UNIVERSIDADE D
COIMBRA

Ticiana Teresa Biasutti de Farias

Os desafios da responsabilidade civil no âmbito do reconhecimento facial e da inteligência artificial

Uma abordagem dinâmica à luz do ordenamento jurídico português e do europeu

Dissertação de Mestrado à Faculdade de Direito da Universidade de Coimbra no âmbito do 2. º Ciclo de Estudos em Direito, na área de Mestrado Científico em Ciências Ciências-Jurídico Civilísticas/ Menção em Direito Civil da Universidade de Coimbra, orientada pela Senhora Professora Doutora Ana Mafalda Castanheira Neves Miranda Barbosa e apresentada a Faculdade de Direito da Universidade de Coimbra.

Outubro de 2021

1 2 9 0

FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA

OS DESAFIOS DA RESPONSABILIDADE CIVIL NO ÂMBITO DO RECONHECIMENTO FACIAL E DA INTELIGÊNCIA ARTIFICIAL

Uma abordagem dinâmica à luz do ordenamento jurídico português e do europeu

Ticiana Teresa Biasutti de Farias

Dissertação de Mestrado à Faculdade de Direito da Universidade de Coimbra no âmbito do 2. º Ciclo de Estudos em Direito, na área de Mestrado Científico em Ciências Ciências-Jurídico Civilísticas/ Menção em Direito Civil da Universidade de Coimbra, orientada pela Senhora Professora Doutora Ana Mafalda Castanheira Neves Miranda Barbosa e apresentada a Faculdade de Direito da Universidade de Coimbra.

Coimbra

Outubro de 2021

1 2  9 0

FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA

Dedico este trabalho aos meus pais que nunca mediram esforços para garantir a concretização desta aspiração académica.

AGRADECIMENTOS

Primeiramente, abro os agradecimentos manifestando a minha gratidão a Deus e a Virgem Maria, a qual sou devota, por proverem sustento espiritual para ultrapassar todos os obstáculos encontrados ao longo da realização deste trabalho.

Agradeço aos meus pais, Selma e Rômulo, aos meus familiares e aos meus amigos que me incentivaram nos momentos difíceis desta jornada académica e que compreenderam a minha ausência enquanto me dedicava à realização este sonho.

Agradeço a Senhora Professora Doutora Ana Mafalda Castanheira Neves Miranda Barbosa, por ter sido minha orientadora pela ajuda, compreensão e paciência com a qual guiaram esta dissertação de Mestrado

Estendo também meus agradecimentos aos demais professores que tive o prazer de ter aulas e conviver durante o Mestrado Científico em Ciências Ciências-Jurídico Civilísticas/Menção em Direito Civil da Universidade de Coimbra.

Agradeço aos meus colegas de Mestrado pelo companheirismo ao logo do percurso.

E, por fim, agradeço a todos que participaram direta ou indiretamente da trajetória de maturação deste trabalho e que enriqueceram o processo de aprendizado.

“Atualmente, sete das dez marcas globais de maior valor são empresas de dados. Dados como o novo óleo? Claramente. Quando você investe em dados, seu armazenamento, sua gestão e sua análise, você está investindo em inovação.” Thomas Harrer, CTO da IBM Systems Hardware Sales Europa

RESUMO

A presente dissertação de mestrado tem por escopo apresentar uma abordagem dinâmica dos possíveis desafios do Direito de responsabilidade civil no âmbito do reconhecimento facial sob a ótica das normas contidas no ordenamento jurídico português e nos regulamentos que tratam deste tema na União Europeia.

Para isso, dedica-se a primeira parte a discorrer sobre a tecnologia de reconhecimento facial focando no seu funcionamento, no surgimento, na sua aplicabilidade e como é utilizado. Nos capítulos dois e três analisa-se minuciosamente o Regulamento Geral de Proteção de Dados do Parlamento Europeu e do Conselho Europeu - Regulação (EU) 2016/79 - e a proposta de regulamento que estabelece regras harmonizadas sobe inteligência artificial na comunidade europeia.

Logo após o último capítulo é destinado a confrontar os desdobramentos da responsabilidade civil frente a situações envolvendo a tecnologia de reconhecimento facial ao realizar exame em tópicos apartados de cada norma e trazendo ao final possíveis remédios. Para então trazer as conclusões deste trabalho.

Palavras-chaves: reconhecimento facial; inteligência artificial; responsabilidade civil; Regulamento Geral de Proteção de Dados; regras harmonizadas sobe inteligência artificial na comunidade europeia.

ABSTRACT

The scope of this master's thesis is to present a dynamic approach to the possible challenges of civil liability law in the context of facial recognition from the perspective of the norms contained in the Portuguese legal system and in the regulations that deal with this subject in the European Union.

For this, the first part is dedicated to discussing facial recognition technology, focusing on its functioning, its appearance, its applicability and how it is used. In chapters two and three we analyze in detail the General Data Protection Regulation of the European Parliament and the European Council - Regulation (EU) 2016/79 - and the proposal for a regulation that establishes harmonized rules on artificial intelligence in the European community.

Afterwards, the last chapter is intended to confront the consequences of civil liability in situations involving facial recognition technology by examining topics separated from each standard and bringing possible remedies at the end. To then bring the conclusions of this work.

Keywords: *facial recognition; artificial intelligence; civil liability; general data protection regulation; harmonized rules on artificial intelligence in the European community.*

LISTA DE SIGLAS E ABREVIATURAS

ACLU - *American Civil Liberties Union*

CC – Código Civil

CF – Constituição Federal

CRP - Constituição da República Portuguesa

DRAPA - *Defense Advanced Research Projects Agency*

DEA - *Drug Enforcement Administration*

DPO - *Data Protection Officer*

EUA – Estados Unidos da América

EU – União Europeia

FAC – Folha de Antecedentes Criminais

FBI - *Federal Bureau of Investigation*

HDSG - Hessishes Datenschutzgesetz

IA – Inteligência Artificial

IoT - *Internet of Things*

LGPD - Lei Geral de Proteção de Dados

NFL - *National Football League*

ONG – Organização não governamental

QR Code - Quick Response Code

RGPD - Regulamento Gral de Proteção de Dados

TFEU - Tratado Sobre o Funcionamento da União Europeia

TJUE - Tribunal de Justiça da União Europeia

SUMÁRIO

INTRODUÇÃO

Nas últimas décadas o progresso tecnológico impulsionado pela 4ª Revolução Industrial ou Revolução 4.0 remodelou a maneira pela qual vivemos em sociedade. Num mundo cada vez mais tecnológico é quase impossível vislumbrar interações humanas sem que haja presença de algum tipo de dispositivo desta natureza. Telefones, celulares, *Notebook*, computadores, *Tablet,* aplicativos, robôs, caixas eletrônicos, aparelhos hospitalares, cripto moedas, carros autônomos, programas computacionais, entre outros, são parte integrantes das relações humanas da sociedade do Século 21 que foram profundamente modificadas pela híper conectividade.

Nesse novo *modus vi vendi* as trocas diárias estão eivadas de interação com os aparatos tecnológicos que possuem inteligência artificial (IA) que circundam as pessoas afetando de igual modo o Direito, vez que esse representa o conjunto de normas que intermedeiam a conduta humana designando-lhes direitos e deveres. Com isso, cabe a ceara jurídica mediar possíveis conflitos em que tais apetrechos estejam presentes.

Notadamente, hoje nos deparamos com dispositivos, dotados de inteligência artificial, capazes de capturar da imagem de alguém e, em questão de segundos, acender a uma vasta gama de informações que englobam desde mapear os padrões de compras alimentícias de uma pessoa até rastrear quais lugares frequenta ou determinar quais redes sócias ela faz parte, etc.

O reconhecimento facial, algo que outrora era considerado futurístico, hoje é de uso corriqueiro, principalmente, em sistemas de monitoramento eletrônico de vias públicas tanto por autoridades governamentais, como intuito de identificar um indivíduo, quanto por agentes privados contratados para fim similar.

À vista disso, o primeiro capítulo desta dissertação é dedicado a discorrer sobre a parte técnica que cerca à tecnologia de reconhecimento facial, vez que é indubitável elucidar pontos como cruciais para a compreensão do contexto histórico do surgimento desta, bem como o seu funcionamento e aplicação. Desta forma, procura-se responder as seguintes

perguntas: o que é: quando e como surgiu; como funciona; e revelar em quais circunstâncias do cotidiano estão presentes aparatos que se utilizam direta e indiretamente do reconhecimento facial.

Logo após, propõem-se investigar a forma pela qual dar-se-á o tratamento dos dados, o que engloba os biométricos, na comunidade europeia, ou seja, procura-se aqui elucidar a maneira pela qual a legislação pertinente ao trabalho acadêmico desenvolvido aborda este tema sensível que engloba processamento, armazenamento e distribuição de dados dos usuários. Por conseguinte, será matéria de apreciação o Regulamento Geral de Proteção de Dados (RGPD), perpassando pela sua entrada no ordenamento jurídico português e, por último, averiguar o jeito pelo qual são arrazoados os dados ditos sensíveis no RGPD. Não obstante, com o intuito de melhor abordar o tema antes de adentrar especificamente no regulamento é importante trazer a visão histórica da proteção de dados na Europa criando desta mineira base para melhor alicerçar o tópico proposto.

Em seguida, vai de encalço ao assunto tratado nesta dissertação esmiuçar a proposta de Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial, isso pois como fica claro na leitura de seu título ela tem por intento realizar uniformização das normas correlatas na União Europeia o que diretamente atinge o Regulamento Geral de Proteção de Dados.

Por fim, o último capítulo é destinado a explorar a responsabilidade civil e as normas as quais são objetos centrais deste trabalho, assim, aprecia-se os desdobramentos da interação do Regulamento Geral de Proteção de Dados (RGDP) e da propositura de Regulamentação de Inteligência Artificial com este ramo do Direito Civil destacando ao final os possíveis remédios aos impasses apontados.

Desta feita, após todas as afirmações realizadas apresentar-se-á a conclusão para dando assim desfecho a esta dissertação de mestrado.

CAPÍTULO I - A TECNOLOGIA DE RECONHECIMENTO FACIAL

1 NO QUE CONSISTE A TECNOLOGIA DE RECONHECIMENTO FACIAL OU *FACIAL RECOGNITION*

Dedica-se o início desta dissertação a explorar parte técnica que cerca à tecnologia de reconhecimento facial, alvo deste estudo, vez que é imprescindível esclarecer os seguintes pontos: o que é; quando e como surgiu; como funciona; e, consequentemente, contextualizar em quais momentos do cotidiano os dispositivos que se utilizam dela estão presentes direta e indiretamente. Tendo estes tópicos esclarecidos prossegue-se o desenrolar dos aspetos jurídicos relacionados ao tema.

1.1 O RECONHECIMENTO FACIAL: O QUE É; COMO FUNCIONA; QUANDO E COMO SURGIU

1.1.1 O que é reconhecimento facial e como funciona?

A tecnologia de reconhecimento facial, também denominada de *Facial Recognition*, consiste em um *software*[1] que por meio de algoritmos[2] mapeia padrões do rosto humano e

[1] "São os programas que nos permitem realizar atividades específicas num computador. Por exemplo, os sistemas operacionais, aplicativos, navegadora web, jogos entre outros.

Esses dois elementos sempre trabalham de mãos dadas. Enquanto o software faz as operações, o hardware é a parte física com a qual essas funções podem ser realizadas." INFORMÁTICA BÁSICA: O QUE SÃO HARDWARE E SOFTWARE? [*S. l.*], [*s. d.*]. Disponível em: https://edu.gcfglobal.org/pt/informatica-basica/o-que-sao-hardware-e-software-/1/. Acesso em: 14 maio 2021.

[2] "Antes de tudo, vamos compreender o conceito de algoritmo. O termo pode ser entendido como **uma sequência de raciocínios, instruções ou operações para alcançar um objetivo**, sendo necessário que os passos sejam finitos e operados sistematicamente.

Parece complexo? Calma, vamos simplificar. Alguns exemplos de algoritmos que podemos citar são: receitas culinárias, manual de instrução de aparelhos, funções matemáticas e até mesmo páginas da Web, como esta que você está lendo.

os comprara a uma base de dados pré-existente de imagens digitais com a finalidade de confirmar ou negar a identidade de certo indivíduo. Trate-se, portanto, de uma modalidade de identificação biométrica que faz uma leitura da face levando em conta os denominados pontos nodais[3] do semblante humano criando uma geometria espacial única que culmina no estabelecimento de características faciais singulares a cada ser humano, dessa maneira, distinguindo uma pessoa da outra tal qual técnica de reconhecimento via impressão digital. A exemplo pode-se citar: a largura do nariz, a profundidade as órbitas, o formato da maçã do rosto etc.

Não obstante, é de extrema importância estabelecer que os sistemas *software* de reconhecimento facial são programas de análise de imagens dotados de inteligência artificial[4], dado que ao ler os pontos nodais fornecidos começa imediatamente e de forma autônoma o processamento de dados, assim, dar-se-á o início de uma varredura nos bancos de imagens – públicos e privados – conectados, com o escopo de encontrar imagens

---

Pense na receita culinária, por exemplo. Ela tem os ingredientes necessários (dados de entrada), passo a passo para realizar a receita (processamento ou instruções lógicas) e atinge um resultado (o prato finalizado).

Um algoritmo, portanto, conta com a entrada (input) e saída (output) de informações mediadas pelas instruções.

É fundamental compreender que o algoritmo se justifica no resultado que ele almeja alcançar, logo, deve ter um objetivo específico. Uma sequência de instruções simples pode se tornar mais complexa conforme a necessidade de considerar outras situações." ALGORITMO: O QUE É, COMO FUNCIONA E QUAIS SÃO OS PRINCIPAIS EXEMPLOS. *In*: ROCK CONTENT - BR. 7 fev. 2019. Disponível em: https://rockcontent.com/br/blog/algoritmo/. Acesso em: 14 maio 2021.

[3] "To begin with, there was no standard method for digitizing photos and no existing database of digital images to draw from. Today's researchers can train their algorithms on millions of freely available selfies, but Panoramic would have to build its database from scratch, photo by photo." PISA, P. **Como funciona o reconhecimento facial**. [*S. l.*], 2012. Site. Disponível em: http://www.techtudo.com.br/artigos/noticia/2012/04/como-funciona-o-reconhecimento-facial.html. Acesso em: 15 maio 2021.

[4] "Definição de Inteligência Artificial (CE)

Relativa a software: assistentes virtuais, software de análise de imagem, motores de busca, sistemas de reconhecimento facial e de voz

Incorporada em hardware: robôs, carros autónomos, Dornes, ou aplicações no âmbito da Internet das Coisas." O QUE É A INTELIGÊNCIA ARTIFICIAL E COMO FUNCIONA? | ATUALIDADE | PARLAMENTO EUROPEU. [*S. l.*], 2020. Disponível em: https://www.europarl.europa.eu/news/pt/headlines/society/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona. Acesso em: 22 maio 2021.

compatíveis com as informações previamente inseridas que sejam compatíveis com os traços perfil procurado.

Diante, deste cenário pode-se traçar seguinte paralelo os softwares de biometria facial trazem modernidade, larga usabilidade e sofisticação ao conhecido "retrato fadado" e ao folheto de "procurado" emblemático nos contos e filmes do velho Oeste, mas claro com um quê a mais, haja vista que ao obter imagens na *World Wilde Web* ou de fonte privativa que se encaixam do padrão de dados fornecidos não se obtém unicamente rosto, mas também uma série de informações dos mais variados graus de abrangência sobre aquele determinado indivíduo que variam desde hábitos de compra até mesmo pessoas com as quais se relaciona com será devidamente investigado nos tópicos desenvolvidos a seguir.

