII uma diferenciação importante entre a atividade de segurança pública e atividade de persecução penal, afinal o tratamento dos dados é distinto conforme os interesses e finalidade em cada área. Se na atividade de segurança pública temos o exercício pelo Estado do direito de preservação da segurança e ordem pública, não se tem aqui, num primeiro momento, uma

investigação em curso com pessoas ‘suspeitas’, pois em tese ainda não há crime. Por outro lado, na persecução penal o âmbito de tratamento se dá no exercício de atividades de investigação, apuração, persecução e repressão de infrações penais e execução de penas.

Avançando em sua análise identificamos que tratamento de dados pessoais sensíveis que guarda relação direta ao tema desta investigação está disposto no art. 13 do anteprojeto, determinando ainda a elaboração de relatórios de impacto e informação ao CNJ, sendo esta autoridade diversa da ANPD, prevista LGPD.[85] Observa-se aqui que o anteprojeto trás uma inovação, propõe a aplicação, supervisão e monitoramento pelo Conselho Nacional de Justiça em razão da sua autonomia, pluralidade e imparcialidade, para isto especifica sua função nos artigos 12 e 59.[86]

Destacamos ainda a criação de um novo tipo penal relacionado à transmissão ilegal de dados. Para tanto o artigo 66 altera o código penal brasileiro, criando o Art. 154-C:

> “Art. 66. O Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
> Capítulo V - Dos crimes contra a proteção de dados pessoais (NR)
> Transmissão ilegal de dados pessoais (NR)
> Art. 154-C. Transmitir, distribuir, usar de forma compartilhada, transferir, comunicar, difundir dados pessoais ou interconectar bancos de dados pessoais sem autorização legal para obter vantagem indevida ou prejudicar o titular dos dados ou a terceiro a ele relacionados: (NR) Pena - reclusão, de 1 (um) a 4 (quatro), anos e multa. (NR) Parágrafo único. Aumenta-se a pena de um a dois terços se: (NR) I - os dados pessoais forem sensíveis ou sigilosos; (NR) II - o crime for praticado por funcionário público em razão do exercício de suas funções. (NR)”

Por óbvio o texto do anteprojeto é muito mais detalhista e robusto que qualquer outro e certamente abre caminho para o aperfeiçoamento da discussão e aprovação legislativa que tanto carece o Brasil, contudo, embora tenhamos optado por sintetizar a proposta não podemos deixar de mencionar de forma mais específica o tema disposto no capítulo VII, pois é o que guarda maior proximidade com a temática desta investigação.

Assim sendo, outro importantíssimo recorte trazido pela minuta do anteprojeto diz respeito às tecnologias de monitoramento e tratamento de dados de elevado risco.

---

[85] Art. 13. O tratamento de dados pessoais sensíveis somente poderá ser realizado por autoridades competentes se estiver previsto em lei, observadas as salvaguardas desta Lei. Parágrafo único. A autoridade competente responsável pelo tratamento de dados pessoais sensíveis elaborará relatório de impacto à proteção de dados pessoais e informará o Conselho Nacional de Justiça.

[86] Art. 12. O Conselho Nacional de Justiça emitirá opiniões técnicas ou recomendações referentes às operações de tratamento e deverá solicitar às autoridades competentes responsáveis relatórios de impacto à proteção de dados pessoais.

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”.

Antes de adentrar no capítulo em questão e corroborando o mencionado acima quanto a maior robustez de definições e clareza do texto, o anteprojeto trás seu artigo 5º definições, dentre elas podemos citar as expressas no inciso XXIII, assim para efeitos da referida Lei considera-se tecnologia de monitoramento como:

> "Equipamento, programa de computador ou sistema informático que possa ser usado ou implementado para tratamento de dados pessoais captados ou analisados, entre outros, em vídeo, imagem ou áudio;

Para, além disto, importante a previsão disposta no art. 42 que dispõe :

> "A utilização de tecnologias de monitoramento ou o tratamento de dados pessoais que representem elevado risco para direitos, liberdades e garantias dos titulares dos dados por autoridades competentes dependerá de previsão legal específica, que estabeleça garantias aos direitos dos titulares e seja precedida de relatório de impacto de vigilância."

Em seu § 3º o art.42 estabelece ainda políticas de garantia os direitos dos titulares de dados incluindo o acesso e tratamento de uso interno de tal tecnologia de vigilância; salvaguardas ou medidas de segurança destinadas a proteger as informações coletadas por tal tecnologia contra o acesso não autorizado, incluindo, mas não se limitando à existência de criptografia e mecanismos de controle de acesso; bem como políticas e procedimentos relativos ao acesso ou uso dos dados tratados por tecnologia de vigilância.

Este mesmo artigo também menciona as hipóteses de uso compartilhado, se admitido, e se algum treinamento é exigido pela autoridade competente para um indivíduo realizar o tratamento, usar tal tecnologia de vigilância ou acessar informações tratadas. Por fim, elenca a necessidade de conter uma descrição da auditoria interna e mecanismos de supervisão dentro da autoridade competente, para garantir a conformidade com a política de uso que rege a utilização da tecnologia de vigilância, assim como diretrizes sobre realização, atualização e revisão do relatório de impacto de proteção de dados pessoais.

Em complemento ao artigo 42º, o texto seguinte trata de importante vedação legal com vistas a coibir a vigilância massiva da população com técnicas de identificação de pessoas indeterminadas em tempo real:

> Art. 43. No âmbito de atividades de segurança pública, é vedada a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial.

Nota-se que este capítulo tem papel importantíssimo, pois elenca diversas inovações regulatórias no âmbito da utilização das ferramentas de monitoramento, principalmente no

que tange a vigilância massiva e a vedação imposta para utilização da identificação de forma contínua quando não houver conexão com a atividade de persecução penal.

Especificamente quanto à utilização de ferramentas de monitoramento, vigilância e identificação, verificou-se a dedicação da comissão em buscar estabelecer um nexo de segurança jurídica que possibilite, com transparência e proporcionalidade, a utilização das novas tecnologias na prevenção e investigação.

O anteprojeto prevê critérios mínimos para utilização de tecnologias automatizadas como as de reconhecimento facial e, ainda que necessário regulação por lei específica, a utilização destas tecnologias não poderão ser discriminatórias assim como deverão ser auditadas regularmente para correção de quaisquer lacunas e viés, ela contempla regras mais robustas e claras no que tange a verificação de acurácia da tecnologia com vistas a coibir a possibilidade de discriminação, o que é necessário e se justifica afinal estas tecnologias tem por base a utilização dos dados sensíveis e geram riscos extremos ao cidadão.

Embora a sua justificativa tenha por base o preenchimento da lacuna legislativa quanto a regulação do tratamento de dados no âmbito da segurança pública87, bem como um alinhamento no que tange a cooperação internacional88, o que se percebe da análise do referido anteprojeto é que o mesmo trás uma perspectiva inovadora e necessária ao cenário brasileiro, muito embora ainda seja necessário uma maior discussão para garantia de sua eficácia, transparência e proporcionalidade, o que por óbvio aumenta o grau de responsabilidade das comissões da Câmara e Senado durante o processo de tramitação do projeto e evidência um longo debate pela frente.

3.3.2- Portugal

[87] Conforme justificativa do anteprojeto: "Enorme déficit de proteção dos cidadãos, visto que não há regulação geral sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal, tampouco direitos estabelecidos ou requisitos para utilização de novas tecnologias que possibilitam um grau de vigilância e monitoramento impensável há alguns anos. Apesar do crescimento vertiginoso de novas técnicas de vigilância e de investigação, a ausência de regulamentação sobre o tema gera uma assimetria de poder muito grande entre os atores envolvidos (Estado e cidadão). Nesse contexto, o titular dos dados é deixado sem garantias normativas mínimas e mecanismos institucionais aplicáveis para resguardar seus direitos de personalidade, suas liberdades individuais e até a observância do devido processo legal".

[88] Conforme justificativa do anteprojeto: "O primeiro problema diz respeito à própria eficiência investigativa dos órgãos brasileiros, visto que a falta de adequação aos padrões internacionais de segurança quanto ao fluxo e ao tratamento de dados obsta a integração do Brasil com órgãos de inteligência e de investigação de caráter internacional (v.g., INTERPOL), obstando o próprio acesso a bancos de dados e a informações relevantes, e coloca o uso de aplicações tecnológicas em segurança pública e a adoção de técnicas modernas de investigação sob questionamento de sua validade jurídica."

Verificamos que a utilização da tecnologia de reconhecimento facial vem sendo alargada e em Portugal não é diferente.

Como aborda o relatório do projeto TELEFI - Rumo ao Intercâmbio de Nível Europeu de Imagens Faciais, muito embora não exista um quadro claro sobre a implementação do reconhecimento facial em Portugal para os próximos anos, o reconhecimento facial é utilizado para controle de cidadão estrangeiros nos aeroportos.[89]

Para, além disto, aduz o relatório que atualmente as comparações de imagens faciais são realizadas pelo Laboratório de Polícia Científica apenas com comparações 1:1 sendo "o cenário mais provável é a adição da funcionalidade de pesquisa facial ao atual AFIS e assim, converter o sistema AFIS em um sistema ABIS."[90]

Conforme aborda ainda o Relatório, as imagens faciais em bancos de dados civis que são armazenados para a emissão de cartão cidadão, passaporte e carteiras de motoristas também podem ser usadas para fins de investigação criminal.[91]

No cenário português verificamos que embora parte da legislação relativa a dado biométrico seja comunitária cumpre ressaltar, de início, maior estabilidade regulatória, pois há Leis Nacionais, Diretivas, Regulamentos e uma Autoridade de Controlo mais estruturada e madura, fatos este que conjugados conferem maior segurança jurídica para o tratamento destes dados e dos dados pessoais em geral.

O ordenamento jurídico português conjuga Regulamentos Europeus, cuja aplicação é vinculativa a todos os Estados–membros, a exemplo, o próprio Regulamento Geral de Proteção de Dados.

As Diretivas fixam os objetivos gerais que todos os países da UE devem alcançar com o diferencial de permitir a cada País transpor, para seu ordenamento jurídico interno, através de leis próprias e consoante as suas características, a melhor forma de alcançar tal objetivo, ou

[89] Disponível em https://www.telefi-project.eu/sites/default/files/TELEFI_LegalAnalysis.pdf Acesso em: 09 mar. 2021.

[90] A utilização do Sistema de Identificação de Impressões Digitais (*Automated Fingerprint Identification System*, AFIS) permite comparar os vestígios lofoscópicos recolhidos no cenário de um crime ou em objetos utilizados na sua preparação ou perpetração com o universo de impressões digitais recolhidas numa escala de processamento. A Polícia Judiciária, através do Laboratório de Polícia Científica, é a entidade responsável pelo ficheiro. Conforme indica o relatório do projeto Telefi, há perspectiva que o AFIS português seja convertido futuramente em um ABIS - Sistema Automatizado de Identificação Biométrica. Disponível em https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf Acesso em: 10 mar. 2021.