1.1.2 Quando e como surgiu a tecnologia de reconhecimento facial?

Esta futurística tecnologia, que até outrora estava restrita ao imaginário fértil dos amantes de filmes, livros e desenhos animados de ficção científica que povoam a cultura jovem teve sua ideia concebida em meados da década de sessenta, mais precisamente no ano de 1963, por Woodrow Wilson Bledsoe[5] matemático e cientista da computação americano considerado pai desta invenção.

[5] "Mas, no início de 1963, foi o destinatário de um tipo de argumento diferente de um Woody Bledsoe: Ele propôs realizar "um estudo para determinar a viabilidade de uma máquina simplificada de reconhecimento facial." Com base no trabalho dele e de Browning como método n-tupla, ele pretendia ensinar um computador a reconhecer 10 faces. Isso é, ele queria dar ao computador um banco de dados de 10 fotos de pessoas diferentes e verse ele conseguisse reconhecer novas fotos de cada um deles. "Logo se esperaria estender o número de pessoas a milhares", escreveu Woody. Em um mês, King Hurley deu-lhe sinal verde." Tradução livre de "But in early 1963, it was the recipient of a different sort of pitch from one Woody Bledsoe: He proposed to conduct "a study to determine the feasibility of a simplified facial recognition machine." Building on his and Browning's work with the n-tuple method, he intended to teach a computer to recognize 10 faces. That is, he wanted to give the computer a database of 10 photos of different people and see if he could get it to recognize new photos of each of them. "Soon one would hope to extend the number of persons to thousands," Woody wrote. Within a month, King Hurley had given him the go-ahead." RAVIV, S. The Secret History of Facial Recognition. **Wired**, [*s. l.*], v. 28, n. 2, p. 56–65, 2020. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&AuthType=cookie,ip,shib,uid&db=edb&AN=141229925&lang=pt-pt&site=eds-live&authtype=sso. Acesso em: 14 maio 2021. P.6.

A época não havia uma base de dados consolidada de fotografias digitais que fosse de fácil acesso como dispomos atualmente - a exemplo do Google Imagens, do Pinterest, do Facebook ou do Instagram– afinal a *internet*[6] com hoje conhecemos não existia ainda, era somente uma ideia, um novo e fértil campo de estudo impulsionado pela corrida tecnológica proporcionada pelo investimento derivados da Guerra Fria, que acabara de ter seu conceito criado por J. C. R Licklider[7], chefe do DRAPA *(Defense Advanced Research Projects Agency*).[8]

Portanto, Bledsoe a fim de tronar viável a ideia elaborada para esse ambicioso projeto, por meio da sua empresa Panoramic Research Incorporated[9], teve de criar,

---

[6] Nota explicativa: embora o conceito clássico de *internet* ainda exista, no qual persiste a ideia de que internet é concebida tão somente pela rede mundial de computadores, se faz oportuno aclarar que atualmente estamos inseridos num mundo altamente tecnológico e deveras conectado devido ao facto de que uma série de objetos (celulares, relógios, etc.) sensíveis a *internet* interagir em entre si autonomamente e trocam informações. Este fenômeno é chamado pelos estudiosos da área como *Internet of Things (IoT*) e faz "parte desse conceito os dispositivos de nosso cotidiano que são equipados com "sensores capazes de captar aspetos do mundo real, como por exemplo temperatura, umidade e presença, e enviá-los a centrais que recebem estas informações e as utilizam de forma inteligente".86 A sigla refere-se a um mundo onde objetos e pessoas, assim como dados e ambientes virtuais, interagem uns com os outros no espaço e no tempo.87" MAGRANI, E. **A internet das coisas**. 1ªed. Rio de Janeiro, RJ, Brasil: FGV Editora, 2018. P.44.

[7] "Já em 1962, J. C. R Licklider, chefe da DARPA e pioneiro da Internet, descreveu o conceito de uma rede galáctica para acessar rapidamente dados de qualquer lugar do mundo.

De forma independente, Paul Baran trabalhou na comutação de pacotes na RAND Corporation. Em 1962, ele apresentou um **sistema de comunicações que, por meio de computadores conectados a uma rede descentralizada, era imune a ataques externos**, já que, se um ou mais eles fossem destruídos, os outros poderiam continuar funcionando." HISTÓRIA DA INTERNET: ORIGEM, QUEM INVENTOU E TUDO SOBRE O ASSUNTO!. *In*: ROCK CONTENT - BR. 27 jan. 2020. Disponível em: https://rockcontent.com/br/blog/historia-da-internet/. Acesso em: 15 maio 2021.

[8] SOBRE DARPA. [*S. l.*], [*s. d.*]. Disponível em: https://www.darpa.mil/about-us/about-darpa. Acesso em: 22 maio 2021.

[9] "Em 1960, Woody riscou com Browning e um terceiro colega Sandia para fundar uma empresa própria. A Panoramic Research Incorporated foi sediada, a princípio, em um pequeno escritório em Palo Alto, Califórnia, no que ainda não era conhecido como Vale do Silício. [...] O negócio da Panoramic, como Woody mais tarde descreveu a um colega, era "experimentar ideias que esperávamos 'mover o mundo'. [...], mas ao longo de sua existência, a Panoramic teve pelo menos um patrono aparentemente confiável que ajudou mantê-lo à tona: a Agência Central de Inteligência. Se alguma menção direta da CIA existiu nos papéis de Woody, provavelmente acabou em cinzas em sua garagem; mas fragmentos de evidências que sobreviveram nos arquivos de Woody sugerem fortemente que, por anos, a Panoramic fez negócios com empresas de fachada da CIA. […] De acordo com os registros obtidos pelo Black Vault, um site especializado em solicitações esotéricas da Lei de Liberdade de Informação, a Panoramic estava entre as 80 organizações que trabalharam no Projeto MK-Ultra, o infame programa de "controle da mente" da CIA, mais conhecido pelas torturas psicológicas que infligia a sujeitos humanos frequentemente relutantes. [...] Woody e seus colegas também receberam dinheiro

primeiramente, um banco de dados por meio do mapeamento digital de um número considerável de fotos com o intuito de capturar os padrões nodais acima mencionados.[10]

Durante o processo de desenvolvimento desse programa deparou-se com diversos obstáculos a serem vencido como: a tridimensionalidade da face humana, a dificuldade de registrar com precisão de diferentes ângulos do rosto, o facto de que nas fotografias a luz faz

---

da Society for the Investigation of Human Ecology, uma frente da CIA que fornecia subsídios para cientistas cujo trabalho pudesse melhorar as técnicas de interrogatório da agência ou atuar como camuflagem para esse trabalho. (A CIA não confirmava nem negava qualquer conhecimento ou conexão com Woody ou Panoramic.) [...], mas no início de 1963, foi o destinatário de um tipo diferente de argumento de Woody Bledsoe: ele propôs reger "Um estudo para determinar a viabilidade de uma máquina simplificada de reconhecimento facial." Com base no trabalho dele e de Browning com o método de n-tupla, ele pretendia ensinar um computador a reconhecer 10 faces. Ou seja, ele queria dar ao computador um banco de dados de 10 fotos de pessoas diferentes e ver se conseguia reconhecer novas fotos de cada uma delas." Tradução livre de "In 1960, Woody struck out with Browning and a third Sandia colleague to found a company of their own. Panoramic Research Incorporated was based, at first, in a small office in Palo Alto, California, in what was not yet known as Silicon Valley. […] Panoramic's business, as Woody later described it to a colleague, was "trying out ideas which we hoped would 'move the world.' [...] But throughout its existence, Panoramic had at least one seemingly reliable patron that helped keep it afloat: the Central Intelligence Agency. If any direct mentions of the CIA ever existed in Woody's papers, they likely ended up in ashes in his driveway; but fragments of evidence that survived in Woody's archives strongly suggest that, for years, Panoramic did business with CIA front companies. […] According to records obtained by the Black Vault, a website that specializes in esoteric Freedom of Information Act requests, Panoramic was among 80 organizations that worked on Project MK-Ultra, the CIA's infamous "mind control" pro- gram, best known for the psychological tortures it inflicted on frequently unwilling human subjects. […] Woody and his colleagues also received money from the Society for the Investigation of Human Ecology, a CIA front that provided grants to scientists whose work might improve the agency's interrogation techniques or act as camouflage for that work. (The CIA would neither confirm nor deny any knowledge of, or connection to, Woody or Panoramic.) [...] But in early 1963, it was the recipient of a different sort of pitch from one Woody Bledsoe: He proposed to conduct "a study to determine the feasibility of a simplified facial recognition machine." Building on his and Browning's work with the *n*-tuple method, he intended to teach a computer to recognize 10 faces. That is, he wanted to give the computer a database of 10 photos of different people and see if he could get it to recognize new photos of each of them.RAVIV, 2020.p. 4-6

[10] "Para começar, não havia um método padrão para digitalizar fotos e nenhum banco de dados de imagens digitais para extrair. Os pesquisadores de hoje podem treinar seus algoritmos em milhões de selfies disponíveis gratuitamente, mas a Panoramic teria de construir seu banco de dados do zero, foto por foto.

" Tradução livre de "Para começar, não existia um método padronizado de digitalização de fotos e nem uma base de dados de imagens digitais para extrair. Os pesquisadores de hoje podem treinar seus algoritmos em milhões de selfies disponíveis gratuitamente, mas a Panoramic teria de construir seu banco de dados do zero, foto por foto." Tradução livre de "To begin with, there was no standard method for digitizing photos and no existing database of digital images to draw from. Today's researchers can train their algorithms on millions of freely available selfies, but Panoramic would have to build its database from scratch, photo by photo." Tradução livre de "To begin with, there was no standard method for digitizing photos and no existing database of digital images to draw from. Today's researchers can train their algorithms on millions of freely available selfies, but Panoramic would have to build its database from scratch, photo by photo." Ibid. p. 6

diferença na captura da imagem, o envelhecimento, as micro expressões faciais que variam a cada reação humana, até mesmo a mudança de estilo de cabelo ou deixar crescer a barba empecilhos, entre outras coisas, pois aquela época não havia certeza de que o equipamento disponível fosse capaz de processar tantos dados, vez que "uma de suas máquinas principais era um CDC 1604 com 192 KB de RAM - cerca de 21.000 vezes menos memória de trabalho do que um *smartphone* moderno básico."[11]

A despeito de parte dos problemas iniciais ainda persistiram, tendo em vista as diversas origens étnicas do ser humano, Bledsoe obteve sucesso ao criar um sistema híbrido no qual primeiro as características da face eram obtidas manualmente via dispositivo gráfico intitulado The RAND Tablet[12] para depois as informações obtidas por esse dispositivo serem inseridas no sistema computacional e processadas para assim o reconhecimento facial ser

11 Tradução livre de "One of their main machines was a CDC 1604 with 192 KB of RAM—about 21,000 times less working memory than a basic modern smartphone." Ibid. p.7

12 "Antes do Apple Newton e do Palm Pilot, havia o RAND Tablet.

Desenvolvido na década de 1960, o tablet de 10 polegadas quadradas usava um programa de reconhecimento de escrita que a RAND chamou de GRAIL (para linguagem de entrada gráfica). Segurando uma caneta, os usuários podiam desenhar formas e texto no tablet, que GRAIL suavizava e renderizava corretamente em um monitor maior em tempo real.

GRAIL foi programado para identificar 53 números, letras, símbolos e formas geométricas desenhados à mão. Ainda mais inovador foi o uso de gestos para manipular o que está na tela: os usuários podem deletar coisas rabiscando ou escrevendo sobre elas, por exemplo, ou podem agarrar uma forma e movê-la ou alterar seu tamanho.

Alan Kay, cujo trabalho para o Xerox PARC resultou em muitas inovações da Apple, às vezes mostra um filme do GRAIL em ação durante as aparições, apontando recursos usados posteriormente em produtos da Apple. "Que sistema notável era aquele", disse Kay em uma apresentação. "Eu senti como se estivesse enfiando minhas mãos direto na tela.

Inicialmente, os economistas e programadores da RAND usaram a tecnologia para criar fluxogramas e escrever códigos. Os economistas, em particular, precisavam do tablet porque "nenhum de nós consegue digitar", disseram eles aos desenvolvedores do GRAIL. Mas a tecnologia encontrou fãs além da RAND: os militares a usaram para fazer anotações em mapas e uma versão posterior poderia traduzir o mandarim.

Então, por que não há um r-Pad na sua mesa de centro? Por um lado, os tablets custam US $ 18.000 cada - ou quase US $ 140.000 hoje. O que faz com que o iPad Pro pareça uma pechincha."MONICA, 1776 Main Street Santa; CALIFÓRNIA 90401-3208. **The RAND Tablet: iPad Predecessor**. [*S. l.*], 2018. Disponível em: https://www.rand.org/blog/rand-review/2018/09/the-rand-tablet-ipad-predecessor.html. Acesso em: 22 maio 2021.

realizado.[13] Tal feito, foi um marco muito importante na vida de Bledsoe, entretanto, por razões governamentais o artigo científico que ele escreveu nunca foi publicado.[14]

A tecnologia de reconhecimento facial somente superou a necessidade da intervenção humano, com assim almejava Bledsoe, quando em 1973 Takeo Kanade, um cientista da computação japonês, desenvolveu um programa que podia extrair autonomamente as características faciais de base num banco de dados de 850 fotografias digitalizadas, tiradas principalmente durante a Feira Mundial de 1970 em Suita, Japão.

1.2 PARA QUE SERVE O RECONHECIMENTO FACIAL E QUEM UTILIZA-SE DELE NO COTIDIANO E QUEM É AFETA

Como todo grande avanço tecnológico de seu tempo a biometria facial nasce do impulso criado pelo ambiente competitivo da Guerra Fria, com isso as primeiras aplicações deste dispositivo foram associadas a ceara militar. Contudo, em poucos anos tal invento tomaria conta do dia a dia e alcançaria patamares que tornaria possível trazer cenários de ficção científica a realidade.

Sai do campo do imaginário e passa a fazer parte do cotidiano e, atualmente, o reconhecimento facial faz parte dos mais diversos dispositivos. A exemplo, cita-se: a utilização do mesmo no âmbito da segurança pública ao integrar sistemas de monitoramento de circulação de pessoas em fronteiras, principalmente, na alfandega de aeroportos; a presença em sistemas de segurança que tem por fim prevenir fraude e roubo de identidade; em sistemas de videovigilância nos transportes públicos; e, mais recentemente, no domínio da proteção de saúde pública, um vez que o cenário pandêmico propiciou um nicho de mercado nunca antes explorado, pelo menos não para esse fim especifico, que tem como

[13] VERBETE DRAFT: O QUE É RECONHECIMENTO FACIAL. *In*: PROJETO DRAFT. 30 maio 2018. Disponível em: https://www.projetodraft.com/verbete-draft-o-que-e-reconhecimento-facial/. Acesso em: 14 maio 2021.

[14] RAVIV, 2020. P.8.

objetivo identificar possíveis infetados por Covid-19, monitorar sua circulação e detetar quem ele contatou fazendo o que denominara de rastreio e isolamento de pessoas contaminadas[15]

Nesse seguimento destaca-se o caso de sucesso da *startup* o Clearview AI[16] que criou um sistema de reconhecimento facial com base em fotografias de sites e redes sociais que pela sua eficiência e longo alcance foi prontamente utilizada pelo governo americano com a finalidade de identificar suspeitos em metros ou durante protestos fornecendo uma variedade de dados, desde nome e endereço do indivíduo alvo a quem tal pessoa possuía conexões e o que faziam.[17]

Indo neste encalço, no Brasil o uso de sistemas dotados de *facial recognition* pelo agentes públicos ocorre desde 2011, entretanto, somente em 2019, durante o período das festividades de Carnaval, é que teve sua escala de aplicabilidade estendida no referido campo de ação no momento em que diversas entidades públicas firmaram parcerias com empresas privadas especializadas em fornecer este serviço, o que proporcionou o emprego deste tipo de monitoramento nas vias públicas de mais de 40 cidades espalhadas pelo país.[18]

No entanto, no âmbito privado, a gama de aplicabilidade deste *gadget* é ainda maior, haja vista que não se limita exclusivamente ao setor de segurança. A princípio, o reconhecimento facial serve como substituto de chaves, códigos numéricos ou leitura biométrica de outra natureza – como o reconhecimento de íris, o que permite o desbloqueio

---

[15] DALSENTER, T. **Reconhecimento Facial: laissez-faire, regular ou banir? - Migalhas**. [*S. l.*], 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/330766/reconhecimento-facial--laissez-faire--regular-ou-banir. Acesso em: 15 maio 2021.