[91] Segundo o relatório do Projeto TELEFI "O banco de dados de identidade contém fotografias coletadas para a emissão de cartões de cidadão (anteriormente Cartões de identificação). O banco de dados é propriedade do Instituto de Registros e Notários (IRN) que é regido pelo Ministério da Justiça. É o maior banco de dados civil de imagens faciais em Portugal." Disponível em https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf Acesso em: 10 mar. 2021.

seja, permite a elaboração por cada Estado Membro de uma legislação própria para dar cumprimento aos objetivos nelas delimitados. [92]

Pois bem. No que tange ao escopo desta investigação podemos dizer que em Portugal tem aplicação o Regulamento (UE) 2016/679 - RGPD, tendo sua execução através da Lei n.º 58/2019 de 08 de agosto.

Em decorrência do RGPD, tem aplicação a Diretiva (EU) 2016/680 relativa ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, tal diretiva foi transporta para o ordenamento jurídico português pela Lei n.º 59/2019 de 08 de agosto.

Há também a Diretiva (EU) 2016/681 relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, detecção, investigação e repressão das infrações terroristas e da criminalidade grave, transposta pela Lei n.º 21/2019 de 25 de fevereiro.

Além destas normas comunitárias de aplicação obrigatória importa destacar que o cenário português comporta uma legislação específica de videovigilância - Lei nº 1/2005 de 10 de janeiro, que regula a utilização de câmeras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum.[93]

A Lei n.º 1/2005 sofreu algumas alterações ao longo dos anos, mas de modo geral embora anterior ao RGPD e a Diretivas n.º 680/2019 e n.º 681/2019 tem um viés garantístico e, quando conjugado as demais leis, proporciona uma melhor aplicação do binômio segurança x privacidade tão importante no cenário de utilização da videovigilância e reconhecimento facial.

Em seu art.1º a Lei n.º 1/2005 tem seu objeto e âmbito de aplicação ao "regular a utilização de sistemas de vigilância por câmeras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum, para captação e gravação de imagem e som e seu posterior tratamento". [94]

Contudo, tal utilização é considerada lícita desde que atendidos a conjugação do quadro legal vigente e também as finalidades descritas no n.º 1 do art. 2° da Lei n.º 1/2005, dentre os quais, destacamos a "proteção da segurança das pessoas e bens, públicos ou

[92] Disponível em: https://europa.eu/european-union/law/legal-acts_pt acesso em 08 mar. 2021.
[93] Disponível em: https://dre.pt/pesquisa/-/search/457049/details/maximized Acesso em: 09 mar. 2021.
[94] Disponível em: https://dre.pt/pesquisa/-/search/457049/details/maximized Acesso em: 11 mar. 2021.

privados, e prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista razoável risco da sua ocorrência".

Ainda no que pertine ao objeto deste trabalho o art. 4º da referida Lei trás importantes critérios sobre as condições de afixação das câmeras que a saber deverão ser afixadas em local visível e, ainda, com informação sobre sua existência, localização e finalidades, o que vai de encontro as normas gerais de proteção de dados.

Igualmente o capítulo IV que versa sobre as condições de utilização, conservação e registo, trás em seu art.7º os princípios mais importantes para sua utilização: proporcionalidade e adequação. O n.º 1 do art.7º dispõe expressamente que "a utilização de câmaras de vídeo rege-se pelo princípio da proporcionalidade." Já adequação disposta no nº.2 do art. 7° especifica que é "autorizada a utilização de câmaras de vídeo quando tal meio se mostre concretamente o mais adequado para a manutenção da segurança e ordem pública e para a prevenção da prática de crimes, tendo em conta as circunstâncias concretas do local a vigiar". Além disto, expressa de forma clara que "a autorização de utilização de câmeras de vídeo pressupõe sempre a existência de riscos objectivos para a segurança e a ordem pública".

Soma-se a este quadro normativo a Lei n.º 34/2013 sobre o exercício da atividade de segurança privada, cujo objetivo é estabelecer medidas de segurança a adotar por entidades, públicas ou privadas, com vista à proteção de pessoas e bens e à prevenção da prática de crimes, com função complementar à atividade das forças e serviços de segurança do Estado e que apresenta critérios bem definidos quantos aos sistemas de videovigilância utilizados para esta finalidade. [95] Cabe aqui salientar que esta Lei foi posteriormente alterada pela Lei n.º 46/2019 que "altera o regime do exercício da atividade de segurança privada e da autoproteção". [96]

A Lei n.º 34/2013[97] estabelece o regime do exercício da atividade de segurança privada e as medidas de segurança a adotar por entidades públicas ou privadas com vista a prevenir a prática de crimes.

A referida Lei prevê a instalação e utilização de sistemas de vídeovigilância e dedica todo o artigo 31º aos Sistemas de Videovigilância, estabelecendo a forma de utilização, prazo de conservação de dados de 30 dias, transparência e informação. Contudo, devido às mudanças da sociedade foi alterada em 2019 pela Lei n.º 46/2019.

[95] Disponível em: https://data.dre.pt/eli/lei/34/2013/05/16/p/dre/pt/html Acesso em: 06 mar. 2021.
[96] Disponível em: https://data.dre.pt/eli/lei/46/2019/07/08/p/dre Acesso em: 11 mar. 2021.
[97] Disponível em: https://dre.pt/pesquisa/-/search/261089/details/maximized acesso em 11 mar. 2021.

A Lei n.º 46/2019[98] alterou o regime do exercício da atividade de segurança privada e da autoproteção. Dentre as alterações relativas a vídeovigilância o art. 31° passou a determinar não só o prazo de conservação de 30 dias, mas também o prazo de 48h para destruição. Manteve-se a necessidade de informação sobre a vídeovigilância, sendo esta mais genérica, sem indicação do local objeto de vigilância.

O n.º 7 do art.31º dispõe sobre as características e princípios norteadores da utilização da videovigilância ao garantir o acesso em tempo real das imagens pelos serviços de segurança, bem como ter um sistema alarmista que permite fazer alertas em caso de iminente perturbação, risco ou ameaça à segurança de pessoas e bens e ainda o registro de acesso e identificação de quem acende os dados, bem como garantia de inviolabilidade dos dados.

Por fim, cabe destaque ao n.º 10 do referido artigo que afirma que a videovigilância somente pode ser utilizada em conformidade com os princípios da adequação e da proporcionalidade, devendo ainda cumprir as demais normas de tratamento de dados pessoais, e garantia do direito de acesso, informação, oposição de titulares e regime sancionatório.

Dá análise deste quadro legal nacional percebe-se que apresenta melhores condições de tratar a temática. Assim, embora ainda não exista uma Lei nacional que vise regular de forma específica a utilização do reconhecimento facial para fins de segurança, há um quadro normativo que, se conjugado, permite minimizar o risco desta utilização tendo em consideração as normas de proteção de dados e leis de videovigilância.

Ainda neste âmbito merece destaque a Diretiva (UE) 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados[99] que é de suma importância no cenário europeu e português, neste último transposta pela a Lei n.º 59/2019 que se tornou importante também para o cenário brasileiro.

A Diretiva (UE) 2016/680, do ponto de vista legal, é o instrumento mais importante no que concerne a possibilidade de tratamento de dados pessoais e, consequentemente da biometria facial, pois determina regras mínimas a serem transpostas pelos Estados Membros para fins de segurança, no que toca ao tratamento de dados pessoais para prevenção, investigação, detecção ou repressão de infrações penais. Logo, necessário destacar alguns de seus principais pontos.

[98] Disponível em: https://dre.pt/home/-/dre/122996202/details/maximized Acesso em: 12 mar. 2021.
[99] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&rid=1 Acesso em: 12 mar. 2021.

Pois bem. A Diretiva tem um rol muito mais cristalino sobre seus princípios e finalidades assim como seu âmbito de aplicação.

Ela estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública, bem como assegura a proteção dos direitos e das liberdades fundamentais das pessoas singulares e o direito à proteção dos dados pessoais, visto ser este um direito fundamental, assim como visa assegurar o intercâmbio de dados pessoais entre autoridades competentes na União.

No que se refere ao âmbito de aplicação e conforme n.º1 do art. 2º da Diretiva, destina–se ao tratamento pelas autoridades competentes de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento de dados pessoais contidos num ficheiro ou a ele destinados por meios não automatizados.

Ela trás um rol de definições em seu art.3º que facilita a interpretação no que tange ao objeto deste trabalho, ela especifica também no n°.13 do art.13º os dados biométricos como sendo os "dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a sua identificação única, tais como imagens faciais ou dados dactiloscópicos."

Trás em seu art. 4º o rol de princípios norteadores para o tratamento de dados pessoais. De acordo com o referido artigo deverá ser observado licitude do tratamento; recolha para finalidades determinadas, explícitas e legítimas; Adequação e limitação, ou seja, deverão ser tratados de acordo com o mínimo necessário relativamente às finalidades. Deverão ainda ser exatos e atualizados, bem como conservados de forma a permitir a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados, e por fim, garantia de segurança adequada, a fim de evitar o seu tratamento não autorizado ou ilícito e a sua perda, destruição ou danificação acidental, recorrendo a medidas técnicas ou organizativas adequadas.

O art. 8º reforça a licitude do tratamento ao enfatizar que **"**Os Estados-Membros preveem que o tratamento só seja lícito se e na medida em que for necessário para o exercício de uma atribuição pela autoridade competente" e estabelece as condições específicas de tratamento no seu art. 9°.

O art. 10º aborda o tratamento de categorias especiais de dados pessoais, como é o dado biométrico, utilizado por ferramentas de reconhecimento facial. Destaca-se aqui que a

utilização da videovigilância e ferramentas de reconhecimento facial pelas forças de segurança deverão ter em conta este artigo.

O referido art.10º somente autoriza este tratamento se for estritamente necessário e, desde que sujeito não só a garantias adequadas dos direitos e liberdades, mas também se "for autorizado pelo direito da União ou de um Estado-Membro e se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular; ou estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados."

O art.11º também trás critérios importantes no que se refere à proteção das pessoas, permitindo a intervenção humana contra decisões automatizadas, além de proibir as definições de perfis que conduzam à discriminação de pessoas com base nas categorias especiais de dados pessoais, que é um dos riscos das ferramentas de reconhecimento facial se mal utilizadas.

Esta Diretiva elenca ainda os direitos dos titulares, que são similares aos disposto no RGPD, bem como distinção entre diferentes categorias de titulares. Prevê também hipóteses de limitação ao direito de acesso.

Conforme art. 15º da Diretiva, o titular poderá ter seu acesso limitado em casos de possibilidade de prejuízo a inquéritos, investigações ou os procedimentos oficiais ou judiciais; prejuízo à prevenção, detecção, investigação ou repressão de infrações penais ou a execução de sanções penais; para proteger a segurança pública e nacional, assim como os direitos e as liberdades de terceiros. Por óbvio esta limitação deve observar critérios de necessidade e proporcionalidade, tendo em conta os direitos fundamentais e os interesses legítimos das pessoas.

Outro aspecto relevante diz respeito aos conceitos de *by design and by default* presentes no art. 20° que visa assegurar medidas técnicas avançadas para garantir o tratamento de dados tanto no momento da definição dos meios de tratamento como no momento do próprio tratamento.

Ainda com relação à utilização de novas tecnologias e reconhecimento facial, o art. 27º trata da avaliação de impacto sobre a proteção de dados, que a nosso sentir é instrumento importantíssimo para viabilizar a utilização do reconhecimento facial, garantindo transparência e mecanismos de auditoria, bem como o respeito aos direitos e liberdades das pessoas singulares.

O n.º 2 do art.27º descreve os requisitos desta avaliação que deverá conter "uma descrição geral das operações de tratamento de dados previstas, uma avaliação dos riscos para

os direitos e liberdades dos titulares dos dados, as medidas previstas para fazer em face de esses riscos, as garantias, medidas de segurança e mecanismos para assegurar a proteção dos dados pessoais e demonstrar a conformidade, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa".

Portanto, no que se refere ao escopo deste trabalho, a utilização do reconhecimento facial ainda não é regulada por legislação específica, contudo há de se ponderar que isto não impede sua utilização ou avanço na implementação da tecnologia, vez que diante do cenário atual o reconhecimento facial para fins de segurança somente poderá ser utilizado em Portugal se adequado e conjugando as seguintes normas em vigor: Lei n.º 1/2005, Lei n.º 34/2013, Lei n.º 58/2019, Lei n.º 59/2019 - Diretiva (UE) 2016/680, uma vez que, este quadro legal, apesar de complexo conjuga regras mínimas de garantia de tratamento.

Imperioso mencionar também o importante papel que a CNPD - Comissão Nacional de Proteção de Dados[100] exerce em Portugal.

Considerando o âmbito de atuação da CNPD, suas competências, atribuições e poderes previstos no RGPD, nota-se que embora tenha abandonado a autorização prévia prevista na Diretiva 95/46/CE e, com isto, reduzido mecanismos de controle prévio, há ainda, conforme assevera Catarina Pina Gonçalves, "três modalidades de consulta a autoridade de controlo, consubstanciado, estas verdadeiras formas de controlo prévio" (Pinheiro, Coelho, Duarte, Gonçalves, & Gonçalves, 2018).

Assim, considerando ser obrigatória a realização de avaliação de impacto sempre que se verifique elevado risco para direitos e liberdades, conforme previsto no art. 35º do RGPD, a emissão de parecer, prevista no art. 36.º, n.º 4 para elaboração de regulamentação legislativa de proteção de dados ou recomendações e, conforme n.º 5 do art. 36º, a possibilidade de exigir consulta a autoridade de controlo sempre que o tratamento de dados seja no exercício de uma missão de interesse público, verifica-se o importante papel da CNPD em Portugal, evidenciando uma estrutura mais sólida, estruturada e madura.

No que pertine ao objeto deste trabalho, e considerando a Lei de videovigilância n.° 1/2005, compete a CNPD emitir parecer quanto à conformidade das regras de proteção de

[100] A Comissão Nacional de Proteção de Dados (CNPD) é uma entidade administrativa independente, com personalidade jurídica de direito público e com poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto da Assembleia da República. A CNPD controla e fiscaliza o cumprimento do RGPD, da Lei 58/2019, da Lei 59/2019 e da Lei 41/2004, bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos dos seus dados pessoais. Disponível em : https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/ Acesso em: 21 jun. 2021.

dados e o respectivo tratamento dos dados recolhidos, conforme n.º 2 do art. 3º da Lei n .º 9/2012 de 23 de fevereiro.[101]

O nº.7 do mesmo diploma permite ainda a CNPD emitir recomendação para assegurar o cumprimento das finalidades legais, de forma que o cumprimento de suas recomendações poderá viabilizar a emissão de um parecer positivo.

Igualmente, compete a CNPD emitir parecer nos casos previstos nos n.º s 4,6 e 7 do art. 7º. Ou seja, sempre que houver solicitação de instalação de câmeras fixas em locais públicos, mas que de sua utilização decorra captação de imagens do interior de residências ou possibilite gravação de som, o que por óbvio gera afetação a intimidade das pessoas.

A fim de melhor ilustrar este cenário português com envolvimento da CNPD, podemos citar o Parecer da CNPD n.º 2020/80[102], que teve como objeto o pedido de alargamento do sistema de videovigilância na cidade da Amadora pela PSP - Polícia de Segurança Pública. Este alargamento previa a monitorização da circulação das pessoas, viaturas e bens, bem como a utilização de tecnologia de inteligência artificial e sistema biométrico de reconhecimento facial.

Conforme exposto no parecer, a CNPD afirma que "as incivilidades, ainda que ilícitas, se apresentam como mera tensão da ordenação social e, portanto, não justificam a restrição de direitos, liberdades e garantias". De igual modo afirma que a pretensão de utilização de um sistema de videovigilância para "monitorização a circulação de pessoas e viaturas na cidade da Amadora vai muito além da finalidade invocada pela lei, não existindo enquadramento legal e constitucional".

O parecer afirma ainda que o tratamento dos dados pessoais decorrente de sistemas de videovigilância deve-se se restringir a "finalidade de proteção da segurança de pessoas e bens em relação a condutas criminalizadas e de prevenção criminal, de acordo com a lei e Constituição portuguesa".

No que tange a utilização da tecnologia de inteligência artificial e reconhecimento facial, o parecer é negativo. Segundo a CNPD, ainda que *IA* se mostre adequada em certas circunstâncias, ou seja, para proteção de condutas criminalizadas, a necessidade de sua utilização carece de demonstração, uma vez que sua utilização gera risco elevado para

[101] Lei n.º 9/2012 de 23 de fevereiro: Procede à terceira alteração à Lei n.º 1/2005, de 10 de janeiro, que regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum. Disponível em: https://dre.pt/pesquisa/-/search/542867/details/maximized acesso em: 21 jun. 2021.

[102] Disponível em: https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2020&type=4&ent= Acesso em: 21 jun. 2021.

direitos, liberdades e garantias das pessoas de modo que apenas o apelo a segurança não é suficientemente permissivo.

Conforme consta do parecer, a utilização requerida pela PSP pressupõe o rastreamento não só de deslocações, mas também de comportamentos das pessoas, o que sucede num condicionamento de liberdades, incompatível com a dignidade humana e preceitos de um Estado Democrático. Soma-se a isto o fato de que o monitoramento discriminatório de certos perfis pode ser facilmente alcançado.

Logo, assente em seu papel, a CNPD concluiu que a necessidade da utilização de reconhecimento facial não ficou demonstrada, assim como as garantias adequadas de tratamentos de dados pessoais. Igualmente, suscitou que não foi exposto a descrição de algoritmos envolvidos na comparação e detecção de padrões, bem como restou omisso quanto aos critérios envolvidos nos padrões e margens de falso positivo/negativo. A CNPD ainda observou que tal tecnologia sequer foi alvo de análise na avaliação de impacto apresentada pela PSP.

Assim, diante das ponderações que lhe cabiam quanto à conformidade do pedido a CNPD acabou por vedar expressamente sua utilização:

> (...) 2.Ainda assim, mesmo para esta finalidade, a utilização de Inteligência Artificial(máxime, de soluções de *soft recognition e Machine Learning)* nos sistemas de videovigilância carece de um específico enquadramento em termos de pressupostos e condições limites da sua aplicação, o qual, no caso, não existe, não tendo sequer sido objeto de apreciação na avaliação de impacto sobre proteção de dados apresentada; nestes termos, a CNPD entende não ser admissível a sua utilização.
> 3. Também a utilização do sistema biométrico de reconhecimento facial na Cidade da Amadora carece de específico fundamento legal, estando por isso manifestamente vedada.
> 4. A CNPD recomenda ainda que sejam corrigidos os aspectos de tratamento de dados pessoais realizados com a utilização do sistema de videovigilância explanados no ponto 3.2.

Pois bem. Para além deste quadro português que se mostra mais maduro, é possível constatar a nível europeu um quadro regulatório ainda mais extenso e complexo, composto por normas comunitárias relacionadas à área de segurança e migração que apresentam certos níveis de utilização e regulação da biometria facial e proteção de dados, dentre os quais podemos citar:

REGULAMENTO (UE) N.º 2018/1861 DO PARLAMENTO EUROPEU E DO CONSELHO - SIS II – *border checks*[103] – contém regras específicas quanto ao estabelecimento, funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos de fronteira. Em seu capítulo VI - consulta com recurso a dados biométricos, dispõe nos artigos 32º e 33º sobre regras específicas para a introdução de fotografias, imagens faciais e dados dactiloscópicos e regras específicas para a verificação ou consulta com recurso a fotografias, imagens faciais e dados dactiloscópicos.

REGULAMENTO (UE) N.º 2018/1860 DO PARLAMENTO EUROPEU E DO CONSELHO[104] - SIS II – Regresso - que tem por objetivo estabelecer as condições e os procedimentos a aplicar à nacionais de países terceiros visados por decisões de regresso emitidas pelos Estados-Membros no Sistema de Informação de Schengen (SIS), estabelecido pelo Regulamento (UE) 2018/1861, bem como intercâmbio de informações suplementares sobre essas indicações, prevê também em seu artigo 4° a introdução no sistema SIS dos dados biométricos e faciais visando por óbvio maior controle no regresso de nacionais de países terceiros.

REGULAMENTO (UE) N.º 2017/2226 DO PARLAMENTO EUROPEU E DO CONSELHO[105] - estabelece o Sistema de Entrada/Saída (SES) para registo dos dados das entradas e saídas e dos dados das recusas de entrada dos nacionais de países terceiros aquando da passagem das fronteiras externas dos Estados-Membros, e determina as condições de acesso ao SES para efeitos de aplicação da lei. Dentre as principais normas estabelecidas destacam-se as dispostas no art. 15 ° e 27° que trata das imagem facial dos nacionais de países terceiros.

Necessário mencionar também o Regulamento VIS[106], qual seja, o REGULAMENTO (CE) N. º 767/2008 DO PARLAMENTO EUROPEU E DO CONSELHO de 9 de Julho

[103] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32018R1861 Acesso em: 18 out. 2020.
[104] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32018R1860&from=PT acesso em: 18 out. 2020.
[105] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32017R2226&from=PT acesso em 18 out. 2020.
[106] Conforme Considerando nº 5: O VIS deverá ter por objectivo melhorar a aplicação da política comum de vistos, a cooperação consular e a consulta entre as autoridades centrais responsáveis pelos vistos ao facilitar o intercâmbio de dados entre os Estados-Membros sobre os pedidos de vistos e as decisões relativas aos mesmos, a fim de facilitar o procedimento de pedido de visto, prevenir a busca do visto mais fácil («*visa shopping*»), facilitar a luta contra a fraude e facilitar os controlos nos pontos de passagem das fronteiras externas e no território dos Estados-Membros. O VIS deverá igualmente contribuir para a identificação de qualquer pessoa que não preencha ou tenha deixado de preencher as condições para a entrada, a permanência ou a residência no território dos Estados-Membros, e facilitar a aplicação do Regulamento (CE) n.º 343/2003 do Conselho, de 18 de Fevereiro de 2003, que estabelece os critérios e mecanismos de determinação do Estado-Membro

de 2008[107] que tem por objetivo facilitar a troca de dados entre Estados-Membros Schengen em pedidos de visto e funciona como um verdadeiro sistema para o intercâmbio de dados sobre vistos entre Estados-Membros.