16 HILL, K. The Secretive Company That Might End Privacy as We Know It. The New York Times, [s. l.], 18 jan. 2020. Technology. Disponível em: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. Acesso em: 16 maio 2021.

17 DALSENTER, 2020.

18 Ibid.

de aparelhos celular, faz parte de jogos eletrônicos no Playsstation e no Xbox, de entre outros.[19]

Todavia, a infinidade que foi mencionada ainda se estende para o uso desta tecnologia para fins comerciais. Nesse domínio, destaca-se alguns casos como: o da empresa brasileira Hering[20], especializada no varejo de vestuário, que em uma de suas unidades fez uso deste aparato para supervisionar a reação dos clientes aos produtos expostos, assim, coletando informações cruciais de aceitação ou rejeição da mercadoria ofertada; e de uma unidade do Carrefour, rede francesa de supermercados, em que na sua loja conceito o cliente poderia optar por utilizar o reconhecimento facial para pagamento ou um *QR Code (Quick Response Code).*[21][22]

Apesar da biometria facial ser mais utilizada no meio privado com forma de dinamizar compras e vendas de um produto ou serviço este mecanismo também é largamente consumido com o fim de prover seguridade dentro dos estabelecimentos privados ao reconhecer indivíduos com antecedentes criminais, por exemplo, que ingressam em

---

19 MENA. Verbete Draft: o que é Reconhecimento Facial. In: PROJETO DRAFT. 30 maio 2018. Disponível em: https://www.projetodraft.com/verbete-draft-o-que-e-reconhecimento-facial/. Acesso em: 13 maio 2021.

20 HERING | ROUPAS FEMININAS E MASCULINAS E INFANTIS. [S. l.], [s. d.]. Disponível em: https://www.hering.com.br/. Acesso em: 22 maio 2021.

21 "Código de resposta rápida. Esse é o nome completo do QR Code (Quick Response Code). Embora esteja sendo mais notado — e adotado — apenas agora, ele já tem 25 anos: foi criado em 1994 pela Denso-Wave (uma empresa do Grupo Toyota), no Japão.

O QR Code é uma evolução do código de barras — que existe desde 1970 e revolucionou a identificação de produtos. Ele consiste em um gráfico 2D (o código de barras comum usa apenas uma dimensão, a horizontal, enquanto o QR usa a vertical e a horizontal) que pode ser lido pelas comeras da maioria dos celulares (alguns modelos ainda requerem aplicativos específicos para isso). Código de resposta rápida. Esse é o nome completo do QR Code (Quick Response Code). Embora esteja sendo mais notado — e adotado — apenas agora, ele já tem 25 anos: foi criado em 1994 pela Denso-Wave (uma empresa do Grupo Toyota), no Japão.

O QR Code é uma evolução do código de barras — que existe desde 1970 e revolucionou a identificação de produtos. Ele consiste em um gráfico 2D (o código de barras comum usa apenas uma dimensão, a horizontal, enquanto o QR usa a vertical e a horizontal) que pode ser lido pelas comeras da maioria dos celulares (alguns modelos ainda requerem aplicativos específicos para isso)." ANDRION, R. Você sabe o que é o QR Code? *In*: OLHAR DIGITAL. 14 set. 2019. Disponível em: https://olhardigital.com.br/2019/09/14/seguranca/voce-sabe-o-que-e-o-qr-code-a-gente-explica/. Acesso em: 22 maio 2021.

22 DALSENTER, 2020.

determinada loja, além de controlar o acesso de pessoas a instituições, áreas residências e zonas empresárias.[23]

Outro caso extremamente interessante de ser reportado e que prova o quanto estamos expostos a este meio demasiadamente conectado, ocorreu quando a concessionária administradora do metrô na cidade de São Paulo, cidade mais populosa do Brasil que figura como uma das com maior índice demográfico no mundo, mais precisamente na linha 4, recolheu via câmaras de vídeo instaladas nas telas das plataformas informações relativas as reações dos passageiros quando estes interagiam com as publicidades exibidas.[24]

Ademais, é valido recordar que as redes sociais *Facebook* e *Instagram* a tempos utilizam-se do reconhecimento facial ao possibilitar que usuários que são amigos na plataforma sejam marcados em fotos que compartilham entre si. Chegando o *Facebook* a informar aos usuários que em consequência dessa nova ferramenta disponibilizou um novo serviço de segurança, que deve ser previamente ativado pelo usuário na aba privacidade, que possibilita informar quando uma foto contendo o seu rosto foi colado da rede ou que ela foi usada no perfil de outro utente.[25]

Não obstante, destaca-se também o projeto inovador da empresa *Cainthus* que por meio do reconhecimento facial identifica padrões de comportamento e de alimentação do gado e caso haja algo fora do normal, segundo a base de dados fornecida para aquela espécie, reconhece o problema que está a passar com animais, indica as possíveis soluções e imediatamente o sistema de inteligência artificial informa ao fazendeiro que faz os ajustes necessário, deste modo, otimizando tempo e dinheiro.[26]

Com isso, é crível afirmar que estamos imersos numa sociedade altamente arraigada ao aspeto tecnológico, em que a cada dia que passa tornamo-nos mais dependentes destes tipos de aparatos high-tech que em si facilitam a rotina, uma vez que ao recorrer a biometria

---

[23] Ibid.
[24] Ibid.
[25] MENA, 2018.
[26] FINALLY, FACIAL RECOGNITION FOR COWS IS HERE. [*S. l.*], [*s. d.*]. Disponível em: https://gizmodo.com/finally-facial-recognition-for-cows-is-here-1822609005. Acesso em: 22 maio 2021.

facial dispensa-se o uso de senha para ter acesso o telefone celular, o *Tablet*, o *Notebook* ou certo aplicativo, pela leitura da face realiza-se pagamentos, acende-se a estabelecimentos, otimiza-se a experiência de varejo, invade a vida no campo, entre outros. Entretanto, não há só benesses advindas deste tipo inovação.

Com já exposto, o desenvolvimento da tecnologia de biometria facial está entrelaçado com a história da Guerra Fria sendo seu investidor inicial o EUA (Estados Unidos da América), por conseguinte, está arraigado a seu desígnio a função de vigilância. E, quanto a isso, já angariou no decurso do tempo algumas situações dignas de serem reportadas, haja vista que levanta dúvidas quanto aos limites de sua aplicabilidade. Neste contesto, cita-se o fato de o governo chinês recorrer ao reconhecimento facial para identificar e perseguir membros dos Uighur, minoria ética no país, que já tiveram milhares integrantes levados a "campos de reeducação".[27]

Há também de reportar o ocorrido nos EUA, como noticiou o jornal *The Washington Post*, quando o FBI (*Federal Bureau of Investigation*) conjuntamente com *Immigration and Customs Enforcement* valeram-se da tecnologia em questão para criar uma rede digital capaz de procurar por suspeitos entre os milhões de rostos providos pelos bancos de dados das carteiras de habilitação de cada estado federativo sem que, por inúmeras vezes, houvesse uma ordem judicial específica para execução daquela busca.[28]

Em 2019, foi revelado pelo *Financial Times* que pesquisadores da Universidade de Stanford e da Microsoft colherem e compartilharam um grande conjunto de dados de imagens faciais sem o conhecimento ou consentimento dos envolvidos causando revolta, o que tentou-se corrigir com a retirada desses dados de circulação, no entanto, permaneceu no ar por tempo suficiente para serem exportados por desenvolvedores de *startups* de tecnologia e uma das academias militares chinesa.[29]

[27] RAVIV, 2020. p.3.
[28] Ibid. p.3.
[29] Ibid. p.3.

É oportuno informar que sistemas que se valem do reconhecimento facial revelam falhas e padrões tendenciosos. Isso ficou evidenciado quando o *Rekognition* da empresa Amazon identificou erroneamente 28 (vinte e oito) jogadores da NFL *(National Football League)* como criminosos, o que levantou alerta fazendo com que a ACLU *(American Civil Liberties Union)*, organização não governamental (ONG) norte-americana que tem por fim defender e preservar direitos e liberdades individuais assegurados pela Constituição e leis dos EUA, processasse o Departamento de Justiça dos Estados Unidos, o FBI e o DEA (*Drug Enforcement Administration*) com intuito obter conhecimento de como eles usam a tecnologia de reconhecimento facial fornecida e produzida por empresas como Microsoft e Amazon.[30]

Deste modo, diante de todo o factoide exposto é verossímil indagar que a grande quantidade de dados sensíveis gerados por todo e qualquer dispositivo que tem acoplado tecnologia de reconhecimento facial está passível de gerar consequências das mais diversas ordens como violação: ao direito de privacidade, ao direito de liberdade, ao direito de igualdade, ao direito a personalidade, ao direito ao anonimato, entre outros. Mas antes de explorar possíveis infrações é oportuno analisar a forma pela qual as normas dos ordenamentos jurídicos em foco nesta dissertação tratam a proteção de dados.

[30] Ibid. p.9.

CAPÍTULO II - A PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA SOB A ÓTICA DO REGEGULAMENTO GERAL DE PROTEÇÃO DE DADOS

Nesta parte, propõem-se buscar a forma pela qual dar-se-á o tratamento dos dados o que inclui os biométricos faciais nas normas reguladoras da comunidade europeia, ou seja, procura-se aqui elucidar a maneira pela qual as legislações pertinentes ao trabalho acadêmico desenvolvido abordam este tema sensível que engloba processamento, armazenamento e distribuição de dados dos usuários.

Por conseguinte, será matéria de análise o Regulamento Geral de Proteção de Dados (RGPD) a qual procurará perpassar pelos seguintes pontos: estabelecer comparação entre o que foi a proposta de regulamentação e o regulamento em vigor; escrevinhar notas gerais sobre o RGPD; explorar o papel das autoridades de controlo no RGPD; abalizar concisamente a forma pela qual o RGPD foi introduzido no ordenamento jurídico português; e, ao final, contemplar o modo pelo qual os dados sensíveis são abordados pela norma em diagnóstico. Todavia, com o fito de melhor explorar o tema antes de adentrar especificamente no regulamento inaugura-se este capítulo com uma visão histórica da proteção de dados na União Europeia criando assim pavimento para melhor embasar o tópico a ser explorado.

2 O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD)

2.1 BREVE EVOLUÇÃO HITÓRICA DA PROTEÇÃO DE DADOS NA EUROPA

Em solo europeu inaugurou-se a proteção de dados com o *Hessishes Datenschutzgesetz (HDSG)*[31], diploma legal aprovado em solo alemão no ano de 1970 pelo Parlamento do Estado de Hesse. E, diferentemente das atuais legislações que buscam ser

[31]Tradução nossa “Lei hessiana de proteção de dados”.

extremamente minuciosas quanto ao tema, o HDSG mantinha em seus incisos campo de aplicação restrita a entidades públicas que recolhiam e tratavam os dados, porem não mencionava qualquer tipo de limitação aos processos de tratamento de dados, somente reconhecia o direito de correção dados ou restauração de dados ilegalmente alterados e criava o Supervisor de Dados Pessoais, autoridade que tinha por função supervisionar o cumprimento da norma.[32]

Seguiu esta tendência o Estado da Renânia-Platinada em 1974 editando e promulgando norma similar. Subsequentemente, em 1977, o legislador federal alemão sanciona o *Bundesdatenschutzgesetz* – ou Lei Federal de Proteção de Dados – que entra em vigência em 1978 e assume o papel de norma geral trazendo um importante avanço ao estender sua aplicação a todos que tratam dados, ou seja, tanto entes públicos quanto privados podem são responsáveis pelo tratamento de dados que chegam aos seus sistemas.[33]

Caminho este adotado também pelo legislador do sueco ao aprovar o *Datalag*, norma de utilização nacional e transversal, como a norma alemã, que tinha por fim medir soluções de caráter jurídico, de registo e de cunho regulatório.[34]

Com bem aponta Lee A. Bygrave está prática de contemplar um diploma nuclear abrangido por legislações setoriais perdurou por décadas na Europa, contudo atualmente minoritária contraria ao modelo estado-unidense, que é hostil a qualquer tipo de enquadramento geral.[35]

Já na década seguinte, 1980, ocorre o que Menezes de Cordeiro designa como período de concretização da proteção de dados na União Europeia, isto pois passam a valer

---

[32] CORDEIRO, A. B. M. **Direito da proteção de dados: à luz do RGPD e da Lei no. 58/2019**. Coimbra: Almedina, 2020. p. 64-65.

[33] Ibid. p.65.

[34] BING, J. Transnacional Data Flows and the Scandinavian Data Protection Legislation. **Stockholm Institute for Scandinavian Law**, [*s. l.*], n. 24, Scandinavian Studies in Law, p. 65–96, 1980. p.69

[35] HIJMANS, H. Lee A. Bygrave, Data Privacy Law, an International Perspective, Oxford University Press, Oxford, 2014, 272 pages, 234 x 156 mm, 75, ISBN 978-0-19-967555-5. **International Data Privacy Law**, [*s. l.*], v. 5, n. 1, p. 88–90, 2015. Disponível em: https://doi.org/10.1093/idpl/ipu031. Acesso em: 18 out. 2021.

para os Estados Membros as *Guidelines Governing the Protection of Privacy and Transborder Flows os Personal Data*[36] de 23 de setembro de 1980 da OCDE conjuntamente com a *Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal*, mais concedida com Convenção 108. Tais normas chancelam o início do que hoje concebemos como Direito europeu de proteção de dados e por meio da Convenção 108 o Conselho Europeu robustece uma gama de princípios gerais e termos base que traçam a base para esse novo ramo do Direito.[37]

Logo após fica evidente a necessidade de harmonização no âmbito jurídico de cada Estado Membro, sendo assim a Comissão Europeia assume a dianteira deste processo e propõem que seja ratificado por cada um de seus membros a Convenção 108 e ainda afirma que caso isso não ocorra em tempo hábil afirma que iria propor ao Conselho Europeu que propugnasse instrumento legislativo próprio. E, ao final, após extensas negociações, foi esta solução que se sucedeu com a aprovação da Diretriz n.°95/46/CE, de 24 de outubro de 1995, a qual seria revogada com a aprovação e a entrada em vigência do Regulamento Geral de Proteção de Dados (RGPD).[38]

2.2 DA PROPOSTA DE REGULAMENTO AO EFETIVO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD)

Antes de adentar propriamente no exame do regulamento em si faz-se necessário esquadrinhar o percurso que levou até ele. À vista disso, recorda-se que foi no *The Stockholm Programme: an open scure Europe serving and protecting citizen*[3940] que o Conselho

[36] Tradução nossa "Diretrizes que regem a Proteção da Privacidade e Fluxos Transfronteiriços os Dados Pessoais".

[37] CORDEIRO, 2020. p. 66-67-

[38] Ibid. p.67-68.

[39] Tradução nossa "O Programa de Estocolmo: uma Europa aberta ao serviço e proteção dos cidadãos".

[40] THE STOCKHOLM PROGRAMME — AN OPEN AND SECURE EUROPE SERVING AND PROTECTING CITIZENS.: NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES. Official Journal of the European Union: Concelho Europeu, 2010.

Europeu enfatizou o quão é primordial prover proteção da privacidade dos cidadãos europeus e de melhor regulamentar o tratamento de transferência de dados pessoais. Contudo, este não foi o único momento em que a Diretriz n.°95/46/CE foi colada em xeque, uma vez que o veloz progresso das novas tecnologias, a aprovação da Carta Europeia dos Direitos dos Fundamentais, o Tratado de Lisboa entre outros, somente evidenciaram a inegável demanda pela revisão urgente e inevitável desta Diretriz haja vista a sua desatualização.

Dada premente desfasagem da norma é apresentado pela Comissão, em 25 de janeiro de 2012, Proposta de Regulamento Geral de Proteção de Dados que a princípio não teve críticas diretas em seus documentos oficiais o que indicaou um excelente e descomplicado caminho para a sua aprovação, contudo Johannes Masing, a época juiz no Tribunal Constitucional alemão, apontou que a substituição da Diretriz n.°95/46/CE por um regulamento, nos moldes com estava, afetaria a competência dos tribunais nacionais de cada Estado Membro em benefício do Tribunal de Justiça da União Europeia (TJUE) o que prejudicaria o direito à autodeterminação informacional.[41]

Após quatro anos e inúmeros pareceres de várias entidades a proposta original e a versão final do RGPD trazem diferenças consubstancias, visto que as competências atribuídas a própria Comissão foram totalmente suprimidas e que na RGPD consolidou-se cláusulas de abertura, ou seja, medidas legislativas facultativas de índole substantiva, assim fica a cargo de cada Estado Membro escolher se vão adotar ou não. Tal facto expõem a real dificuldade em criar-se unificação entre os países que compõem a União Europeia e que, portanto, para obter-se aprovação necessária durante o processo negocial todos em algum ponto tiveram de ceder em parte.[42]

[41] CORDEIRO, 2020. p. 82.
[42] Ibid. p. 83-84.

2.3 NOTAS GERAIS SOBRE O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD)

O Regulamento Geral de Proteção de Dados (RGPD)[43] entrou em vigor em 25 de maio de 2018, em substituição a antiga Diretiva de Proteção de Dados da União Europeia de 1995, com a finalidade de estabelecer diretrizes básicas para o processamento de dados na União Europeia, assim, buscando: harmonia entre as leis acerca de privacidade de dados que vigoram nos países pertencentes ao bloco europeu; robustecer a proteção do direito dos indivíduos sobre seus próprios dados; e exigir das empresas do setor maior comprometimento ao tratar os dados que colhem sob a pena de sofrer graves sanções.[44]

Numa primeira leitura, fica evidente a preocupação do legislador europeu com o consentimento[45] daquele que os dados pertencem ao sedimentar a ideia de que este deve ser

---

[43] UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados).

[44] IRAMINA, A. RGPD V. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. Revista de Direito, Estado e Telecomunicações, [*s. l.*], v. 12, n. 2, Brasil, p. 91–117, 2020. Disponível em: https://doi.org/10.26512/lstr.v12i2.34692. Acesso em: 25 maio 2021. p.94.

[45] Artigo 7. °

Condições aplicáveis ao consentimento

1. Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.

2. Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento.

3. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.

4. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato. UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu de 27 de abril

conferido por meio de uma ação afirmativa clara, assim, conferindo licitude ao tratamento de dados que não pode desvirtuar o propósito ao que foi apanhado como é definido no artigo 6. °, ponto 4.[46] Recorda-se que na hipótese de os dados serem referentes a menores de 16 anos – caso não tenha legislação do Estado-Membro determinando idade mínima inferior sem ultrapassar os 13 anos - a anuência fica restrita aos titulares das responsabilidades parentais, artigo 8. °.[47]

---

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 (Regulamento Geral sobre a Proteção de Dados

[46] Artigo 6°

Licitude do tratamento

[…]

4. Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.º, n.º 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta:

a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;

b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;

c)A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.o, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.o;

d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;

e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização. (grifo nosso) UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados).

[47]Artigo 8. °

Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação

1. Quando for aplicável o artigo 6.o, n.º 1, alínea a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança.

Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos.

2. Nesses casos, o responsável pelo tratamento envida todos os esforços adequados para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível.

É oportuno salientar que se cria uma categoria de dados especiais, artigo 9. °[48], ao expressamente vedar a utilização indiscriminada de informações referentes religião, posicionamento político, raça, origem étnica, filiação sindical, saúde, orientação sexual, bem como dados biométricos e genéticos, salvo as exceções expressas no mesmo diploma. Deste modo, busca-se evitar discriminação por parte de quem tem colhe e processa a referentes dados, bem como, preserva-se a privacidade daqueles que os fornecem, haja vista que como preceitua Rochfeld[49] ao salvaguardar tais dados não só se protege um bem ou valor econômico, mas também tutela a privacidade do indivíduo ao conferir transparência no processamento de suas informações digitais.

Nessa conjuntura de proteção aos direitos individuais o RGPD preserva aqueles já colecionados na antiga Diretiva da UE de 1995 e, vai além, uma vez que prevê novos direitos como o direito da portabilidade e recuperação dos dados o que restaura ao sujeito o controle sob as informações que lhe pertencem originalmente.

Não obstante, é importante destacar que uma das principais inovações da diretiva europeia é justamente a inserção do princípio da *accountability*[50], presente no artigo 24. ° do RGPD[51], o qual estabelece que as organizações devem adotar políticas e procedimentos para

3. O disposto no n.º 1 não afeta o direito contratual geral dos Estados-Membros, como as disposições que regulam a validade, a formação ou os efeitos de um contrato em relação a uma criança. Ibid.

[48] Artigo 9.o

Tratamento de categorias especiais de dados pessoais

1.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 relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. Ibid.

[49] ROCHFELD, J. Como qualificar os dados pessoais? Uma perspetiva teórica e normativa da União Europeia em face dos gigantes da Internet. Law, State and Telecommunications Review, [s. l.], v. 10, n. 1, p. 61–84, 2018. Disponível em: https://doi.org/10.26512/lstr.v10i1.21500. Acesso em: 28 maio 2021. P. 69.

[50] Tradução nossa “Princípio da Prestação de Contas”.

[51] Artigo 24.o

Responsabilidade do responsável pelo tratamento

1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

a implementação das obrigações previstas do regime geral de proteção de dados e que sejam capazes de demonstrar referida implementação, uma vez que a *accountablity* tem por fim promover por meio de boas práticas das entidades o correto te responsável tratamento dos dados dos indivíduos, como leciona a cartilha do *Center for Information Policy Leadership*[52].

Nesse diapasão, cria-se a figura do *Data Protection Officer* (DPO), nos artigos 37. °, 38. ° e 39. °[53], um profissional que tem, especificamente, a função de ajudar as empresas no

---

2 Caso sejam proporcionadas em relação às atividades de tratamento, as medidas a que se refere o n.º 1 incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento.

3. O cumprimento de códigos de conduta aprovados conforme referido no artigo 40.o ou de procedimentos de certificação aprovados conforme referido no artigo 42.o pode ser utilizada como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento. Ibid.

[52] HUNTON ANDREWS KURTH LLP. **Centre for information policy leadership**. [*S. l.: s. n.*], 2019. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_paper_-_learning_from_the_eu_gdpr_-_what_elements_should_the_us_ado....pdf.

[53] Artigo 37. °

Designação do encarregado da proteção de dados

1. O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que:

a) O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional;

b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou

c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9. ° e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.°.

2. Um grupo empresarial pode também designar um único encarregado da proteção de dados desde que haja um encarregado da proteção de dados que seja facilmente acessível a partir de cada estabelecimento.

3. Quando o responsável pelo tratamento ou o subcontratante for uma autoridade ou um organismo público, pode ser designado um único encarregado da proteção de dados para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e dimensão.

4. Em casos diferentes dos visados no n.°1, o responsável pelo tratamento ou o subcontratante ou as associações e outros organismos que representem categorias de responsáveis pelo tratamento ou de subcontratantes podem, ou, se tal lhes for exigido pelo direito da União ou dos Estados-Membros, designar um encarregado da proteção de dados. O encarregado da proteção de dados pode agir em nome das associações e de outros organismos que representem os responsáveis pelo tratamento ou os subcontratantes.

5. O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39. °

6. O encarregado da proteção de dados pode ser um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante, ou exercer as suas funções com base num contrato de prestação de serviços.

7. O responsável pelo tratamento ou o subcontratante publica os contactos do encarregado da proteção de dados e comunica-os à autoridade de controlo.

Artigo 38. °

Posição do encarregado da proteção de dados

1. O responsável pelo tratamento e o subcontratante asseguram que o encarregado da proteção de dados seja envolvido, de forma adequada e em tempo útil, a todas as questões relacionadas com a proteção de dados pessoais.

2. O responsável pelo tratamento e o subcontratante apoia o encarregado da proteção de dados no exercício das funções a que se refere o artigo 39.o, fornecendo-lhe os recursos necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento.

3. O responsável pelo tratamento e o subcontratante asseguram que da proteção de dados não recebe instruções relativamente ao exercício das suas funções. O encarregado não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções. O encarregado da proteção de dados informa diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante.

4. Os titulares dos dados podem contactar o encarregado da proteção de dados sobre todas questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos que lhe são conferidos pelo presente regulamento.

5. O encarregado da proteção de dados está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o direito da União ou dos Estados-Membros.

6. O encarregado da proteção de dados pode exercer outras funções e atribuições. O responsável pelo tratamento ou o subcontratante assegura que essas funções e atribuições não resultam num conflito de interesses.

Artigo 39. °

Funções do encarregado da proteção de dados

1. O encarregado da proteção de dados tem, pelo menos, as seguintes funções:

a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;

b) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

c) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35. °;

d) Coopera com a autoridade de controlo;

e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.o, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.

2. No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento. UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao

processamento de tais dados com o fim de protegê-los ao assegurar que aqueles que os detém estão cumprindo restritamente as regras impostas pela legislação premente na União Europeia (EU) por meio de um monitoramento, auditorias, treinamento de equipe *etc*.

Ademais, o RGPD salienta que quanto tais dados entram na categoria de risco demanda-se que seja realizado um *Data Protection Impact Assessment*,[54] conforme leciona o artigo 35. ° desta norma[55], com o intuito de ponderar as possíveis repercussões da proteção destes dados que podem ser rotulados de dados sensíveis ou frágeis.

---

tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

[54] Tradução nossa "Avaliação do impacto da proteção de dados".

[55] Artigo 35. °

Avaliação de impacto sobre a proteção de dados

1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.

2. Ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento solicita o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado.

3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.°1 é obrigatória nomeadamente em caso de:

a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;

b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9. °, n.°1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10. °; ou

c) Controlo sistemático de zonas acessíveis ao público em grande escala.

4. A autoridade de controlo elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados por força do n.°1. A autoridade de controlo comunica essas listas ao Comité referido no artigo 68.°.

5. A autoridade de controlo pode também elaborar e tornar pública uma lista dos tipos de operações de tratamento em relação aos quais não é obrigatória uma análise de impacto sobre a proteção de dados. A autoridade de controlo comunica essas listas ao Comité.

6. Antes de adotar as listas a que se referem os n.°4 e 5, a autoridade de controlo competente aplica o procedimento de controlo da coerência referido no artigo 63. ° sempre que essas listas enunciem atividades de tratamento relacionadas com a oferta de bens ou serviços a titulares de dados ou com o controlo do seu comportamento em diversos Estados-Membros, ou possam afetar substancialmente a livre circulação de dados pessoais na União.

7. A avaliação inclui, pelo menos:

Ainda nessa busca pelo aperfeiçoamento o RGPD requer o denominado *privacy by design* em que se exige dos criadores não se esqueçam de observar a proteção de dados na etapa de desenvolvimento de produtos, de serviços ou de projetos, vez que o legislador ao elaborar esta norma busca proteger a privacidade em todos os momentos evitando-se sua possível transgressão.[56]

Acompanhando esta tendência ao aprimoramento do RGPD a própria União Europeia cria uma equipe composta por civis, por representante do empresariado e por especialistas em determinadas áreas correlacionadas ao tema em crivo, especificamente

---

a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;

b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;

c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o n.°1; e

d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

8. Ao avaliar o impacto das operações de tratamento efetuadas pelos responsáveis pelo tratamento ou pelos subcontratantes, em especial para efeitos de uma avaliação de impacto sobre a proteção de dados, é tido na devida conta o cumprimento dos códigos de conduta aprovados a que se refere o artigo 40.o por parte desses responsáveis ou subcontratantes.

9. Se for adequado, o responsável pelo tratamento solicita a opinião dos titulares de dados ou dos seus representantes sobre o tratamento previsto, sem prejuízo da defesa dos interesses comerciais ou públicos ou da segurança das operações de tratamento.

10. Se o tratamento efetuado por força do artigo 6.o, n.°1, alínea c) ou e), tiver por fundamento jurídico o direito da União ou do Estado-Membro a que o responsável pelo tratamento está sujeito, e esse direito regular a operação ou as operações de tratamento específicas em questão, e se já tiver sido realizada uma avaliação de impacto sobre a proteção de dados no âmbito de uma avaliação de impacto geral no contexto da adoção desse fundamento jurídico, não são aplicáveis os n.°1 a 7, salvo se os Estados-Membros considerarem necessário proceder a essa avaliação antes das atividades de tratamento.

11. Se necessário, o responsável pelo tratamento procede a um controlo para avaliar se o tratamento é realizado em conformidade com a avaliação de impacto sobre a proteção de dados, pelo menos quando haja uma alteração dos riscos que as operações de tratamento representam. UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados).

[56] IRAMINA, 2020. P.97

destinado na identificação dos entraves para implementação do próprio regulamento intitulado *Multistakeholder Exert Group*[57].

Referido grupo produziu relatório em 2019 no qual expõem os principais entraves para efetiva funcionalidade da norma em comento, como: problemas em renovar o procedimento de consentimento dos indivíduos; empecilho nas atualizações de contratos e notas ou notificações informando as atualizações nas diretrizes de proteção de dados; necessidade de promover campanhas de conscientização e capacitação acerca da tema tanto para o usuário quanto aqueles que trabalham na área; premente demanda elaborar políticas especificamente destinada a violações de dados; etc.

Curiosamente, tais entraves evidenciaram que para um pleno cumprimento dos objetivos impostos na hodierna diretriz regulatória os Estados Membros encontraram, de forma quase unanime, certo óbice financeiro, uma vez que para realizar de forma plena a exigida *accountability* pela RGPD é necessário aplicação e destinação de um volume substantivo de recursos monetários para adequar as diversas etapas e garantir a plena conformidade do regulamento.[58]

Além disso, é importante esclarecer que embora os embora o Regulamento Geral de Proteção de Dados seja uma norma diretamente aplicável aos Estados Membro, com determina o artigo 288. °[59] do Tratado Sobre o Funcionamento da União Europeia (TFEU),

---

[57] MULTISTAKEHOLDER EXPERT GROUP. CONTRIBUTION FROM THE MULTISTAKEHOLDER EXPERT GROUP TO THE STOCK-TAKING EXERCISE OF JUNE 2019 ON ONE YEAR OF GDPR APPLICATION. Europa: União Europeia, 2019. Disponível em: https://ec.europa.eu/info/sites/default/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf. Acesso em: 24 maio 2021.

[58] IRAMINA, 2020. p.97.

[59] Artigo 288. º
(ex-artigo 249. º TCE)
Para exercerem as competências da União, as instituições adotam regulamentos, diretivas, decisões, recomendações e pareceres. O regulamento tem caráter geral. É obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.
A diretiva vincula o Estado-Membro destinatário quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios.
A decisão é obrigatória em todos os seus elementos. Quando designa destinatários, só é obrigatória para estes.

ainda sim é preciso que cada um incorpore medidas legais a nível nacional. Quanto a este quesito em Portugal o RGPD foi inserido no ordenamento jurídico por meio da Lei n.°58/2019[60], mais conhecida como Lei da Proteção de Dados Pessoais.