Dentre os artigos do regulamento destacamos o artigo 3°, que aponta a disponibilidade dos dados do sistema VIS para efeitos de prevenção, detecção e investigação das infracções terroristas e de outras infracções penais graves, já indicando finalidade de aplicação da lei na garantia da segurança dos estados membros, nomeadamente quanto ao terrorismo, ou seja, a disponibilização dos dados VIS com objetivo de prevenção e repressão ao terrorismo.

Outro importante regulamento europeu que consolidou a sistemática da utilização dos dados biométricos e hoje se mostra importante ferramenta dos Estados Membros é o EURODAC.

O REGULAMENTO (UE) N.º 603/2013 DO PARLAMENTO EUROPEU E DO CONSELHO de 26 de junho de 2013[108] cria o sistema Eurodac de comparação de impressões digitais para efeitos da aplicação efetiva do Regulamento (UE) N.º 604/2013, que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de proteção internacional apresentado num dos Estados-Membros por um nacional de um país terceiro ou um apátrida, e de pedidos de comparação com os dados Eurodac apresentados pelas autoridades responsáveis dos Estados-Membros e pela Europol para fins de aplicação da lei e que altera o Regulamento (UE) N.º 1077/2011 que cria uma Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça.

Muito embora *a priori* o Eurodac trate apenas de dados biométricos datisloscópicos, ou seja, as impressões digitais, fato é sua utilização tem por base a prevenção, detecção ou investigação de infrações terroristas ou outras infrações penais graves, bem como as garantias necessárias para assegurar a proteção do direito fundamental ao respeito pela vida privada dos indivíduos cujos dados pessoais são objeto de tratamento no Eurodac.[109]

---

responsável pela análise de um pedido de asilo apresentado num dos Estados-Membros por um nacional de um país terceiro ([3]), e contribuir para a prevenção de ameaças à segurança interna dos Estados-Membros.

[107] Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32008R0767&from=PT Acesso em: 18 out. 2020

[108] Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32013R0603 Acesso em: 18 out. 2020.

[109] Considerando nº 15 do REGULAMENTO (UE) Nº 603/2013 DO PARLAMENTO EUROPEU E DO CONSELHO de 26 de junho de 2013. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32013R0603 Acesso em: 18 out. 2020.

Mais recentemente, o REGULAMENTO (UE) N.º 2019/816 DO PARLAMENTO EUROPEU E DO CONSELHO de 17 de abril de 2019[110] passou a abordar a utilização de reconhecimento facial e imagem facial, mas apenas para fins de identidade de uma pessoa, ou seja, apenas para confirmação de identidade, inclusive, nota-se que sua disposição converge para que a utilização automatizada de imagens faciais possa ocorrer no futuro, mas apenas em casos de necessidade e desde que salvaguardadas a proporcionalidade e que os softwares de reconhecimento facial assim possam ser executados, ou seja, a utilização e tratamento de imagens faciais deverá ser realizada estritamente para confirmar a identidade, devendo respeitar os direitos fundamentais e estar em conformidade com as regras da União aplicáveis em matéria de proteção de dados.

O Regulamento (UE) n.º 2019/816 cria um sistema centralizado para a determinação dos Estados-Membros que possuem informações sobre condenações de nacionais de países terceiros e de apátridas (ECRIS-TCN), tendo em vista completar o Sistema Europeu de Informação sobre Registos Criminais e altera o Regulamento (UE) 2018/1726.

Conforme considerando nº 5 o ECRIS-TCN deverá conter apenas informações sobre a identidade de nacionais de países terceiros objeto de condenação por um tribunal penal da União. Essas informações relativas à identidade deverão incluir dados alfanuméricos e dactiloscópicos. Deverá ser possível inserir imagens faciais, na medida em que o direito do Estado-Membro em que a condenação é proferida permita a recolha e o armazenamento de imagens faciais de pessoas objeto de condenação.

O Considerando 24 aduz que:

> "Numa primeira fase, as imagens faciais inseridas no ECRIS-TCN só deverão ser utilizadas para efeitos de confirmação da identidade de um nacional de um país terceiro a fim de identificar o Estado-Membro ou Estados-Membros que possuem informações sobre condenações anteriores desse nacional de um país terceiro. No futuro, deverá ser possível que as imagens faciais possam ser utilizadas para fins de correspondência biométrica automatizada, desde que sejam cumpridos os requisitos técnicos e estratégicos para esse efeito. Tendo em conta a necessidade e a proporcionalidade, bem como a evolução técnica no domínio do software de reconhecimento facial, a Comissão deverá avaliar a disponibilidade e o grau de preparação da tecnologia exigida antes de adotar um ato delegado relativo à utilização de imagens faciais para efeitos de identificação de nacionais de países terceiros, a fim de identificar o Estado-Membro ou Estados-Membros que possuem informações sobre condenações anteriores relativas a essas pessoas".

[110] Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32019R0816 acesso em 18 out. 2019.

Artigo 6° do Regulamento trata especificamente das imagens faciais: "As imagens faciais podem ser utilizadas exclusivamente para confirmar a identidade do nacional de país terceiro que tenha sido identificado em resultado de uma pesquisa alfanumérica ou de uma pesquisa com recurso a dados dactiloscópicos".

Contudo, o n.°2 do referido artigo menciona que a "Comissão fica habilitada a adotar atos que completem o presente regulamento para garantir utilização de imagens faciais desde que tendo em conta a necessidade e a proporcionalidade, bem como a evolução técnica no domínio do software de reconhecimento facial, avalia a disponibilidade e o estado de desenvolvimento da tecnologia necessária."

O REGULAMENTO (UE) N.º 2019/817 DO PARLAMENTO EUROPEU E DO CONSELHO de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho, e as Decisões 2004/512/CE e 2008/633/JAI do Conselho.[111]

Conforme considerando n.°1 o objetivo deste Regulamento é alcançar a interoperabilidade entre os sistemas de informação da UE para a segurança e a gestão de fronteiras e da migração, a fim de enfrentar as deficiências estruturais relacionadas com estes sistemas que dificultam o trabalho das autoridades nacionais, e assegurar que os guardas de fronteira, as autoridades aduaneiras, os agentes de polícia e as autoridades judiciárias têm as informações necessárias à sua disposição.

Já o considerando 18 aduz que:

> "Os dados biométricos, como as impressões digitais e as imagens faciais, são únicos e, por conseguinte, muito mais fiáveis do que os dados alfanuméricos para efeito de identificação de uma pessoa. O serviço partilhado BMS deverá constituir um instrumento técnico para reforçar e facilitar o trabalho dos sistemas de informação da UE pertinentes e de outros componentes de interoperabilidade. O principal objetivo do serviço partilhado BMS deverá consistir na facilitação da identificação de uma pessoa que possa estar registada em várias bases de dados, procurando correspondências com os seus dados biométricos nos diferentes sistemas e baseando-se num único componente tecnológico em vez de em diversos componentes, em cada um dos sistemas subjacentes. O serviço partilhado BMS trará vantagens em termos de segurança, bem como em termos financeiros, de manutenção e operacionais. Todos os sistemas automáticos de identificação dactiloscópica, incluindo os que são presentemente utilizados no Eurodac, VIS e SIS, utilizam modelos biométricos constituídos por dados provenientes de uma

[111] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0817&from=DE Acesso em: 19 out. 2020.

> extração de características de amostras biométricas reais. O serviço partilhado BMS deverá reunir e armazenar todos estes modelos biométricos — separados, segundo um método lógico, de acordo com o sistema de informação de que provêm os dados — num único local, facilitando assim as comparações entre sistemas, mediante utilização de modelos biométricos, e permitindo economias de escala no desenvolvimento e manutenção de sistemas centrais da UE."

O regulamento visa garantir a interoperabilidade entre o Sistema de Entrada/Saída (SES), o Sistema de Informação sobre Vistos (VIS), o Sistema Europeu de Informação e Autorização de Viagem (ETIAS), o Eurodac, o Sistema de Informação Schengen (SIS) e o Sistema Europeu de Informação sobre os Registos Criminais de nacionais de países terceiros (ECRIS-TCN).

Prevê ainda um Portal Europeu de Pesquisa (ESP) em seu artigo 6º para facilitar o acesso rápido das autoridades dos Estados-Membros e das agências da União aos sistemas de informação da UE, aos dados da Europol, Interpol, acesso ao SES, ao VIS, ao ETIAS, ao Eurodac, ao SIS e ao ECRIS-TCN .

Com um serviço partilhado de correspondências biométricas (serviço partilhado BMS), um repositório comum de dados de identificação, um detector de identidades múltiplas (MID), ele visa adaptar e facilitar os procedimentos para fins de prevenção, detecção ou investigação de infrações terroristas ou de outras infrações penais graves.

Destaca-se, também, as disposições sobre os requisitos de qualidade dos dados, a elaboração de relatórios e estatísticas (e as responsabilidades dos Estados-Membros e da Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço da liberdade, segurança e justiça (eu-LISA), no que diz respeito à conceção, ao desenvolvimento e ao funcionamento dos componentes de interoperabilidade.

REGULAMENTO (UE) N.º 2019/818 DO PARLAMENTO EUROPEU E DO CONSELHO, DE 20 DE MAIO DE 2019[112], juntamente com o Regulamento (UE) 2019/817 estabelece um quadro para a interoperabilidade entre os sistemas de informação da UE no domínio da cooperação policial e judiciária, asilo e migração, para que os sistemas se complementem.

Pois bem. Diante deste quadro complexo e extenso de regulamentos constatamos que a União Europeia tem bases mais sólidas e maduras para garantir a proteção de dados e o tratamento automatizados da biometria facial em conformidade.

[112]Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0818&from=EN Acesso em: 19 out. 2020.

Não obstante, a utilização e regulação da tecnologia de reconhecimento facial é um tema vivo, em constante mutação, e vem desencadeado uma forte discussão entre os Estados-Membros sobre os riscos e impactos em direitos fundamentais. Tanto é assim que a Agência de Direitos Fundamentais da União Europeia - FRA, publicou em 2019 um artigo de relevada importância, qual seja: "Tecnologia de Reconhecimento facial: considerações de direitos fundamentais no contexto da aplicação da Lei" [113] que visa abordar as implicações da utilização da tecnologia de reconhecimento facial nos direitos fundamentais. (AGENCY FOR FUNDAMENTAL RIGHTS, 2019)

O artigo converge com a análise desta investigação quanto os riscos envolvidos e ainda aponta os projetos de pesquisa e discussões sobre a potencial aplicação da tecnologia de reconhecimento facial na área de segurança e gestão de fronteiras, além disto informa que a Comissão Europeia está realizando vários estudos e discutindo a expansão da utilização dos dados biométricos para viabilizar e melhorar as capacidades dos seus sistemas com fito de garantir maior intercâmbio de informações entre Estados Membros. (AGENCY FOR FUNDAMENTAL RIGHTS, 2019)

Dentre os estudos e projetos citados destacamos o projeto TELEFI - Rumo ao intercâmbio de nível europeu de imagens faciais. Este projeto de pesquisa examina como o reconhecimento facial está sendo atualmente usado para a investigação de crime em todos Estados Membros. O projeto é implementado pelos Departamentos Forenses de Finlândia, Letônia, Suécia e Holanda, sob a liderança do Ministério da Justiça da Estônia. (AGENCY FOR FUNDAMENTAL RIGHTS, 2019)

O relatório do projeto TELEFI foi disponibilizado em fevereiro de 2020 e seus resultados apontaram para mesma direção desta investigação quanto à necessidade de reconhecer que o quadro regulatório da União Europeia é extenso e complexo, e que não existe um instrumento regulatório único e específico sobre a regulação do reconhecimento facial na União Europeia.