2.4 ANOTAÇÕES SOBRE A AUTORIDADE NACIONAL DE CONTROLO NA PROTEÇÃO DE DADOS SEGUNDO O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD)

No Regulamento Geral de Proteção de Dados a figura da autoridade nacional é preenchida pelo próprio Estado Membro, ou a quem dentro da estrutura estatal for designado este papel, que tem por função fazer cumprir as normas advindas de referido diploma legal. Esta forma de condução muito se assemelha a uma estrutura de governança, uma fez que cabe a autoridade nacional cumprir o papel de *enforcer*[61]. Isso significa que são capazes de abrirem investigações e, caso seja preciso, aplicar coimas que podem alcançar valores exorbitantes a depender da gravidade da infração.

Um bom exemplo para ilustrar a ação de uma autoridade nacional foi o caso envolvendo a empresa Google e o governo da França. Nele a autoridade de proteção de dados francesa decidiu aplicar coima na casa dos cinquenta milhões de euros a empresa americana após constar em investigação que as denuncias apresentadas por *None of Yours Business* e *La Quadratura du Net* - dois grupos que se propõem a defender a proteção de usuários - que estavam representando o interesse de mais de dez mil indivíduos, eram verdadeiras vez que ficou comprovado que o Google não foi transparente, apresentou informação inadequada e não houve consentimento válido dos usuários no quesito personalização de propaganda, já

As recomendações e os pareceres não são vinculativos. UNIÃO EUROPEIA. Tratado Sobre o Funcionamento da União Europeia (Versão Consolidada). Publicada em: 20/06/2016

[60] PORTUGAL. Lei da Proteção de Dados Pessoais. 8 ago. 2019.

[61] Nota explicativa: Nesse contexto trata-se de uma entidade pública ou funcionário público que tem por função aplicar leis, normas, regulamentos etc.

que se contatou dificuldade para os mesmos alterarem no segmento preferências como os seus dados seriam usados.[62]

Embora essa função mais coercitiva da governança exercida pela autoridade nacional de proteção de dados seja sempre mais eficiente não é o objetivo fim, pois com o próprio RGPD estabelece que o propósito a principal dele é provocar uma mudança cultural. Nesse sentido expõem Hodges que a maneira mais eficiente de alterar de facto o comportamento de um grupo de indivíduos num futuro próximo deve ser adotando um engajamento construtivo e responsivo das partes envolvidas.[63]

E com este intuito o legislador ao redigir o regulamento inseriu mecanismos na norma para que a autoridade nacional de proteção de dados possa por exemplo: fazer advertências; realizar repreensões; ordenar que os pedidos de exercício de direitos apresentados pelo titular dos dados nos termos do presente regulamento sejam cumpridos; exigir ratificação ou eliminação de dados pessoais ou limitação de seu processamento; estabelecer limitação temporariamente o definitiva ao tratamento de dados pessoais e, até mesmo, ordenar a sua proibição; emite ordem para a suspensão do envio de dados de determinado indivíduo para destinatários em outros países ou para organizações internacionais; entre outros. Estas ferramentas são intituladas de poderes de coerção e estão elencadas nas alíneas do artigo 58. °/2 do RGPD[64].

---

[62] FRANCE FINES GOOGLE €50 MILLION USING GDPR PRIVACY LAW. [S. l.], 2019. Disponível em: https://www.euronews.com/2019/01/21/france-fines-google-50-million-using-eu-s-transparency-and-consent-law. Acesso em: 17 out. 2021.

[63] HODGES, C. Delivering data protection: Trust and Ethical Culture. **The Legal Publisher Lexxion**, [*s. l.*], v. 4, n. 1, European Data Protection Law Review, p. 65–79, 2018. Disponível em: https://doi.org/10.21552/edpl/2018/1/9

[64] Artigo 58. °
Poderes
[...]
2. Cada autoridade de controlo dispõe dos seguintes poderes de correção:
a) Fazer advertências ao responsável pelo tratamento ou ao subcontratante no sentido de que as operações de tratamento previstas são suscetíveis de violar as disposições do presente regulamento;
b) Fazer repreensões ao responsável pelo tratamento ou ao subcontratante sempre que as operações de tratamento tiverem violado as disposições do presente regulamento;
c) Ordenar ao responsável pelo tratamento ou ao subcontratante que satisfaça os pedidos de exercício de direitos apresentados pelo titular dos dados nos termos do presente regulamento;

É oportuno esclarecer que os referidos mecanismos de coerção enumerados no artigo 58. ° devem ser exclusivamente aplicados em infrações de menor potencial ofensivo ou em situações em que a aplicação da coima acabe constituindo um encargo desproporcional. Desse modo, a autoridade nacional de controlo deve "a natureza, gravidade e duração da infração, o seu caráter doloso, as medidas voltadas para atenuar os danos sofridos, o grau de responsabilidade ou infrações anteriores, a via pela qual a infração chegou ao conhecimento da autoridade de controlo, o cumprimento das medidas ordenadas contra o responsável pelo tratamento ou subcontratante, o cumprimento de um código de conduta ou quaisquer outros fatores agravantes ou atenuantes."[65] Contudo, é imperioso salientar que referida reprensão não produz quaisquer efeito jurídico, uma vez que o não há vinculação de ação ou omissão daquele é responsável pelo tratamento dos dados ou subcontratante que simplesmente recebem a repreensão.

Além dos poderes de sanção e repreensão acima elencados cabe também a autoridade de controlo deter poderes consultivos e de autorização, desta forma compete a ela:

---

d) Ordenar ao responsável pelo tratamento ou ao subcontratante que tome medidas para que as operações de tratamento cumpram as disposições do presente regulamento e, se necessário, de uma forma específica e dentro de um prazo determinado;

e) Ordenar ao responsável pelo tratamento que comunique ao titular dos dados uma violação de dados pessoais;

f) Impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição;

g) Ordenar a retificação ou o apagamento de dados pessoais ou a limitação do tratamento nos termos dos artigos 16. º, 17. º e 18. º, bem como a notificação dessas medidas aos destinatários a quem tenham sido divulgados os dados pessoais nos termos do artigo 17.o, n.º 2, e do artigo 19. º;

h) Retirar a certificação ou ordenar ao organismo de certificação que retire uma certificação emitida nos termos dos artigos 42. º e 43.º, ou ordenar ao organismo de certificação que não emita uma certificação se os requisitos de certificação não estiverem ou deixarem de estar cumpridos;

i) Impor uma coima nos termos do artigo 83. º, para além ou em vez das medidas referidas no presente número, consoante as circunstâncias de cada caso;

j) Ordenar a suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais.

f) Impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição.

j) Ordenar a suspensão do envio de dados para destinatários em países terceiros ou para associações internacionais. UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados).

[65] Considerando 148. Ibid.

aconselhar o responsável nos termos do artigo 36 do diploma em voga (Anon., s.d.)[66]; emitir parecer cujo conteúdo avalie a compatibilidade de um código de ética já existente ou da criação de um e o novo regulamento segundo o artigo 40.°/5[67]; assentir o tratamento

[66] Artigo 36. °
Consulta prévia
1. O Responsável cabelo Tratamento consulta a Autoridade de Controlo Antes de Proceder Ao Tratamento quando uma Avaliação de Impacto Sobre a Proteção de Dados nos termos do artigo 35° indicar que o tratamento resultaria num Elevado Risco na ausência das Medidas Tomadas cabelo Responsável pelo tratamento para atenuar o risco.
2. Sempre que considerar que o tratamento previsto no n.°1 violaria o disposto no presente regulamento, nomeadamente se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, a autoridade de controlo, no prazo máximo de oito semanas a contar da receção do pedido de consulta, dá orientações, por escrito, ao responsável pelo tratamento e, se o houver, ao subcontratante e pode recorrer a todos os seus poderes apurar no artigo 58. o. Esse prazo pode ser prorrogado até seis semanas, tendo em conta a complexidade do tratamento previsto. A autoridade de controlo informa da prorrogação o responsável pelo tratamento ou, se o houver, o subcontratante no prazo de um mês a contar da data de receção do pedido de consulta, juntamente com os motivos do atraso. Esses prazos podem ser suspensos até que a autoridade de controlo tenha estabelecido como informações que solicitou para efeitos da consulta.
3. Quando consultar a autoridade de controlo nos termos do n.°1, o responsável pelo tratamento comunica-lhe os seguintes elementos:
a) Se for aplicável, a repartição de responsabilidades entre o responsável pelo tratamento, os responsáveis pelos conjuntos pelo tratamento e os subcontratantes executados no tratamento, nomeadamente no caso de um tratamento dentro de um grupo empresarial;
b) As finalidades e os meios do tratamento previsto;
c) As medidas e garantias previstas para a defesa dos direitos e liberdades dos titulares dos dados nos termos do presente regulamento;
d) Se aplicável, os contactos do encarregado da proteção de dados;
e) A avaliação de impacto sobre a proteção de dados prevista no artigo 35. °; e
f) Quaisquer outras informações solicitadas pela autoridade de controlo.
4. Os Estados-Membros consultam a autoridade de controlo durante a preparação de uma proposta de medida legislativa a adotar por um parlamento nacional ou de uma medida regulamentar baseada nessa medida legislativa, que está relacionada com o tratamento de dados.
5. Não obstante o n.°1, o direito dos Estados-Membros pode exigir que o responsável pelo tratamento consulte a autoridade de controlo e dela obtenham uma autorização prévia em relação ao tratamento por um responsável no exercício de uma missão de interesse público, incluindo o tratamento por motivos de proteção social e de saúde pública. Ibid

[67] Artigo 40. °
Códigos de conduta
[...]
5. As associações e outros organismos a que se refere o n.°2 do presente artigo que tencionem elaborar um código de conduta, ou alterar ou aditar um código existente, apresentar o projeto de código, alterar ou aditar à autoridade de controlo que é competente por força do artigo 55.°. A autoridade de controlo emite um parecer sobre a conformidade do projeto de código de conduta ou da alteração ou do aditamento com o presente regulamento e aprova este projeto, esta alteração ou este aditamento se determinar que são devidos adequados. Ibid.

mencionado no artigo 36.°/5[68]; emitir e renovar certificações segundo o disposto no artigo 43.°[69]; igualmente certificar nos ditames do artigo 42. °/5[70]; tutelar as clausulas de proteção

[68] Ver nota de rodapé número 64

[69] Artigo 43. °

Organismos de certificação

1. Sem prejuízo das atribuições e poderes da autoridade de controlo competente nos termos dos artigos 57. ° e 58. ° um organismo de certificação que possui um nível adequado de competência em matéria de proteção de dados emite e renova a certificação, após informar a autoridade de controlo para que esta escolha exercer as suas competências nos termos do artigo 58. °, n.°2, alínea h), sempre que necessário. Os Estados-Membros asseguram que estes organismos de certificação são acreditados:

a) Pela autoridade de controlo que é competente nos termos do artigo 55. ° ou 56. °;

b) Pelo organismo nacional de acreditação, designado nos termos do Regulamento (CE) n.°765/2008 do Parlamento Europeu e do Conselho (20), em compliance com a norma EN-ISO / IEC 17065/2012 e com os requisitos adicionais produzidos pela autoridade de controlo que é competente nos termos do artigo 55. ° ou 56.°.

2. Os organismos de certificação, n. º1 são acreditados em compliance com o mesmo, apenas se:

a) Tiverem determinada que gozam de independência e preparação dos conhecimentos em relação ao objeto da certificação, de forma satisfatória para a autoridade de controle competente;

b) Se ela comprometeu-se a respeitar os critérios apurados no artigo 42. °, n.°5, e influenciado pela autoridade de controlo que é competente por força do artigo 55. o ou 56. o ou pelo Comité por força do artigo 63. °;

c) Tiverem estabeleceu procedimentos para a emissão, revisão periódica e retirada de procedimentos de certificação, selos e marcas de proteção de dados;

d) Tiverem estabeleceu procedimentos e estruturas para tratar reclamações relativas a violações de certificação ou à forma como uma certificação tenha sido implementada pelo tratamento ou subcontratante, e para tornar estes procedimentos e estruturas transparentes para os titulares dos dados e o público; e

e) Demonstrarem, de forma satisfatória para a autoridade de controlo competente, que as suas funções e atribuições não implicam um conflito de interesses.

3. A acreditação dos organismos de certificação nos n.°1 e 2 do presente artigo, é efetuada com base nos critérios cumpridos pela autoridade de controlo que é competente por força do artigo 55. ° ou 56. ° ou pelo Comité por força do artigo 63.°. No caso de acreditações nos termos do n.°1, alínea b), do presente artigo, esses requisitos complementam os requisitos do Regulamento (CE) n.°765/2008 e as regras técnicas que descrevem os métodos e procedimentos dos organismos de certificação.

4. Os organismos de certificação a que se referência o n.°1 são responsáveis pela correta avaliação necessária à certificação, ou pela revogação dessa certificação, sem prejuízo da responsabilidade que cabe ao responsável pelo tratamento ou ao subcontratante pelo cumprimento do presente regulamento. A acreditação é emitida por um período máximo de cinco anos e pode ser renovada nas condições, desde que o organismo de certificação reúna os requisitos necessários no presente artigo.

5. Os organismos de certificação a que se referência o n.°1 fornece às autoridades de controlo os motivos que levaram à concessão ou revogação da certificação solicitada.

6. Os requisitos exigidos no n.°3 do presente artigo, e os critérios de aprovação no artigo 42. °, n.°5, são publicados pela autoridade de controlo sob uma forma facilmente acessível. As autoridades de controlo também comunicam estes requisitos e estas informações ao Comité. O Comité recolhe todos os procedimentos de certificação e seleção de proteção de dados num registo e disponibiliza-os ao público por todos os meios adequados.

7. Sem prejuízo do capítulo VIII, autoridade de controlo competente ou o organismo nacional de acreditação revoga uma acreditação do organismo de certificação nos termos do n.°1 do presente artigo, se as condições para a acreditação não incluída ou devida de estar reunidas, ou se as medidas tomadas pelo organismo de certificação violarem o presente regulamento.

8. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 92. °, a fim de especificar os requisitos a ter em conta aos procedimentos de certificação em matéria de proteção de dados constar do artigo 42. °, n.°1.

9. A Comissão pode adotar atos de execução estabelecendo normas técnicas para os procedimentos de certificação e os selos e marcas em matéria de proteção de dados, e regras para promover e reconhecer esses procedimentos de certificação, selos e marcas. Os atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93. °, n.°2. UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados).

[70] Artigo 42. °

Certificação

[...]

5. A certificação prevista no presente artigo é emitida pelos organismos de certificação no artigo 43. ° ou pela autoridade de controlo competente, com base nos critérios por esta obrigação por força do artigo 58. °, n.°3, ou pelo Comité por força do artigo 63.°. Caso os critérios sejam observados pelo Comité, podem ter como resultado uma certificação comum, o Selo Europeu de Proteção de Dados. Ibid.

de dados dos artigos 28. °/8 e 46. °/2[71], alínea *d)*; anuir as cláusulas contratuais do artigo 46. °/3, *a)*[72]; validar acordos administrativos do artigo 46. °/3, *b)*[73]; e, por fim, aquiescer regras cabíveis a empresas segundo leciona o artigo 47. °[74].[75]

---

[71] Artigo 28. °
Subcontratante
[...]
8. A autoridade de controlo pode estabelecer cláusulas de tipo contratuais para as referências relacionadas com os n. os 3 e 4 do presente artigo e de acordo com o procedimento de controlo da coerência referida no artigo 63. º.
[...]
Artigo 46. º
Transferências mencionadas a seguir
[...]
2. Podem ser previstos como concluídos no n.º1, sem requerer permissão específica de uma autoridade de controle, por meio de:
d) Cláusulas-tipo de proteção de dados adotados por uma autoridade de controlo e aprovadas pela Comissão pelo procedimento de exame referido no artigo 93°, n.°2; Ibid.

[72] ver nota de rodapé subsequente.