O relatório também indica ser imperioso observar que a nível europeu, a Diretiva (UE) 2016/680, é o instrumento mais importante no que concerne a possibilidade de tratamento da biometria facial e sistemas de reconhecimento facial, vez que elenca regras mínimas a serem

[113] Disponível https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law Acesso em: 19 out. 2020.

transpostas pelos Estados Membros para fins de segurança e tratamento de dados pessoais para prevenção, investigação, detecção ou repressão de infrações penais.[114]

Dentro ainda do escopo deste trabalho, cumpre destacar o surgimento da proposta de um Regulamento Europeu com vistas a harmonizar regras em matéria de Inteligência Artificial. A proposta de Regulamento de Inteligência Artificial apresentada em 21 de abril de 2021 garantirá a segurança e a defesa dos direitos fundamentais das pessoas e das empresas, reforçando simultaneamente o investimento, a inovação e a utilização da inteligência artificial, em toda a União Europeia.[115]

As regras seguem uma abordagem baseada no risco, onde todos os sistemas de identificação biométrica à distância são considerados de risco elevado e sujeitos a requisitos rigorosos. Deste modo, a utilização em tempo real de sistemas de reconhecimento facial associado à inteligência artificial será, em princípio, proibida, ainda que para fins de segurança. Conforme consta da proposta, ainda que haja exceções estas são estritamente definidas e regulamentadas, como por exemplo, "quando for necessário procurar uma criança desaparecida, para prevenir uma ameaça terrorista específica e iminente ou para detetar, localizar, identificar ou julgar um autor ou suspeito de uma infração penal grave".[116]

A proposta cuja previsão de aplicação é dois anos após sua aprovação elenca de forma expressa práticas de inteligência artificial proibidas, a classificação de sistemas de inteligência artificial conforme o risco e requisitos aplicáveis, obrigações de fornecedores e utilizadores de sistemas, normas de avaliação, conformidade, certificação e registo, bem como obrigações de transparência aplicáveis a determinados sistemas de inteligência artificial e medidas de apoio à inovação, dispõe ainda sobre código de condutas, sanções dentre outras normas de governação e execução.[117]

A proposta do Regulamento da Inteligência Artificial representa uma importante alteração e atualização no quadro legislativo europeu que considera de forma expressa a evolução destas tecnologias e seus impactos, bem como tem ciência de sua necessidade para o desenvolvimento da sociedade, indicando mais uma vez a posição pioneira e equilibrada na qual a EU sustenta a proteção dos direitos fundamentais.

---

[114] Disponível em: https://www.telefi-project.eu/sites/default/files/TELEFI_LegalAnalysis.pdf Acesso em: 10 mar. 2021.

[115] Disponível em: https://ec.europa.eu/portugal/news/Europe-fit-for-the-Digital-Age-EC-proposes-new-rules-and-actions-for-excellence-and-trust-in-Artificial-Intelligence_pt Acesso em: 21 jun. 2021.

[116] Disponível em: https://ec.europa.eu/portugal/news/Europe-fit-for-the-Digital-Age-EC-proposes-new-rules-and-actions-for-excellence-and-trust-in-Artificial-Intelligence_pt Acesso em: 21 jun. 2021.

[117] Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC_1&format=PDF Acesso em: 21 abr. 2021.

Portanto, após a análise exploratória do quadro regulatório luso brasileiro é possível verificar que Portugal se mostra um passo à frente do Brasil. Os instrumentos regulatórios existentes quando conjugados evidenciam maior maturidade do ordenamento jurídico de Portugal uma vez que as Leis nacionais, somadas ao conjunto de normas comunitárias, conferem maior solidez ao tratamento de dados pessoais para fins de segurança.

Assim, muito embora não exista ainda uma Lei específica sobre o uso da tecnologia de reconhecimento facial, há um vasto quadro legal, que prevê desde critérios de videovigilância interna e proteção de dados até o tratamento de dados de biometria facial pelas autoridades europeias de segurança e migração.

CONCLUSÃO

A segurança é uma tarefa que hoje exige uma visão múltipla e se traduz em um conceito holístico.

Ainda que sempre se relacione com suas premissas originárias de se fazer seguro foi possível perceber ao longo deste trabalho que, com o passar do tempo e desenvolvimento da sociedade, deixou sua visão estatocentrica, agregando novas aceções como de *safety e security*. A segurança passou a centrar-se no indivíduo, tendo como principal expoente a concretização da segurança humana.

A segurança se consolidou no cenário internacional como mecanismo de bem estar coletivo. Neste sentido, sua função primeira continua em pleno vigor, ela apenas deixou de se centrar numa questão de poderio bélico e estatal para, diante da globalização e novos riscos, centrar-se no indivíduo, tendo por base uma compreensão multissetorial das inseguranças que envolve o ser humano.

Ela foi consagrada no cenário internacional como direito fundamental. Os direitos fundamentais são a essência basilar de qualquer Estado Democrático e, neste aspecto, Brasil e Portugal reconhecem em seus ordenamentos jurídicos a segurança como direito fundamental.

Relativamente à privacidade igualmente há positivação e reconhecimento em ambos os ordenamentos jurídicos.

A privacidade se revelou um conceito elástico e, apesar de comportar inicialmente a ideia de ser deixado só, ou não ser exposto a público, o desenvolvimento da sociedade fez como que este direito fosse se reposicionando ao longo do tempo. Foi também positivada

como direito fundamental nas Constituições de Brasil e Portugal, assim como no cenário internacional.

Resta evidente, portanto, que a privacidade, assim como a segurança, são pilares para o desenvolvimento da dignidade humana e democracia.

Contudo, com o advento da sociedade de informação percebe-se uma maior expectativa e alargamento da privacidade, conquanto se observa sua fragilidade diante das novas tecnologias que garantem as mais diversas e rápidas formas de interação. Nesta sociedade hiperconectada que hoje vivemos, o fluxo de dados tornou-se critério de sobrevivência.

Os dados pessoais são matérias primas e justamente por isto foram também consagrados a direito fundamental, evidenciando um novo capítulo da privacidade.

Nesta reconfiguração e alargamento da privacidade temos o reconhecimento da tutela de proteção de dados e nos chama á atenção o contributo europeu, que ao longo da história se desenvolveu através de vários diplomas até a entrada em vigor do Regulamento Geral de Proteção de Dados.

No Brasil o maior reflexo deste contributo culminou na aprovação da Lei Geral de Proteção de Dados e no recente reconhecimento da proteção de dados como direito fundamental pelo Supremo Tribunal Federal, seguindo novamente os passos europeus.

Dentre os elementos abordados numa dimensão comparativa entre as legislações de proteção de dados foi possível constatar de fato que o modelo brasileiro tem sua fonte no RGPD. Como crítica, do ponto de vista da norma posta, verificamos que a LGPD comporta algumas deficiências no que tange ao encadeamento de definições e formas de tratamento que evidenciam sua fragilidade se comparada ao RGPD. Devido a esta fragilidade há um consenso entre os operadores de Direito no que tange a necessidade de recorrer ao Regulamento Europeu para sanar lacunas.

Podemos afirmar que o cenário brasileiro necessita não só de um amadurecimento da proteção de dados do ponto de vista legal, mas também social, isto se deve naturalmente a ausência de uma cultura firme de proteção de dados, que no caso de Portugal e UE se desenvolveu ao longo dos anos estando hoje muito mais sólida e rica.

Ainda no tocante à proteção de dados importante foi a verificação de alguns conceitos e formas de tratamentos do dado biométrico, eis que estes dados são utilizados para reconhecimento facial.

Como visto, há mais convergências que divergências. O RGPD, contudo, é mais rígido que a LGPD, mas de maneira geral podemos dizer que os dados biométricos somente podem ser tratados de forma excepcional, para finalidades restritas e especificadas em lei, sendo ainda observada a conformidade, proporcionalidade, respeito à proteção de dados e prestação de garantias adequadas.

Dentre as exceções para tratamento destes dados destacam-se as finalidades relacionadas à segurança.

Assim, considerando que a utilização da tecnologia de reconhecimento facial vem sendo alargada em diversos setores e na área de segurança se torna importante instrumento de proteção e persecução penal, contribuindo não só para melhoria da prestação de serviço e monitoramento pelas forças de segurança pública, mas também para busca por desaparecidos, controle migratório ou busca por foragidos é de se ponderar os riscos intrínsecos a esta tecnologia que é falível por natureza, a fim de garantir o equilíbrio do binômio segurança e privacidade, visto que ambos são direitos fundamentais.

Assim, foi necessário analisar se há instrumentos regulatórios específicos e eficazes no que tange à utilização do reconhecimento facial para fins de segurança, bem como foi necessário analisar o grau de maturidade dos ordenamentos jurídicos, a partir da estruturação do quadro legal vigente, ou seja, a maturidade foi avaliada conforme instrumentos jurídicos em vigor e conforme as garantias mínimas que estes proporcionam para o equilíbrio entre os direitos fundamentais, nomeadamente segurança, privacidade, proteção de dados e dignidade humana.

No cenário português foi possível constatar a existência de um quadro jurídico mais sólido, tanto para proteção de dados como para tratamento de dados biométricos para fins de segurança e migração.

Foi possível verificar ainda que embora parte da legislação relativa a dado biométrico seja comunitária há em Portugal maior estabilidade regulatória se comparado ao Brasil. Embora se revele um quadro fragmentado, em que não exista um instrumento específico que regule o reconhecimento facial para fins de segurança, há leis nacionais como por exemplo a Lei de videovigilância, Diretivas e Regulamentos Europeus que conjugados conferem maior segurança jurídica para o tratamento dos dados biométricos para fins de segurança.

Notamos também que o quadro regulatório da União Europeia é extenso e complexo e que não existe um instrumento regulatório único, específico sobre a regulação do reconhecimento facial, porém é imperioso observar que a nível europeu, a Diretiva (UE) n.º

2016/680, do ponto de vista legal, é até o momento, o instrumento mais importante no que concerne a possibilidade de tratamento da biometria facial, pois determina regras mínimas a serem transpostas pelos Estados Membros para fins de segurança, no que toca ao tratamento de dados pessoais para prevenção, investigação, detecção ou repressão de infrações penais, tendo sido trasposta ao ordenamento jurídico português pela Lei n.º 59/2019 de 08 de agosto de 2019.

Logo é possível concluir que há no cenário português um maior nível garantístico e uma maior maturidade para o tratamento dos dados pessoais e biométricos e, consequentemente, para utilização do reconhecimento facial.

Em contrapartida, no cenário brasileiro as Leis ou projetos existentes sobre reconhecimento facial se revelam instrumentos insatisfatórios, que não proporcionam a regulação de forma adequada e uniforme, assim como não preveem garantias mínimas de proteção de dados e respeito aos direitos e garantias fundamentais.

Como vimos a maior parte dos projetos de lei sobre reconhecimento facial no Brasil está interessado na pergunta: ‘’Você é quem afirma ser?’’ e se limitam a prever a implantação dos sistemas de reconhecimento facial em determinados setores.

A Lei do Distrito Federal, longe de ser ideal, é a que mais se aproxima em sanar o vazio normativo naquele ente federativo e mesmo a considerando um avanço do ponto de vista legal é de certa forma bastante genérica e demanda regulação de pontos omissos e melhores definições para, em consonância com a LGPD, proporcionar maior segurança jurídica e evitar violação de direitos e monitoramento massivo da população.

Contudo, considerando a inexistência de uma lei nacional para fins de segurança ou que vise à regulação do reconhecimento facial é inegável a inovação e contributo desta Lei Distrital.

No que toca ao anteprojeto da LGPD Penal, trata-se ainda de uma perspectiva que demanda esforços legislativos e inúmeras discussões para aperfeiçoamento e apesar da pretensão de ser um instrumento nacional de regulação do tratamento de dados para fins de segurança pública e persecução penal, comporta lacunas quanto à regulação específica das ferramentas de reconhecimento facial.

Logo, é de se concluir que até o momento de elaboração desta dissertação, não há no cenário brasileiro uma legislação que a nível nacional, regule de forma eficaz a utilização dos dados pessoais para fins de segurança, bem como regule o tratamento de dados de biometria facial e o emprego das ferramentas de reconhecimento facial. Muito embora existam

instrumentos de regulação na esfera estadual estes em sua maioria são genéricos e insatisfatórios, e não atendem a critérios mínimos de garantias de proteção de dados e Direitos Fundamentais.

Este fato se deve, a nosso sentir, a ausência de uma maturidade global do ordenamento jurídico brasileiro para tratar o tema, recorde-se aqui apenas recentemente a proteção de dados foi reconhecida como direito fundamental o que evidencia que ordenamento brasileiro ainda caminha para a consolidação de uma cultura jurídica e social de proteção de dados que em contrapartida é muito mais madura em Portugal.

Assim, após este estudo exploratório e em resposta as questões iniciais, podemos dizer que no cenário brasileiro, a despeito da perspectiva trazida no anteprojeto da LGPD Penal, o campo regulatório até o momento de elaboração desta investigação deixa a desejar se comparado a Portugal. Embora em ambos os ordenamentos jurídicos não exista um instrumento regulatório específico sobre a utilização do reconhecimento facial para fins de segurança, Portugal está um passo a frente devido à maturidade espelhada no quadro legal vigente, que advém da conjugação de leis nacionais, regulamentos e diretivas, nomeadamente a Diretiva (EU) n.º 2016/680, que até o momento é o principal instrumento regulador da utilização dos dados pessoais para fins de segurança, além do papel fundamental exercido por sua autoridade de controlo, a CNPD. Somam-se a isto os estudos e as propostas de regulação da inteligência artificial, bem como as intensas discussões e debates sobre a utilização do reconhecimento facial que estão a decorrer no cenário europeu.

REFERÊNCIAS BIBLIOGRÁFICAS

ADECECIJA. (2020). Reconhecimento Facial nos Estádios de futebol: Inteligência Artificial banida da União Europeia? Acesso em 11 de Outubro de 2020, disponível em https://adcecija.pt/reconhecimento-facial-nos-estadios-de-futebol-inteligencia-artificial-banida-da-uniao-europeia/

AGENCY FOR FUNDAMENTAL RIGHTS. (2019). *Facial recognition technology:fundamental rights considerations in the context of law enforcement*. Acesso em 10 de março de 2021, disponível em https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

AGENCY FOR FUNDAMENTAL RIGHTS. (2019). *Facial recognition technology:fundamental rights considerations in the context of law enforcement*. Acesso em 12 de Outubro de 2020, disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

ALENCAR, M. N. (2015). Debates dos Estudos de Segurança Internacional e Segurança Humana: uma breve análise sobre a evolução dos Estudos de Segurança. Conjuntura Global, Vol. 4, n. 2, maio/ago., p. 185-195. Acesso em 10 de dezembro de 2020, disponível em https://revistas.ufpr.br/conjgloblal/article/viewFile/43172/26168

ALENCAR, M. N. (2016). Segurança Humana: qual a relação da segurança humana com o debate conceitual de violência e paz dentro dos estudos de segurança internacional. Acesso em 10 de dezembro de 2020, disponível em http://www.humanas.ufpr.br/portal/nepri/files/2016/11/artigo-workshop.pdf

AMAZON. (s.d.). Os fatos sobre a tecnologia de reconhecimento facial com inteligência artificial. Acesso em 10 de outubro de 2020, disponível em https://aws.amazon.com/pt/rekognition/the-facts-on-facial-recognition-with-artificial-intelligence/

APPLE. (s.d.). Acerca da tecnologia avançada do Face ID. Acesso em 10 de outubro de 2020, disponível em https://support.apple.com/pt-pt/HT208108

BAIÃO, K. S., & Gonçalves, K. C. (2014). A Garantia da Privacidade na Sociedade Tecnológica: Um Imperativo à Concretização do Princípio da Dignidade Humana. Civilistica. Acesso em 02 de fevereiro de 2021, disponível em https://civilistica.emnuvens.com.br/redc/article/view/151/119

BBC. (2018). Os óculos de reconhecimento facial da polícia chinesa que identificam suspeitos em tempo real. Acesso em 05 de março de 2021, disponível https://www.bbc.com/portuguese/geral-43011505

BECK, U. (2010). Sociedade de Risco - Rumo a uma outra Modernidade. (S. Nascimento, Trad.) São Paulo: Editora 34.

BOBBIO, N. (2004). A Era dos Direitos (7ª reimpressão ed.). (C. N. Coutinho, Trad.) Rio de Janeiro: Elsevier.

BRASIL. (1988). Constituição da República Federativa do Brasil. Acesso em 21 de maio de 2020, disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BRASIL. (2012). Lei n.º 12.737 de 30 de novembro 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Acesso em 20 de maio de 2020, disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

BRASIL. (2014). Lei n.º 12.965 de 23 de abril de 2014. Marco Civil da Internet. Acesso em 21 de maio de 2020, disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BRASIL. (2018). Lei n.º 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Acesso em 1 de outubro de 2020, disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

BRASIL.(2020). Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal. Acesso em 08 de março de 2021, disponível em https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf

CABRAL, J. A. (2011). Do direito à segurança à segurança do Direito. *Fourth International Conference on "The Legal Reforms of Macau in Global Context" - Social Rights and Environmental Protection.* Macau. Acesso em 19 de outubro de 2020, disponível em https://www.stj.pt/wp-content/uploads/2018/01/macaufaculdadedireito.pdf

CALVÃO, F. U. (2015). O Modelo de Supervisão de Tratamento de Dados Pessoais na União Europeia: Da atual Diretiva ao futuro Regulamento. Forum de Proteção de Dados Pessoais, CNPD. Acesso em 20 de junho de 2021, disponível em https://www.cnpd.pt/media/owgnsrp2/forum_1_af_web_low.pdf

CALVÃO, F. U. (2018). Direito da Proteção de Dados Pessoais: Relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina. Porto. Universidade Católica Editora.

CANOTILHO, J. J. (1993). Direito Constitucional (6ª ed.). Coimbra: Almedina.

CARVALHO, W. A. (2020). Vigilância das forças de segurança através de câmeras de reconhecimento facial e o conflito com o direito à privacidade – Brasil e Portugal. Dissertação de Mestrado, Universidade Nova de Lisboa. Acesso em 01 de outubro de 2020, disponível em https://run.unl.pt/handle/10362/97545

CEARÁ. (2019). Lei n.º 16.873 de 10 de maio de 2019. Dispõe sobre o comércio e consumo de bebida alcoólica em estádios e arenas desportivas no Estado do Ceará e define penalidades pelo descumprimento às normas de comercialização. Acesso em 05 de março de 2021, disponível em https://belt.al.ce.gov.br/index.php/legislacao-do-ceara/organizacao-tematica/cultura-e-esportes/item/6638-lei-n-16-873-de-10-05-19-d-o-10-05-19

CENTRO DE ESTUDOS DE SEGURANÇA E CIDADANIA - UCAMCESEC. (2019). Retratos da Violência. Rede de Observatórios da Segurança. Acesso em 01 de março de 2021. Disponível em https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf

CHAU, R. A. (2017). Direito à Liberdade e à Segurança no Estado de Direito Democrático: Os limites da Atuação Policial - Uma perspectiva jurídico-constitucional da Polícia.

Dissertação de Mestrado. Instituto Superior de Ciências Policiais e Segurança Interna. Acesso em 09 de outubro de 2020, disponível em https://comum.rcaap.pt/handle/10400.26/19925

CNIL. (2019). *RECONNAISSANCE FACIALE - POUR UN DEBAT À LA HAUTEUR DES ENJEUX*. Acesso em 02 de março de 2021, disponível em https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

COMISSÃO EUROPEIA. (2020). Livro Branco sobre a Inteligência Artificial - Uma abordagem europeia virada para a excelência e a confiança. Acesso em 23 de janeiro de 2021, disponível em https://op.europa.eu/pt/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

COMISSÃO EUROPEIA. (2021). Uma Europa Preparada para a Era Digital: Comissão propõe novas regras e ações para promover a excelência e a confiança na inteligência artificial. Acesso em 21 de junho de 2021, disponível em https://ec.europa.eu/commission/presscorner/detail/PT/ip_21_1682

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. Convenção Americana sobre Direitos Humanos. (1969). Acesso em 03 de fevereiro de 2021, disponível em https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS. Parecer n.º 2020/80 de 17 de Julho de 2020. Sobre o Pedido de Alargamento dos Sistemas de Videovigilância da Cidade da Amadora. Acesso em 17 de junho de 2021, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2020&type=4&ent=

CONSELHO DA EUROPA. (1981). Convenção 108 - Convenção para a proteção de indivíduos com relação ao processamento automático de dados pessoais. Acesso em 26 de maio de 2020, disponível em https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/convencao_protecao_pessoas_tratamento_automatizado_dados_caracter_pessoal.pdf

CONSELHO DA EUROPA. (1950). Convenção Europeia dos Direitos do Homem. Acesso em 03 de fevereiro de 2021, disponível em https://gddc.ministeriopublico.pt/sites/default/files/convention_por.pdf

CONSELHO DA EUROPA. (1950). Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais. Acesso em 03 de fevereiro de 2021, disponível em https://gddc.ministeriopublico.pt/instrumento/convencao-para-proteccao-dos-direitos-do-homem-e-das-liberdades-fundamentais

CONSILIUM EUROPA. (2009). Estratégia Europeia em matéria de Segurança: Uma Europa segura num mundo melhor. Acesso em 29 de março de 2020, disponível em https://www.consilium.europa.eu/media/30824/qc7809568ptc.pdf

CORREIA, V. (2016). Sobre a Privacidade. Sinapis.