[73] Artigo 46. °
Transferências mencionadas a seguir
[...]
3. Sob reserva de autorização da autoridade de controlo competente, podem também ser fornecidos como conforme n.º1, nomeadamente por meio de:
a) Cláusulas contratuais entre os responsáveis pelo tratamento ou subcontratantes e os responsáveis pelo tratamento, subcontratantes ou destinatários dos dados pessoais no país terceiro ou organização internacional; ou
b) Disposições a inserir nos acordos administrativos entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados.

[74] Artigo 47. °
Regras vinculativas aplicáveis às empresas
1. Pelo procedimento de controlo da coerência previsto no artigo 63. °, a autoridade de controlo competente aprova regras vinculativas aplicáveis às empresas, que devem:
a) Ser juridicamente vinculativas e aplicáveis a todas as entidades em causa do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, incluindo os seus funcionários, as quais deverão assegurar o seu cumprimento;
b) Conferir expressamente aos titulares dos dados direitos oponíveis relativamente ao tratamento dos seus dados pessoais; e
c) Preencher os requisitos estabelecidos no n.º 2.
2. As regras vinculativas aplicáveis às empresas a que se refere o n.º 1 especificam, pelo menos:
a) A estrutura e os contactos do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta e de cada uma das entidades que o compõe;
b) As transferências ou conjunto de transferências de dados, incluindo as categorias de dados pessoais, o tipo de tratamento e suas finalidades, o tipo de titulares de dados afetados e a identificação do país ou países terceiros em questão;
c) O seu caráter juridicamente vinculativo, a nível interno e externo;

d) A aplicação dos princípios gerais de proteção de dados, nomeadamente a limitação das finalidades, a minimização dos dados, a limitação dos prazos de conservação, a qualidade dos dados, a proteção dos dados desde a conceção e por defeito, o fundamento jurídico para o tratamento, o tratamento de categorias especiais de dados pessoais, as medidas de garantia da segurança dos dados e os requisitos aplicáveis a transferências posteriores para organismos não abrangidos pelas regras vinculativas aplicáveis às empresas;

e) Os direitos dos titulares dos dados relativamente ao tratamento e regras de exercício desses direitos, incluindo o direito de não ser objeto de decisões baseadas unicamente no tratamento automatizado, nomeadamente a definição de perfis a que se refere o artigo 22.°, o direito de apresentar uma reclamação à autoridade de controlo competente e aos tribunais competentes dos Estados-Membros nos termos do artigo 79.°, bem como o de obter reparação e, se for caso disso, indemnização pela violação das regras vinculativas aplicáveis às empresas;

f) A aceitação, por parte do responsável pelo tratamento ou subcontratante estabelecido no território de um Estado-Membro, da responsabilidade por toda e qualquer violação das regras vinculativas aplicáveis às empresas cometida por uma entidade envolvida que não se encontre estabelecida na União; o responsável pelo tratamento ou o subcontratante só pode ser exonerado dessa responsabilidade, no todo ou em parte, mediante prova de que o facto que causou o dano não é imputável à referida entidade;

g) A forma como as informações sobre as regras vinculativas aplicáveis às empresas, nomeadamente, sobre as disposições referidas nas alíneas d), e) e f) do presente número, são comunicadas aos titulares dos dados para além das informações referidas nos artigos 13. ° e 14. °;

h) As funções de qualquer encarregado da proteção de dados, designado nos termos do artigo 37. ° ou de qualquer outra pessoa ou entidade responsável pelo controlo do cumprimento das regras vinculativas aplicáveis às empresas, a nível do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, e pela supervisão das ações de formação e do tratamento de reclamações;

i) Os procedimentos de reclamação;

j) Os procedimentos existentes no grupo empresarial ou no grupo de empresas envolvidas numa atividade económica conjunta para assegurar a verificação do cumprimento das regras vinculativas aplicáveis às empresas. Esses procedimentos incluem a realização de auditorias sobre a proteção de dados e o recurso a métodos que garantam a adoção de medidas corretivas capazes de preservar os direitos dos respetivos titulares. Os resultados dessa verificação devem ser comunicados à pessoa ou entidade referida na alínea h) e ao Conselho de Administração da empresa ou grupo empresarial que exerce o controlo ou do grupo de empresas envolvidas numa atividade económica conjunta, devendo também ser facultados à autoridade de controlo competente, a pedido desta;

k) Os procedimentos de elaboração de relatórios e de registo de alterações às regras, bem como de comunicação dessas alterações à autoridade de controlo;

l) O procedimento de cooperação com a autoridade de controlo para assegurar o cumprimento, por qualquer entidade do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, em especial facultando à autoridade de controlo os resultados de verificações das medidas referidas na alínea j);

m) Os procedimentos de comunicação, à autoridade de controlo competente, de todos os requisitos legais a que uma entidade do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta esteja sujeita num país terceiro que sejam passíveis de ter forte impacto negativo nas garantias dadas pelas regras vinculativas aplicáveis às empresas; e

n) Ações de formação especificamente dirigidas a pessoas que tenham, em permanência ou regularmente, acesso a dados de natureza pessoal.

3. A Comissão pode especificar o formato e os procedimentos de intercâmbio de informações entre os responsáveis pelo tratamento, os subcontratantes e as autoridades de controlo no que respeita às regras vinculativas aplicáveis às empresas na aceção do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.o, n.º 2. UNIÃO EUROPEIA. Regulação (EU) 2016/79

Esquiva-se desta lógica o artigo 58. °/3, *b)* [76] do RGPD ao permitir que a autoridade de controlo nacional atenda pedido do Parlamento Europeu para emitir parecer sobre determinado assunto ou por iniciativa própria, ademais, pode os Estados Membros outorgar esta faculdade a outras entidades públicas o que classifica esta cláusula com uma cláusula de abertura, entretanto, ela não obteve êxito em ser incluída na Lei de Execuções do Regulamento Geral de Proteção de Dados em Portugal.

2.5 OS DADOS SENSÍVEIS NO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD)

2.5.1 Conceito de dados sensíveis

Em tese, não há conceito pré-definido no Regulamento de Geral de Proteção de Dados fixando o que são dados sensíveis ou especiais, entretanto, o Considerando 51[77] do

---

do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados).

[75] CORDEIRO, 2020. p. 419.

[76] Artigo 58. °
Poderes
[...]
3. Cada autoridade de controlo dispõe dos seguintes poderes consultivos e de autorização:
b) Emitir, por iniciativa própria ou se lhe for solicitado, pareceres dirigidos ao Parlamento nacional, ao Governo do Estado-Membro ou, nos termos do direito do Estado-Membro, a outras instituições e organismos, bem como ao público, sobre qualquer assunto relacionado com a proteção de dados pessoais; UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados).

[77] Considerando 51: Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais dados pessoais não deverão ser objeto

regulamento traz alguns parâmetros para compreender este tema, assim, exprime que valem salvaguarda específica os dados pessoais que por sua natureza delicada podem pôr em xeque direitos e liberdades fundamentais, ou seja, caso tais informações forem tratadas com desídias poderá implicar em riscos.

Desta maneira, pode-se descrever dados sensíveis com sendo aqueles que carecem que prudência ao serem processados tendo em conta que a negligência para com eles pode gerar efeitos negativos afetando toda a sorte de direitos do indivíduo a que pertencem.

A despeito de serem classificados como uma categoria especial de dados intrinsecamente pessoais vê-se no dia a dia uma grande incidência deles, a exemplo disso cita-se que: comparecer a determinada manifestação tem potencial de demostrar o viés político de alguém, o nome e a morada podem indicar a origem racial ou étnica do indivíduo, entre outros.[78]

2.5.2 Tipos de dados especiais

Como já assentado no tópico precedente carece o Regime Geral de Proteção de Dados de definição de dados sensíveis porém traz em seu amago, mais precisamente no artigo 9.°[79],

---

de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros 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. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais. UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados

[78] CORDEIRO, 2020. p. 133-134.

[79] Artigo 9. °
Tratamento de categorias especiais de dados pessoais

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

2. O disposto no n. º 1 não se aplica se se verificar um dos seguintes casos:

a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.º 1 não pode ser anulada pelo titular dos dados;

b) Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados;

c) Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento;

d) Se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares;

e) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;

f) Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional;

g) Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;

h) Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.º 3;

i) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;

j) Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n. º 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.

3. Os dados pessoais referidos no n.º 1 podem ser tratados para os fins referidos no n.º 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas

oito tipos de dados especiais que podem ser subdivididos em: dados de origem racial; dados de origem étnica; dados que evidenciam opiniões políticas; dados que tracem convicções religiosas ou filosóficas; dados que indiquem filiação sindical; dados genéticos; dados biométricos; dados relativos à saúde; e dados relativos a orientação sexual ou referentes à vida sexual.

Os dados de origem racial têm por fim combater rotulagem de certos sujeitos por raça, deste modo evidenciando a intenção do legislador europeu de combater a discriminação. Sendo assim, entram nesta classe de dados características físicas, a exemplo: formato dos olhos e nariz, cor da pele, entre outros, isto é, traços biológicos e hereditários. Isso difere dos dados de origem étnica, visto que estes estão mais atrelados a particularidades culturais comuns pertencentes a um certo povo, como o sobrenome, o local de nascimento, o idioma, a história, os usos e costumes, os valores e os hábitos de prática da convivência social (ex.: na sociedade japonesa há uma forma específica de se cumprimentar alguém com uma reverência).[80]

Já os dados catalogados como de origem política podem são aqueles que englobam a afiliação em partidos políticos, assinatura em petições públicas, participação em manifestações políticas, doações a organizações políticas, tipo de roupa utilizada e, até mesmo, comportamento em redes sociais. Os dados ditos de filiação sindical podem ser confundidos com o anterior, entretanto, neste especificamente foi cunhado para proteger o direito de livre associação tão historicamente perseguida atividade sindical.[81]

Para Menezes de Cordeiro o legislador ao conferir anteparo aos dados concernentes as convicções religiosas o fiz tanto pensando na assunção do credo quanto nas vertentes que

autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes.

4. Os Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde. Ibid.

[80] CORDEIRO, 2020.p.136.

[81] Ibid. p.136-138

a negam, ateísmo e agnosticismo. Enquanto atribui aos dados relativos as convicções filosóficas caráter mais amplo, pois admite também se alcance opiniões ideológicas.[82]

Os dados genéticos, positivados na artigo 4.°/13[83], resultam de informações colhidas a partir de amostra biológica de certo indivíduo como "análise de cromossomas, ácido desoxirribonucleico (ADN) ou ácido ribonucleico (ARN), ou da análise de um outro elemento que permita obter informações equivalentes"[84] que indicam perfil psicológico, físico, médico, ascendência, descendência ou outras ligações familiares conhecidos ou não pelo seu titular que podem suscitar hostilidade no âmbito criminal, financeiro (banca, bolsas e seguros) ou laboral.[85]

Em contrapartida, os dados relativos à saúde, presente no artigo 4. °/*15)*[86], são de caráter mais amplo, uma vez que abrange todas as informações de saúde-física e mental de uma pessoa cobrindo o passado, o presente e até o futuro, que podem ser obtidas via inscrição para a prestação um serviço de saúde, por meio de resultados de exame clínicos, histórico clínico, entre outros conforme enumerado no Considerando 35[87].

---

[82] Ibid. p.137.

[83] Artigo 4. °
Definições
Para efeitos do presente regulamento, entende-se por:
13) «Dados genéticos», os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa;

[84] Considerando 34. UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados

[85] CORDEIRO, 2020. p.137-138.

[86] Artigo 4. °
Definições
Para efeitos do presente regulamento, entende-se por:
[...]
15)«Dados relativos à saúde», dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde; Ibid.

[87] Ibid.

Inclusive com a veloz aprimoramento tecnológica promovido pela 4. ° Revolução Industrial há aqueles defendem que também sejam abrangidos por esses dispositivos os dados recolhidos e processados por aplicativos de saúde, *fitness apps* presentes em celulares, computadores, *Tablet e Notebook* e, até mesmo, *smart whatches ou smart fones*.

Além disso, são identicamente tutelados pelo diploma em comento os dados alusivos à vida sexual ou à orientação sexual de um indivíduo que podem ser coletados das mais diversas formas desde produtos farmacêuticos e intervenções cirúrgicas até participação em eventos ou maneira de se vestir.[88] Convém aclarar que a defesa do sigilo destes dados tem respaldo no artigo 13.º/2[89] da Constituição da República Portuguesa (CRP) e concomitantemente no artigo 21.º do RGPD[90].

Esclarece, pois que aos dados biométricos dedicar-se tópico apartado em virtude da sua importância para o estudo em questão, assim sendo passa-se para a efetiva explanação deles.

---

[88] CORDEIRO, 2020.p.141-142-

[89] Artigo 13.º

Princípio da igualdade

1. Todos os cidadãos têm a mesma dignidade social e são iguais perante a lei.

2. Ninguém pode ser privilegiado, beneficiado, prejudicado, privado de qualquer direito ou isento de qualquer dever em razão de ascendência, sexo, raça, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou orientação sexual. PORTUGAL, Constituição da República Portuguesa. Publicada em: 2/04/1976.

[90] Artigo 21.º

Direito de oposição

1. O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.o, n.º 1, alínea e) ou f), ou no artigo 6.o, n.º 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial. UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados).

2.6 O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD) E OS DADOS BIOMÉTRICOS

No Regulamento Geral de Proteção de Dados os dados biométricos, presentes do artigo 4. °/*14)*[91], são conceituados como aqueles decorrentes de tratamento técnico que contenham características físicas, comportamentais ou fisiológicas de certa pessoa que bastam para constatar a identificação dela.

Com isso, constata-se que o legislador europeu ratifica em lei definição restrita dos são biomédicos ao afirmar que somente os serão considerados aqueles que permitam identificação precisa do indivíduo e que sejam resultantes de um tratamento técnico específico que faculte este reconhecimento categórico. Sendo assim, entra neste grupo comportam dados próprios da face, íris, voz, odor, micro bioma e impressões digitais.[92]

Entretanto, destaca-se a ressalva do Considerando 51[93] em que apenas aqueles dados faciais advindos de fotografias biométricas contam para a efetivação desta norma como as

---

[91] Artigo 4.º
Definições
Para efeitos do presente regulamento, entende-se por:
[...]
14)
«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 dactiloscópicos; Ibid.

[92] CORDEIRO, 2020.p.140

[93] Considerando 51: Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros 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. Para além dos requisitos específicos para este tipo de

que constam nos modernos modelos de passaportes digital ou cartão de cidadão europeu[94], assim exclui-se sumariamente as fotos comuns.

Algo inegável quanto aos dados biométricos e que eles sofrem modificações com o decurso do tempo devido ao envelhecimento, alterações em virtude de doenças e transformações intencionais de cunho estético com as cirurgias plásticas. Apesar disso, seu emprego ainda é extremamente vasto compreendendo desde o setor público, principalmente os ligados a segurança pública, quanto no setor privado no qual o uso pode destravar por meio de leitura facial ou de íris de uma porta ou em uso meramente pessoal mesma técnica ser usada por sistemas similar para destravar a tela de um. celular ou qualquer outro *gadget* de uso pessoal.

2.6.1 O tratamento dos dados sensíveis no RGPD

Extrai-se da leitura do artigo 9. º do RGPD[95] que aos dados sensíveis foi designado certo regime próprio de tratamento, ou seja, um regime de tratamento especial distinto do regime comum circunscrito no artigo 6. º[96] no mesmo diploma. A justificativa legal para tal diferenciação se dá em virtude da natureza frágil destes dados o que exigiria requisitos legais mais rigorosos. E embora o regulamento em seus artigos enumere diversos fundamentos que embasam a demanda por um regime de tratamento próprio dois chamam a atenção, sendo os seguintes: o consentimento explícito e os dados tornados público pelo próprio titular.

---

tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais. UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados

[94] TJUE 17-out-2013, processo c-291/12

[95] Ver ponto 79.

[96] Ver ponto 46.

No caso do consentimento requer-se que este seja explicito, ou seja, o indivíduo ao deparara-se com a utilização de seus dados biométricos, por exemplo, para o funcionamento de aplicativo de celular deve ser indagado pelo sintam de software se está disposto ou não em conceder aquele informação, uma vez que como já explanado no primeiro capítulo desta dissertação é sabido que há no mercado sistemas que propiciam o reconhecimento da alguém de fácil acesso que podem utilizar tais informações com o intuito de inseri-las num banco de imagens como o Google Imagens e terá acesso a diversos outros dados desde de como quais lugares aquele indivíduo frequenta até que círculos de amizade tem.

Já quanto aos dados que são publicitados pelo próprio titular, vide artigo 9. º/2, *e)*, interpreta-se que ele renunciou a proteção conferida a tais dados, vez que assume que o possível tratamento ilícito delas não o lesa ou seja enfadonho, em caso de blogs, Facebook ou Instagram.[97]

[97] CORDEIRO, 2020.p. 245-246.

CAPÍTULO III - PROPOSTA DE REGULAMENTO QUE ESTABELECE REGRAS HARMONIZADAS SOBRE INTELIGÊNCIA ARTIFICIAL NA COMUNIDADE EUROPEIA

Vai de encalço ao assunto tratado nesta dissertação esmiuçar a proposta de regulamento da inteligência artificial, isso pois como fica claro na leitura de seu título ela tem por intento realizar uniformização das normas acerca da inteligência artificial presentes na União Europeia. Sendo assim, tendo por esta intenção busca traçar uma linha de raciocínio ao explicar a conjuntura na qual surge essa ideia de normatização da IA na União Europeia.

Com isso pretende-se. trazer a base jurídica para tanto; perpassar pelos motivos e objetivos; determinar a quem ela aplica-se; elencar quais práticas são proibidas; e, ao final, falar dos sistemas de riscos elevados.

3 NOTAS SOBRE A PROPOSTA DE REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA UNIÃO EUROPEIA

3.1 EXPOSIÇÕES DE MOTIVOS E OS OBJETIVOS DA PROPOSTA

No documento que contêm a proposta de regulamento para a uniformidade acerca da utilização da inteligência artificial (IA) na União Europeia o legislador logo expõe que em virtude da frenética ascensão da mesma e dos proveitos a se ganhar na área social e econômica, sendo especialmente necessária naqueles considerados de maior impacto – saúde, meio ambiente, agricultura, finanças, alterações climáticas, setor público, mobilidade etc. – não se pode mais postergar, portanto, este deve ser enfrentado com a máxima de cuidado uma vez que tais benesses também trazem consigo desconhecidas ameaças e, possivelmente, consequências nefastas. À vista disso, cabe ao legislador europeu tratar este assunto com cautela para alcançar uma ótica prudente, em favor de tanto propiciar a

hegemonia da União neste novo campo a ser desbravado quanto preservar valores, princípios e direitos fundamentais positivados pela mesma e garantidos aos cidadãos europeus. [98]

A apresentação deste documento faz-se cumprir o compromisso de Ursula von der Leyen ao subscrever nas orientações políticas de 2019-2024 nas quais determina que a Comissão Europeia fica ao cargo de apresentar proposta legislativa que abrangesse inferências humanas e éticas da inteligência artificial. Logo após, em 19 de fevereiro de 2019, é divulgado o "Livro branco sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança"[99], manuscrito no qual busca promoção da IA atentando-se aos riscos da legitimação da mesma via ecossistemas de confiança por meio de adoção pelos Estados Membros de uma lei regulando sua utilização. [100]

Sendo assim, depreende-se da leitura do Livro Branco que a inteligência artificial deve ser considerada um aparato tecnológico que tem por finalidade promover o bem-estar dos seres humanos, portanto, para tais dispositivos atuarem em solo europeu devem ser cumprir norma legal específica, assim, salvaguardando o papel de destaque da União Europeia neste campo cumprindo quesitos como segurança, confiança e ética, conforme extrai-se das conclusões a reunião extraordinária do Conselho Europeu de 2 de outubro de 2020.[101]

Acresce aos argumentos, já delineados a advertência extraída das conclusões que o Conselho Europeu faz na Carta dos Direitos Fundamentais no contexto da inteligência artificial e da transformação digital, ao afirmar ser preciso superar a complexidade e

---

[98] p. 1.

[99] COMISSÃO EUROPEIA. **Livro Branco sobre a inteligência artificial - uma abordagem europeia virada para a excelência e a confiança**. [*S. l.: s. n.*], 2020. Disponível em: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_pt.pdf.

[100] COMISSÃO EUROPEIA. **Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos**. Bruxelas, 23 abr. 2021. P1.

[101] CONSELHO EUROPEU. **Reunião extraordinária do Conselho Europeu (1 e 2 de outubro de 2020) – Conclusões**. Bruxelas/BE: [*s. n.*], 2021. P.6.

obscuridade do tema sem esquecer que a IA tem elevado grau de imprevisibilidade tendo em vista a autonomia.[102]

Com isso, os objetivos específicos da proposta de regulamento de harmonização em matéria de inteligência artificial são: *i)* salvaguardar que os sistemas que usem I.A. ofertados no mercado da comunidade europeia sejam seguros e de acordo com a legislação que aborde direitos fundamentais e valores do bloco; *ii)* acautelar a segurança jurídica como finalidade de promover a vinda de investimentos para esse setor; *iii)* aplicar ade forma efetiva a norma sobre o tema; *iv)* proporcionar a promoção e expansão de mercado exclusivo de IA seguras e confiáveis.[103]

3.4 PRÁTICAS PORIBIDAS DE INTELIGÊNCIA ARTIFICIAL

Embora a utilização de inteligência artificial tenha vários proveitos não há como negar que a mesma também pode ser utilizada para fins duvidosos em que promova práticas exploratórias, manipuladoras e de controle social, portanto, considera-se práticas proibidas de inteligência artificial aquelas que "desrespeitam valores da União, como a dignidade do ser humano, a liberdade, a igualdade, a democracia e o Estado de direito, bem como direitos fundamentais da União, incluindo o direito à não discriminação, à proteção de dados pessoais e à privacidade, e os direitos das crianças.", conforme estabelece o Considerando 15[104].

Em linhas gerais fica proibido segundo o artigo 5. º: colocar no mercado serviço ou sistema de IA que possa manipular a consciência de uma pessoa com o intuito de alterar seu comportamento a ponde de causar danos físicos e psicológicos a ela própria ou que ela possa fazer a terceiros; colocar no mercado serviço ou software de IA que se aproveite de qualquer

[102] CONSELHO EUROPEU. **Conclusões da Presidência – A Carta dos Direitos Fundamentais no contexto da inteligência artificial e da transformação digital**. Bruxelas/BE: [*s. n.*], 2020. p.3.

[103] COMISSÃO EUROPEIA, 2021.

[104] UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados

tipo de fragilidade de um certo grupo de indivíduos devido a idade, deficiência física ou mental persuadindo-as a causar danos a si ou outrem; que autoridades públicas usarem IA com o fim de avaliar ou classificar pessoas com base no comportamento social, característica da personalidade ou pessoal; também participando deste rol o emprego indevido de sistemas de IA que façam uso de identificação biométrica seja à distância o em tempo real.

3.5 OS DADOS BIMÉTRICOS NA PROPOSTA DE REGULAMENTO DE INTELIGÊNCIA ARTIFICIAL

O legislador europeu ao elaborar a propositura da norma que regula atividade de inteligência artificial emprega o já existente parâmetro de dados biométricos que está consonância com o "artigo 4. º, ponto 14, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho35, do artigo 3. º, ponto 18, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho36 e do artigo 3. º, ponto 13, da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho."[105]

Quanto ao tema identidade biométrica à distância é estabelecido como um sistema de IA em que tem por funcionalidade a identificação de certo indivíduo via comparação de informações contidas em um banco de dados biométricos com os dados desta natureza da pessoa procurada.

Para além, da sua funcionalidade o próprio legislador considera que a tal tecnologia pode ser usada "em tempo real" e "em deferido". Aqueles que operam "em tempo real" se distinguem, basicamente, pelo facto de aplicarem o que se denomina de "ao vivo" ou "quase ao vivo", uma vez que a o processamento, a comparação e a identificação dar-se-ão de imediato ou, pelo menos, sem atraso significativo mesmo que ocorra ligeiros problemas no *software* de IA operado em vídeo monitoramento e demais aparatos análogos. Em

[105] Considerando 7. COMISSÃO EUROPEIA, 2021.P.22

contrapartida, os sistemas "em deferido" são aqueles que analisam imagens obtidas de circuito fechado de vigilância ou de outras formas de dispositivos privados a posteriori.[106] Ressalva o legislador no Considerando 23 que em caso de aplicação de tecnologia de inteligência artificial à distância em tempo real em espaços comuns para manutenção de ordem pública implica necessariamente em tratamento de dados biométricos e, em regra, acarretaria na sua proibição segundo "o artigo 16.o do TFUE, devem aplicar-se como *lex specialis* relativamente as regras em matéria de tratamento de dados biométricos previstas no artigo 10.o da Diretiva (UE) 2016/680, regulando assim essa utilização e o tratamento de dados biométricos conexo de uma forma exaustiva."[107]

Com isso, para o uso dos mesmos sem ser para fins policiais - em que se aplica requisitos de autorização e regras de execução previstas no ordenamento jurídico do Estado Membro – deve-se seguir o disposto no "artigo 9. º n.º 1, do Regulamento (UE) 2016/679, do artigo 10.o, n.º 1, do Regulamento (UE) 2018/1725 e do artigo 10. º da Diretiva (UE) 2016/680".[108]

De resto, quanto aos dados biométricos é nítida a tentativa do legislador europeu na proposta de harmonização de regras para inteligência artificial em salvaguardar diversos aspetos que a possam tornar a utilização deste tipo de tecnologia nocivos aos cidadãos. Desta forma, insere conceito vasto sobre dados biométricos classificando-os como dados pessoais nos quais se contem características físicas, comportamentais ou fisiológicas de uma pessoa que permite confirmar a sua identidade. Desta forma, inclui-se infirmações obtidas via datiloscopia e de imagem do rosto, obtidas.

Não se olvidou também há incluir como dados biométricos proibidos, incluído artigo 5. º da proposta de regulamento, aqueles advindos de *softwares* capazes de reconhecer emoções e aqueles que também sejam desenvolvidos especificamente para pessoas singulares com características específicas, como: sexo, coloração de cabelo, cor dos olhos,

[106] Considerando 8. Ibid.
[107] Considerando 23. Ibid.
[108] Considerando 24. Ibid.

idade, se possui ou não tatuagem orientação sexual, origem étnica e, até mesmo, orientação política. [109]

[109] Considerando 33, 34, e 35. Ibid.

CAPÍTULO IV - RESPONSABILIDADE CIVIL *VS.* O RECONHECIMENTO FACIAL

Diante o caminho percorrido é chegado a hora de confrontar a responsabilidade civil e as normas as quais são objetos centrais deste trabalho. Desta forma, passa-se para a exploração da interação do Regulamento Geral de Proteção de Dados (RGDP) e da propositura de Regulamentação de Inteligência Artificial com este ramo do Direito Civil.

4 A RESPONSABILIDADE CIVIL NO REGULAMENTO GERAL DE PROTELÇAO DE DADOS (RGPD)

No tocante a responsabilidade civil o RGPD garante, nos termos do artigo 82. º/1, que qualquer pessoa que tenha sofrido danos matérias e imateriais devido a violação dos preceitos elencados neste regulamento tem o direito de buscar reparação via indenização. E para a efetivação do ressarcimento pretendido segue-se o determinado pelo artigo 33. º da Lei de Proteção de Dados Pessoais que em seu ponto 1 que estende a responsabilidade do subcontratante ao descumprimento da legislação local de cada Estado Membro acerca da proteção de dados pessoais e no ponto 3 afirma que será aplicado à responsabilidade civil o regime contido na Lei n.º 67/2007, de 31 de dezembro com a devidas adaptações.

4.1 OS ELEMENTOS

Como é sabido a responsabilidade civil somente será efetivada quando comprovado os três elementos que a compõem, sendo eles. a ilicitude do facto, o dano e a causalidade. Tedo isso em mente, passa-se a analisar um a um a luz do Regulamento Geral de Proteção de Dado.

No campo da ilicitude o RGPD mostra ampla aplicabilidade tendo em vista que permite que qualquer pessoa possa propor ação civil em virtude da violação do regulamento, um resquício legal da Diretriz n.º 95/46/CE que não foi desperdiçado pela Comissão no esboço da propositura sendo positivada no artigo 82 º do RGPD. Embora numa leitura fria da lei possa parecer que somente as ilicitudes cometidas durante o tratamento de dados serão passiveis de responsabilização tal facto não prospera, vez que se compreende também atos delegados ou de execução segundo os termos do regulamento, assim não se finda os mecanismos de defesa, como leciona o Considerando 146[110].

Curiosamente, no regulamento não há nenhuma menção a dano isso ocorre, pois, a ceara do Direito da União ainda não desenvolveu tal conceito, com isso cabe ao Tribunal de Justiça (TJUE) e ao Direito interno de cada Estado-Membro. No entanto, é importante esclarecer que os tribunais de justiça dos Estados Membros devem seguir as balizas estabelecidas no Considerando 146[111] tanto para determinar o montante de danos materiais

[110] Considerando 146: O responsável pelo tratamento ou o subcontratante deverão reparar quaisquer danos de que alguém possa ser vítima em virtude de um tratamento que viole o presente regulamento responsável pelo tratamento. O responsável pelo tratamento ou o subcontratante pode ser exonerado da responsabilidade se provar que o facto que causou o dano não lhe é de modo algum imputável. O conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos do presente regulamento. Tal não prejudica os pedidos de indemnização por danos provocados pela violação de outras regras do direito da União ou dos Estados-Membros. Os tratamentos que violem o presente regulamento abrangem igualmente os que violem os atos delegados e de execução adotados nos termos do presente regulamento e o direito dos Estados-Membros que dê execução a regras do presente regulamento. Os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido. Sempre que os responsáveis pelo tratamento ou os subcontratantes estiverem envolvidos no mesmo tratamento, cada um deles deverá ser responsabilizado pela totalidade dos danos causados. Porém, se os processos forem associados a um mesmo processo judicial, em conformidade com o direito dos Estados-Membros, a indemnização poderá ser repartida em função da responsabilidade que caiba a cada responsável pelo tratamento ou subcontratante pelos danos causados em virtude do tratamento efetuado, na condição de ficar assegurada a indemnização integral e efetiva do titular dos dados pelos danos que tenha sofrido. Qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indemnização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento. UNIÃO EUROPEIA. Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados

[111] Ver ponto 102.

quanto o montante de danos imateriais, sendo esse último o que mais necessita da escorreita utilização destas balizas.

Além disso, quanto ao valor da indenização é de entendimento de decisões do TJUE que deve ser apropriado ao infortúnio sofrido compensando-o na sua integralidade.[112] Por fim, temos o nexo causalidade o qual fica evidente no artigo 82. º do RGPD ao ler-se "em virtude de" ou "devido a".

4.2 OS SUJEITOS

Compõem os sujeitos o lesado, o responsável pelo tratamento e o subcontratante. Como já foi explanado em tópico anterior o lesado pode ser qualquer pessoa. Embora haja certa discussão doutrinária sobre se o lesado deve ou não ser o titular de tais dados deixa-se claro que neste trabalho acompanha-se o pensamento de Menezes de Cordeiro acerca deste assunto ao defender que o espírito consagrado no "RGPD apontam no sentido da proteção de todos os direitos e liberdades fundamentais das pessoas singulares, sem exceção. Em caso de dívida (...) cabe aos tribunais assumir a solução que melhor acautele os direitos das pessoas singulares."[113]

Ainda nesta temática há aqueles que defendam que caberia fala em pessoa coletiva, contudo, por se tratar de uma norma recém aditada tanto no ordenamento jurídico europeu quanto no ordenamento jurídico de cada Estado Membro, sendo assim, peca-se pela prudência e aguarda-se como os tribunais nacionais e europeu irão elucidar esta matéria.[114]

Outros sujeitos elencados no regulamento são os responsáveis pelo tratamento de dados e os subcontratantes, entretanto, é válido recordar que isso não impede que o lesado

[112] TJUE 5-mar-1996, processo C-68/93 e C-48/93,90; e TJUE 2-ago-1993, processo C-271/91 (Marshall),26.