DONEDA, D. (2006). Da Privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar.

DUARTE, F. P. (2015). Sociedade de Risco. In: J. B. Gouveia, & S. Santos, Enciclopédia de Direito e Segurança. Lisboa: Almedina.

FACEBOOOK. (s.d.). O que é a configuração de reconhecimento facial no Facebook e como ela funciona? Acesso em 10 de outubro de 2020, disponível em https://www.facebook.com/help/122175507864081

FERNANDES, A. H. (2015). O Conceito de Segurança: Um obstáculo a paz. Relações Internacionais, n.º 48. Acesso em 20 de novembro de 2020, disponível em http://www.ipri.pt/images/publicacoes/revista_ri/pdf/ri48/n48a09.pdf

FERNANDES, C. S., & Raad, E. (2020). Reconhecimento Facial: laissez-faire, regular ou banir?. Migalhas. Acesso em 20 de fevereiro de 2021, disponível em https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/330766/reconhecimento-facial--laissez-faire--regular-ou-banir

FERREIRA, M. F. (2014). A Governação da Segurança: Responsabilidade de Intervir e Proteger. Observare - Janus 2014 - Metamorfoses da violência. Acesso em 29 de novembro de 2020, disponível em https://www.janusonline.pt/images/anuario2014/3.9_MarcosFerreira_GovernacaoSeguranca.pdf

FOLHA DE SÃO PAULO. (2019). Rio e Salvador terão sistema de reconhecimento facial no carnaval. Acesso em 11 de outubro de 2020, disponível em https://www1.folha.uol.com.br/cotidiano/2019/02/rio-e-salvador-terao-sistema-de-reconhecimento-facial-no-carnaval.shtml

FRANCISCO, Pedro Augusto et al. (2020). Regulação do Reconhecimento Facial no Setor Público: Avaliação de Experiências Internacionais. Instituto Igarapé. Acesso em 10 de outubro de 2020, disponível em https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf

G1, GLOBO. (2019). Sistema de reconhecimento facial da PM do RJ falha, e mulher são detida por engano. Acesso em 11 de outubro de 2021, disponível em https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml

G1, GLOBO. (2018). Escolas de Nova Venécia usam reconhecimento facial para controlar frequência e desperdício de merenda. (s.d.). Acesso em 11 de outubro de 2020, disponível em https://g1.globo.com/es/espirito-santo/noticia/escolas-de-nova-venecia-usam-reconhecimento-facial-para-controlar-frequencia-e-desperdicio-de-merenda.ghtml

GHISI, S. (2014). Legítimas Expectativas de Privacidade na Sociedade da Informação. Dissertação de Mestrado. Universidade do Oeste de Santa Catarina. Acesso em 20 de dezembro de 2020, disponível em https://www.academia.edu/36379063/LEG%C3%8DTIMAS_EXPECTATIVAS_DE_PRIVACIDADE_NA_SOCIEDADE_DA_INFORMA%C3%87%C3%83º

GOMES, Daniel Machado; GAZOLLA, CARDOSO, Frederico Jacinto; CICILIO, Tiago da Silva; SOUZA, Felipe César Santiago de. (2020). Controle e Vigilância na Sociedade da Informação: Novas Formas de Panoptismo. CAED - Jus - Conselho Internacional de Altos Estudos em Direito. Acesso em 19 de fevereiro de 2021, disponível em: https://www.caedjus.com/wp-content/uploads/2020/08/Livro_Direito_privado_contempor%C3%A2neo_2-edicao.pdf

GOUVEIA, J. B. (2018). Direito a Segurança, Cidadania, Soberania e Cosmopolitismo (1ª ed.). Lisboa: Almedina.

LAPIN. (2021). Nota Técnica Lei 6.712/20 - 10 Recomendações para o uso de reconhecimento facial para segurança pública no DF. Acesso em 05 de março de 2021, disponível em: https://lapin.org.br/wp-content/uploads/2021/02/NT_LD_67122020_reconhecimento_facial_DF_LAPIN-1.pdf

LEI GERAL DE PROTEÇÃO DE DADOS - LGPD. (s.d.). Guia LGPD Comentada. Acesso em 03 de março de 2021, disponível em: https://guialgpd.com.br/lgpd-comentada/

LEIAJÁ. (2019). Hering responde por uso indevido de reconhecimento facial. Acesso em 10 de outubro de 2020, disponível em https://www.leiaja.com/tecnologia/2019/09/03/hering-responde-por-uso-indevido-de-reconhecimento-facial/

LYNCH, J. (2018). *Face Off: Law Enforcement Use of Face Recognition Technology*. Acesso em 11 de abril de 2020, disponível em https://www.eff.org/wp/law-enforcement-use-face-recognition

MASTERCARD. (s.d.). *Mastercard Identity Check: Facial Recognition Biometrics*. Acesso em 10 de outubro de 2020, disponível em https://newsroom.mastercard.com/videos/mastercard-identity-check-facial-recognition-biometrics/

MENDES, G. F., COELHO, I. M., & BRANCO, P. G. (2000). Hermenêutica Constitucional e Direitos Fundamentais. Brasília: Brasília Jurídica LTDA.

MINAS GERAIS. (2015). Lei n.º 21.737 de 05 de agosto de 2015. Dispõe sobre a comercialização e o consumo de bebida alcoólica nos estádios de futebol localizados no Estado e dá outras providências. Acesso em 05 de março de 2021, disponível: https://www.almg.gov.br/consulte/legislacao/completa/completa.html?tipo=LEI&num=21737&comp=&ano=2015

MIRANDA, J. (1992). Funções do Estado. Revista de Direito Administrativo, 85-99.

NUNES, P. (2019). Novas Ferramentas, Velhas Práticas: Reconhecimento Facial e Policiamento no Brasil. Rede de Observatórios da Segurança - Retratos da Violência - Cinco meses de monitoramento, análises e descobertas. Acesso em 05 de março de 2021, disponível em https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf

OCDE. (2013). Diretrizes de privacidade da OCDE. Acesso em 09 de fevereiro de 2021, disponível em https://www.oecd.org/digital/ieconomy/privacy-guidelines.htm

OLHAR DIGITAL. (2020). Senacon multa Hering em R$ 58 mil por uso indevido de reconhecimento facial. Acesso em 10 de outubro de 2020, disponível em https://olhardigital.com.br/2020/08/27/noticias/senacon-multa-hering-em-r-58-mil-por-uso-indevido-de-reconhecimento-facial/

OLHAR DIGITAL. (2019). Professores brasileiros realizam chamada por reconhecimento facial. Acesso em 11 de outubro de 2020, disponível em https://olhardigital.com.br/2019/10/24/noticias/professores-brasileiros-realizam-chamada-por-reconhecimento-facial/

OLIVEIRA, S. R., & COSTA, R. S. (2019). O Uso de tecnologias de reconhecimento facial em sistemas de vigilância e suas implicações no direito à privacidade. Revista de Direito, Governança e Novas Tecnologias. Acesso em 02 de março de 2021, disponível em https://indexlaw.org/index.php/revistadgnt/article/view/5777

ONU. (1948). Declaração Universal dos Direitos do Homem. Acesso em 02 de fevereiro de 2021, disponível em https://dre.pt/declaracao-universal-dos-direitos-humanos

ONU. (1948). Declaração Universal dos Direitos Humanos. Acesso em 03 de fevereiro de 2021, disponível em https://unric.org/pt/declaracao-universal-dos-direitos-humanos/

ONU. (1966). Pacto Internacional sobre os Direitos Civis e Políticos. Acesso em 03 de fevereiro de 2021, disponível em https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/pacto_internacional_sobre_os_direitos_civis_e_politicos.pdf

ONU. (1990). Convenção sobre os Direitos da Criança. Acesso em 03 de fevereiro de 2021, disponível em Disponível em: https://www.unicef.pt/media/2766/unicef_convenc-a-o_dos_direitos_da_crianca.pdf

ONU. (2003). Convenção Internacional sobre a Proteção dos Direitos de Todos os Trabalhadores Migrantes e dos membros das suas famílias. Acesso em 03 de fevereiro de 2021, disponível em https://gddc.ministeriopublico.pt/sites/default/files/convencaomigrantes.pdf

PARLAMENTO EUROPEU E DO CONSELHO. (2008). Regulamento (CE) N.º 767/2008 de 09 de julho. Relativo ao Sistema de Informação sobre Vistos (VIS) e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração («Regulamento VIS»). Acesso em 18 de outubro de 2020, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32008R0767&from=PT

PARLAMENTO EUROPEU E DO CONSELHO. (2013). Regulamento (UE) n.º 603/2013 de 26 de junho de 2013. Relativo à criação do sistema «Eurodac» de comparação de impressões digitais para efeitos da aplicação efetiva do Regulamento (UE) n.º 604/2013. Acesso em 18 de outubro de 2020, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32013R0603

PARLAMENTO EUROPEU E DO CONSELHO. (2016). Diretiva (UE) 2016/680 de 27 de abril de 2016. Relativa à 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, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Acesso em 12 de março de 2021, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680

PARLAMENTO EUROPEU E DO CONSELHO. (2016). Diretiva (UE) 2016/680 de 27 de abril de 2016. Relativa à 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, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Acesso em 13 de março de 2021, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&rid=1

PARLAMENTO EUROPEU E DO CONSELHO. (2016). Regulamento (UE) 2016/679 de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Acesso em 09 de fevereiro de 2021, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EM

PARLAMENTO EUROPEU E DO CONSELHO. (2017). Regulamento (UE) 2017/2226 de 30 de novembro de 2017. Estabelece o Sistema de Entrada/Saída (SES) para registo dos dados das entradas e saídas e dos dados das recusas de entrada dos nacionais de países terceiros aquando da passagem das fronteiras externas dos Estados-Membros. Acesso em 18 de outubro de 2020, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32017R2226&from=PT

PARLAMENTO EUROPEU E DO CONSELHO. (2018). Regulamento (UE) 2018/1860 de 28 de novembro de 2018. Relativo à utilização do Sistema de Informação de Schengen para efeitos de regresso dos nacionais de países terceiros em situação irregular. Acesso em 18 de outubro de 2020, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32018R1860&from=PT

PARLAMENTO EUROPEU E DO CONSELHO. (2018). Regulamento (UE) 2018/1861 de 28 de novembro de 2021. Relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos de fronteira, e que altera a Convenção de Aplicação do Acordo de Schengen. Acesso em 20 de outubro de 2020, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32018R1861&from=PT

PARLAMENTO EUROPEU E DO CONSELHO. (2019). Regulamento (UE) 2019/816 de 17 de abril de 2019. Cria um sistema centralizado para a determinação dos Estados-Membros que possuem informações sobre condenações de nacionais de países terceiros e de apátridas (ECRIS-TCN) . Acesso em 18 de outubro de 2020, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32019R0816

PARLAMENTO EUROPEU E DO CONSELHO. (2019). Regulamento (UE) 2019/817 de 20 de maio de 2019. Relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE. Acesso em 19 de outubro de 2020, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0817&from=DE

PARLAMENTO EUROPEU E DO CONSELHO. (2019). Regulamento (UE) 2019/818 de 20 de maio de 2019. Relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE . Acesso em 23 de março de 2021, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0818&from=EM

PARLAMENTO EUROPEU E DO CONSELHO. (2021). Proposta de Regulamento de 21 de abril de 2021. Estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União. Acesso em 21 de junho de 2021, disponível https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206

PARLAMENTO EUROPEU E DO CONSELHO. (2016). Carta dos Direitos Fundamentais da União Europeia. Acesso em 10 de outubro de 2020, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR

PARLAMENTO EUROPEU. (s.d.). Carta dos Direitos Fundamentais da União Europeia. Acesso em 03 de fevereiro de 2021, disponível em https://op.europa.eu/webpub/com/carta-dos-direitos-fundamentais/pt/

PARLAMENTO EUROPEU. (s.d.). Fichas temáticas sobre a União Europeia - Proteção dos dados pessoais. Acesso em 01 de março de 2021, disponível em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf

PB HOJE. (2019). Onze pessoas foram presas através da tecnologia de reconhecimento facial no São João de Campina Grande. (s.d.). Acesso em 11 de outubro de 2020, disponível em https://www.pbhoje.com.br/noticias/65563/onze-pessoas-foram-presas-atraves-da-tecnologia-de-reconhecimento-facial-no-sao-joao-de-campina-grande.html

PINHEIRO, A. S. (2015). *Privacy* e Protecção de Dados Pessoais: A Construção Dogmática do Direito a Identidade Informacional. Lisboa: AAFDL.

PINHEIRO, A. S., COELHO, C. P., DUARTE, T., GONÇALVES, C. J., & GONÇALVES, C. P. (2018). Comentário ao Regulamento Geral de Proteção de Dados. Almedina.

PORTUGAL. (1976). Constituição da República Portuguesa. Acesso em 20 de novembro de 2020, disponível em https://dre.pt/legislacao-consolidada/-/lc/34520775/view

PORTUGAL. (2005). Lei n.º 1/2005 de 10 de janeiro de 2005. Regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum. Acesso em 09 de março de 2021, disponível em https://dre.pt/pesquisa/-/search/457049/details/maximized

PORTUGAL. (2005). Lei n.º 1/2005 de 10 de janeiro de 2005. Regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum. Acesso em 11 de março de 2021, disponível em https://dre.pt/pesquisa/-/search/457049/details/maximized

PORTUGAL. (2012). Lei n.º 9/2012 de 23 de fevereiro de 2012. Procede à terceira alteração à Lei n.º 1/2005, de 10 de janeiro, que regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum. Acesso em 20 de junho de 2021, disponível em https://dre.pt/pesquisa/-/search/542867/details/maximized

PORTUGAL. (2013). Lei n.º 34/2013 de 16 de maio de 2013. Estabelece o regime do exercício da atividade de segurança privada e procede à primeira alteração à Lei n.º 49/2008, de 27 de agosto (Lei de Organização da Investigação Criminal). Acesso em 06 de março de 2021, disponível em https://data.dre.pt/eli/lei/34/2013/05/16/p/dre/pt/html

PORTUGAL. (2019). Lei n.º 46/2019 de 08 de julho de 2019. Altera o regime do exercício da atividade de segurança privada e da autoproteção. Acesso em 12 de março de 2021, disponível em https://dre.pt/home/-/dre/122996202/details/maximized

PORTUGAL. (2019). Lei n.º 46/2019 de 08 de julho de 2019. Altera o regime do exercício da atividade de segurança privada e da autoproteção. Acesso em 11 de março de 2021, disponível em https://data.dre.pt/eli/lei/46/2019/07/08/p/dre

PORTUGAL. (2019). Lei n.º 59/2019 de 08 de agosto de 2019. Aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680.

Acesso em 12 de março de 2021, disponível em https://dre.pt/home/-/dre/123815983/details/maximized

PORTUGAL. (2019). Lei n.º 58/2019 de 08 de agosto de 2019. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Acesso em 12 de março de 2021, disponível em https://dre.pt/pesquisa/-/search/123815982/details/maximized

PROJECT, T. (2020). *Towards the European Level Exchange of Facial - Legal Analysis for TELEFI project*. Acesso em 09 de março de 2021, disponível em https://www.telefi-project.eu/sites/default/files/TELEFI_LegalAnalysis.pdf

PROJECT, T. (2021). *Summary Report*. Acesso em 09 de março de 2021, disponível em https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf

REIS, C. (2021). Nota Técnica sobre a Lei 6.712/20 - 10 Recomendações para o uso do Reconhecimento Facial para Segurança no DF. Laboratório de Políticas Públicas e Internet - LAPIN. Acesso em 05 de março de 2021, disponível em: https://lapin.org.br/wp-content/uploads/2021/02/NT_LD_67122020_reconhecimento_facial_DF_LAPIN-1.pdf

RIO DE JANEIRO. (2015). Lei n.º 7.123 de 08 de dezembro 2015. Acesso em 05 de março de 2021, disponível em: http://www3.alerj.rj.gov.br/lotus_notes/default.asp?id=53&url=L2NvbnRsZWkubnNmL2IyNGEyZGE1YTA3Nzg0N2MwMzI1NjRmNDAwNWQ0YmYyL2VhODExNDg5YmY3MmY4YjI4MzI1N2YxODAwNTg0M2E4P09wZW5Eb2N1bWVudA==#

RIO DE JANEIRO. (2021). Lei n.º 9.167 de 06 de janeiro de 2021. Acesso em 05 de março de 2021, disponível em: http://alerjln1.alerj.rj.gov.br/contlei.nsf/f25edae7e64db53b032564fe005262ef/017e439b81aa5b700325865700640e38?OpenDocument

ROBOREDO, N. P. (2010). A evolução do conceito de segurança e as implicações nas operações militares do séc. XXI. Trabalho de Investigação Individual do CPOS-Marinha. Acesso em 29 de março de 2020, disponível em https://comum.rcaap.pt/bitstream/10400.26/1121/1/BE_Roboredo%202010.pdf

RODRIGUES, G. (2019). Reconhecimento Facial na Segurança Pública: Controvérsias, riscos e regulamentação. Instituto de Referência em Internet e Sociedade. Acesso em 11 de abril de 2020, disponível em http://irisbh.com.br/reconhecimento-facial-na-seguranca-publica-controversias-riscos-e-regulamentacao/

SALDANHA, N. (2018). Novo Regulamento Geral de Proteção de Dados. O que é? a quem se aplica? como implementar? Lisboa: FCA - Editora de Informática.

SANTOS, Á. M. (2016). Segurança e Globalização: A Perspectiva dos Estudos Críticos de Segurança. Proelium X, P.107-114. Acesso em 03 de janeiro de 2021, disponível em https://revistas.rcaap.pt/proelium/article/view/8916

SILVA, Caroline Targino B. R. (s.d.). A evolução Teórica do Conceito de Segurança e a Percepção das Novas Ameaças pela Região Andina e o Cone Sul. Acesso em 03 de novembro

de 2020, disponível em https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xii/a_evolucao_teorica.pdf

SILVA, J. A. (2005). Curso de Direito Constitucional Positivo (25ª ed.). Malheiros.

SILVA, M. G. (2019). Segurança Humana, Responsabilidade de Proteger e Direito Internacional: O Caso de Intervenção na Líbia. Dissertação de Mestrado - Universidade do Minho. Acesso em 10 de novembro de 2020, disponível em http://repositorium.sdum.uminho.pt/handle/1822/58858

SIMÃO, B., FRAGOSO, N., & ROBERTO, E. (2020). Reconhecimento Facial e Setor Privado. Guia de Adoção de Boas Práticas - Reconhecimento Facial e o Setor Privado. Idec e InternetLab. Acesso em 24 de fevereiro de 2021, disponível em https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf

TECNOBLOG. (2019). Rio de Janeiro identificou 8 mil pessoas com reconhecimento facial no Carnaval. Acesso em 11 de outubro de 2020, disponível em https://tecnoblog.net/289696/rio-de-janeiro-identificou-8-mil-reconhecimento-facial

TEFFÉ, Chiara Spadaccini de, E. R. (2020). Tratamento de Dados Sensíveis por Tecnologias de Reconhecimento Facial: Proteção e Limites. O Direito Civil na era da Inteligência Artificial (pp. 283-315). São Paulo. Acesso em 20 de fevereiro de 2021, disponível em https://www.academia.edu/44127917/Tratamento_de_dados_sens%C3%ADveis_por_tecnologias_de_reconhecimento_facial_prote%C3%A7%C3%A3o_e_limites

THE GUARDIAN. (2015). Google pede desculpas por racista auto-tag em aplicativo de fotos. Acesso em 02 de março de 2021, disponível em https://www.theguardian.com/technology/2015/jul/01/google-sorry-racist-auto-tag-photo-app

THE GUARDIAN. (s.d.). China traz reconhecimento facial obrigatório para usuários de telefones celulares. Acesso em 02 de março de 2021, disponível https://www.theguardian.com/world/2019/dec/02/china-brings-in-mandatory-facial-recognition-for-mobile-phone-users

TIMES, T. N. (2016). O problema do cara branco da inteligência artificial. Acesso em 02 de março de 2021, disponível em https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html

TODODIA. (2020). Japão considera usar reconhecimento facial para rastreamento em grandes eventos. Acesso em 10 de outubro de 2020, disponível em https://tododia.jp/japao-considera-usar-reconhecimento-facial-para-rastreamento-em-grandes-eventos/

UNIÃO EUROPEIA. (s.d.). Regulamentos, diretivas e outros atos legislativos, Acesso em 08 de março de 2021, disponível em https://europa.eu/european-union/law/legal-acts_pt

UNIÃO EUROPEIA. (2016.). Tratado sobre o Funcionamento da União Europeia. Acesso em 26 de maio de 2020, disponível em https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF

UOL. (2019). A sociedade mais vigiada do mundo: como a China usa o reconhecimento facial. Acesso em 02 de março de 2021, disponível em

https://www.uol.com.br/tilt/noticias/redacao/2019/01/19/a-sociedade-mais-vigiada-do-mundo-como-a-china-usa-o-reconhecimento-facial.htm

VALENTE, M. M. (2012). Teoria geral do Direito Policial. Coimbra: Almedina.

WARREN, S. D., & BRANDEIS, L. D. (1980). *The Right to Privacy - Harvard Law Review*, vol. 4, no. 5, 1890, pp. 193–220. Acesso em 8 de fevereiro de 2021, disponível em www.jstor.org/stable/1321160.