[113] CORDEIRO, 2020.p.390.

[114] Ibid. P. 390.

proponha ações maculação ao seu direito à autodeterminação informacional contra os demais com base em legislação europeia e nacional.[115]

Quanto e estes dois personagens Mafalda Miranda faz profícua explanação diferenciando-os. Para ela o *controller* é a pessoa responsável por controlar os dados e por este motivo é imputado a ela deveres especiais e responsabilidades caso ocorra descumprimento de alguns deles. Lembra também que segundo o artigo 29. º do RGPD o controle é derivado: de competência legal, competência técnica derivada de um contrato e de uma influência de facto. Traduz, portanto, a ideia de que o controle não seja meramente formal mais sim compatível com a realidade, ou seja, "*controller é uma noção dinâmica, que não se deixa aprisionar por determinações abstratas formuladas a priori*, antes procurando espelhar o efetivo controlo de facto sobre as finalidades e os meios de tratamento de dados."[116]

Já a figura do *processor* é o subcontratante aquele que opera o tratamento de dados em virtude do *controller*, contudo, as finalidades do tratamento não são determinadas, em regra, pelo *porcessor*, mas sim pelo *controller*. Destaca-se, pois, que nem mesmo a criação de uma nova finalidade isso se reverte. Caso confirme a nova finalidade o *processor* deverá ser compreendido "como um terceiro do mesmo modo que deve ser tido como terceiro se a finalidade eleita implicar uma violação dos direitos que estão na base da proteção de dados."[117]

---

[115] BARBOSA, A. M. C. N. de M. Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil. **Instituto de Direito Bancário, da Bolsa e dos Valores**, [*s. l.*], n. 3, REVISTA ONLINE BANCA, BOLSAESEGUROS, p. 147–214, 2018.
[116] Ibid. p. 164- 167.
[117] Ibid. P. 176.

4.3 A RESPONSABILIDADE DO EXTRACONTRATUAL

4.3.1 A responsabilidade do responsável pelo tratamento dos dados: controlo conjunto

A responsabilidade do encarregado pelo tratamento de dados é prevista no artigo 82. º/2 do regulamento geral de proteção de dados é deixa claro que ele é passível de ser responsabilizado caso comprove-se seu envolvimento numa fase de tratamento em que ouve violação ao disposto do RGPD, que está de pelo acordo com o disposto no artigo 497. º do Código Civil.

Porém dá forma como o regulamento foi montado não há exigência explicita que tal figura tenha um papel importante na produção do dano, deste modo caso ocorra transmissão lícita por ele de informações para terceiros processam-nas de forma ilícita podem ainda suscitar ainda a responsabilidade do responsável pelo tratamento.[118]

Trata-se, portanto, de caso de controlo conjunto como bem descreve Mafalda Miranda Barbosa, pois "não mais representa do que uma estrutura problemática que, pela partilha de finalidade e de meios, determina que haja apenas um tratamento para o qual convergem duas esferas de responsabilidade subjetivas. Se aquele tratamento envolve a preterição de dados pessoais, então, porque o controlo de finalidades e meios é comum e determina um só tratamento, tornam-se atuantes diversas esferas de risco/responsabilidade."[119].

4.3.2 A responsabilidade do subcontratante: controle paralelo

[118] CORDEIRO, 2020.
[119] BARBOSA, 2018.p. 177

A responsabilidade do subcontratante, uma inovação do RGPD só pode ser arguida em unicamente duas situações: quando as obrigações violadas estão efetivamente a cargo deles, e quando não cumprem as instruções lícitas que recebeu do responsável pelo tratamento de dados que delegou determinada função.[120]

Tecnicamente esta responsabilidade do subcontratante está positivada no artigo 28.º do RGPD, mas como bem recorda Menezes de Cordeiro ela não se exaure neste dispositivo, assim podendo ser encontrada nos artigos 29. º, 32. º, 37. º, 38.º do regulamento respetivamente.[121] Desta maneira, há uma responsabilidade direta subjetiva como bem defende Mafalda Miranda ao afirmar que "se se provar que violou a obrigação de apenas recorrer a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas, de modo que o tratamento satisfaçam os requisitos do regulamento geral de proteção de dados."[122]

Confirma-se, assim, a ideia de que a responsabilidade do quem controla os dados não afasta a responsabilidade daquele que processa os dados cabendo desta forma responsabilidade do comitente, uma modalidade de responsabilidade objetiva, positivada noa artigo 500. º do Código Civil.

4.4 A RESPONSABILIDADE CONTRATATUAL

Em linhas gerais, a responsabilidade contratual é aquela que deduz a existência contrato antecedente. Logo, evoca-se a responsabilidade em virtude de violação do tratamento de dados quando esse é objeto do contrato. Contudo, mesmo não o sendo há possibilidade de se avocar a aplicação da boa-fé que impõem deveres de cuidado que onerem responsabilidade civil quando maculados. Isso, pois, a relação contratual é vista como uma

[120] CORDEIRO, 2020. p.391-392
[121] Ibid. p. 392
[122] BARBOSA, 2018. p. 184

relação obrigacional complexa assimilada a responsabilidade contratual, como bem leciona Mafalda Miranda.[123]

Tal entendimento cabe perfeitamente a realidade do controlo sobre o tratamento de dados ser exercido por mais de um sujeito, contudo no caso de contratos que preveem o que chamam de controlo paralelo se aplicaria o artigo 800. ° do CC em que o devedor responde pelos atos lesivos dos terceiros que estão imbuídos em realizar suas obrigações.[124] Desse modo, projeta-se a atitude do auxiliar no devedor verificando se a responsabilidade compete a ele ou não.[125] Este fenómeno é descrito como teoria da ficção[126] ou responsabilidade civil por ato alheio[127].

Deste modo, é possível delinear dois cenários: no primeiro quando o devedor age com culpa *in elegendo*, *in instruendo* ou *in vigilando* deve ser responsabilizado fundado na culpa, sem ser preciso aplicar o disposto no artigo 800. º do CC, já no segundo mesmo atuando diligentemente o devedor é responsabilizado à custa de ato danoso do terceiro auxiliar, conforme leciona o artigo 800. º do CC. [128]

Embora reconheçam ambos contextos na doutrina portuguesa há certa divergência em como classificá-las. Sendo assim, parte dos autores portugueses pugnam que a falta de culpa doa auxiliar afastaria a responsabilidade do devedor, outros aquiescem que nos casos de culpa *in instruendo*, *in vigilando* e *in elegendo* não há necessidade de aferição de culpa,

---

[123] BARBOSA, A. M. C. N. de M. **Lições de responsabilidade civil**. 1ªed. Parede: Principia, 2017b. p. 19 e ss.

[124] BARBOSA, 2018.p. 185.

[125] CARNEIRO DA FRADA, M. A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana. *In*: DIREITO E JUSTIÇA. Lisboa: [*s. n.*], 1998. (Volumes Comemorativos dos 30 anos da Universidade Católica Portuguesa e dos 20 anos do seu Curso de Direito).v. II, p. 297–311.

[126] CAENEIRO DA FRADA, M. A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana. *In*: CONTRATO E DEVERES DE PROTECÇÃO, SEPARATA DO BOLETIM DA FACULDADE DE DIREITO DA UNIVERSIDADE DE COIMBRA. Coimbra/PT: [*s. n.*], 1994. p.301

[127] VARELA, A. **Das obrigações em geral**. 7ª (reimpressão)ed. Coimbra/PT: Almedina, 2001. v. II p. 103.

[128] BARBOSA, 2018. P. 187.

como defende Carneiro da Fraga ao deixar entender que se deve ponderar o que entende por intencionalidade normativa do preceito.[129]

Nos ensina Vaz Serra que o devedor deve responder pelos atos de todos aqueles que estão sob a sua tutela ou que estão a contribuir de certa forma no cumprimento das obrigações.[130] Com isso, evita-se que o devedor encontre uma maneira simplória de suprimir a sua responsabilidade ao chamar outro para realizar a prestação o que poderia incorrer em abusos patentes.[131] Dessa maneria, o facto do devedor utilizar auxiliar para realizar cumprimento de uma obrigação não o exonera dos possíveis danos.[132]

Como bem disserta Mafalda Miranda diante de dificuldades prática de imputação o artigo 800. º do CC nos leva a solução simplista, pois a responsabilidade passa a ser balizar a imputação, *a priori*, pelos deveres que precedem a relação o obrigacional.[133] Com isso, o problema persiste e cresce com a violação dos acessório e dos deveres de conduta e não necessariamente com a atendado aos deveres de prestação.[134]

Em virtude disso, cabe igual entendimento ao elemento culpa, portanto, "se a responsabilidade do terceiro auxiliar é tida como responsabilidade do próprio devedor, então deve entender-se que, uma vez excluída a culpa do primeiro, se exclui concomitantemente a responsabilidade do segundo."[135]

Assim, somente no campo da obrigação previamente assumida pelo devedor que ira balizar o alcance da responsabilidade dele via aplicação do artigo 800. º do CC em virtude de obrigação no sentido técnico. Portanto, evoca-se a responsabilidade contratual com a finalidade de alcançar a responsabilidade do *controller* pelos atos do subcontratante. Nesse

---

[129] CARNEIRO DA FRADA, 1998.p. 303.

[130] VAZ SERRA, A. Responsabilidade do devedor pelos actos dos auxiliares, dos representantes legais ou dos substitutos. **Boletin n. º72**, [*s. l.*], n. 2, [*s. d.*]. p. 273.

[131] PAULO MOTA PINTO. **A. Pinto monteiro, Cláusulas limitativas e de exclusão da responsabilidade**. Coimbra/PT: Almedina, 2003. P. 284 e ss.

[132] Ibid. p. 287 e ss.

[133] BARBOSA, 2018.p.194

[134] Ibid. P. 194

[135] Ibid. P. 196

caso, o contrato em que figuram responsável pelo tratamento dos dados e o subcontratante será co eficácia de proteção para com terceiros. [136]

Quanto a isto Mota Pinto faz ressalva quanto a quem podem ser esses terceiros e afirma que devem ser pessoas que, segundo sua natureza, sejam próximas ao credor e que, por isso, transmitam confiança ao devedor.[137]

5 A RESPONSABILIDADE CIVL E A PROPOSTA DE REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL DO PARLAMENTO EUROPEU

5.1 COMO A RESPONSABILIDADE CIVIL É DELINEADA NA PROPOSTA DE HARMONIZAÇÃO DE INTELIGÊNCIA ARTIFICIAL

É oportuno observar que não há na proposta de regulamento que estabelece regras harmonizadas em matéria de inteligência artificial secção específica para tratar da responsabilidade civil, pois como bem explicou o legislador europeu não há necessidade de uma revisão completa dos regimes de responsabilidade civil nos Estados Membros, mas somente demanda por ajustes para que aquele que sofra com algum infortúnio patrimonial receba a devida indenização. Ademais, subscreve que toda atividade realizada por aplicativo físico (robôs) ou virtual que operem via uso de IA podem, do ponto de vista técnico, até serem o motivo direto ou indireto de certo malefício, todavia sempre serão fruto da interação de um indivíduo (pessoa) que o utiliza, o construiu ou interfere no sistema.[138]

Além disso, no texto “Regime de responsabilidade civil aplicável à inteligência artificial” o legislador argumenta não ser necessário conferir personalidade jurídica sistema

---

[136] Ibid. P. 197-198.

[137] PINTO, C. A. da M. **Cessão da posição contratual**. Reimpred. Coimbra: Livraria Almedina, 2003. (Colecção teses).p.423.

[138] PARLAMENTO EUROPEU. **Regime de responsabilidade civil aplicável à inteligência artificial**. 20 out. 2020.

de IA alegando ser difícil ou até mesmo impossível determinar se o dano foi ocasionado por ação exclusiva do ente dotado de IA ou houve interferência humana, assim, justificando que tais obstruções interpretativas podem ser contornadas com as soluções já existente na ceara da responsabilidade civil.[139]

Sendo assim, a título de recorde analítico utilizar-se-á com objeto de analise os robôs e veículos autónomos que possuam sistemas de IA de identificação biométrica, que nada mais é do que o reconhecimento facial, que foi objeto meticuloso exame no capítulo I deste trabalho académico.

Após explanar as ideias do legislador passa-se para a efetiva investigação da responsabilidade civil versus proposta de regulamentação da inteligência artificial, na qual não será descartada a possibilidade de apuração da viabilização da personalidade jurídica de sistemas dotados de inteligência artificial.

5.2 OS POSSÍVEIS DESDOBRAMENTOS EM MATÉRIA DE RESPONSABILIDADE CIVIL

5.2.1 A centralidade da culpa nos modelos de responsabilidade civil

Extrai-se da literatura clássica do Direito português que a centralidade da culpa nos modelos de responsabilidade civil vem do facto de que a pura imputabilidade do agente não basta para a sua responsabilização, assim, reconhece-se a necessidade de que o imputável tenha agido culposamente. Com magistralmente aponta Antunes Varela "a culpa exprime um juízo de reprobabilidade pessoal da conduta do agente: o lesante, em face das circunstâncias específicas do caso, devia e podia ter agido de outro modo."[140], ou seja, é um juízo de censura que estabelece conexão entre o facto e a vontade do autor.

---

[139] Ibid.

[140] VARELA, A. **Das obrigações em geral**. 10.ª ed. rev. e actualiz.:15ªed. Coimbra: Almedina, 2018. v. I p.566.

Entretanto, ao confrontar esta linha argumentativa com possíveis factos danosos envolvendo ente autônomos indaga-se como auferir culpa a um robô ou a um androide dotado de inteligência artificial, entes, em tese, despersonalizado. Especificamente, robôs com que por meio da inteligência artificial sejam capazes de ler faces de seres humanos identificando os indivíduos na sua passagem exploratória e, consequentemente, recolhendo dados biométricos deles.

Com escopo de elucidar tal indagação recorresse em primeiro as estruturas clássicas da responsabilidade civil, entretanto, desde logo percebe-se que elas não são adequadas haja vista que a independência de aprendizado de máquina dificulta traçar a fronteira entre o puramente erro humana de programação prévia, uma vez que essa autonomia é derivada do *machine learnning*[141] que tem escopo de proporcionar a esse ente a capacidade de decidir quando e como agir tornando, desta maneira, seu comportamento imprevisível.

Por conseguinte, o cenário quanto a apuração da culpa parece desolador, contudo, realizando um exame no Código Civil Português, Decreto Lei n.º 47344/66, de 25 de novembro, pode-se aventar a utilização do disposto no artigo 493.º[142], dessa maneira, surge

[141]Aprendizado de Máquina é uma área de IA cujo objetivo é o desenvolvimento de técnicas computacionais sobre o aprendizado bem como a construção de sistemas capazes de adquirir conhecimento de forma automática. Um sistema de aprendizado é um programa de computador que toma decisões baseado em experiências acumuladas através da solução bem sucedida de problemas anteriores. BARANAUSKAS, J. A.; MONARD, M. C. Capítulo 4 - Conceitos sobre Aprendizado de Máquina. *In*: SISTEMAS INTELIGENTES-FUNDAMENTOS E APLICAÇÕES. 1ªed. Barueri/SP: Manoele Ltda, 2003. p. 89–114. *E-book*.

[142] Artigo 493.º

(Danos causados por coisas, animais ou actividades)

1. Quem tiver em seu poder coisa móvel ou imóvel, com o dever de a vigiar, e bem assim quem tiver assumido o encargo da vigilância de quaisquer animais, responde pelos danos que a coisa ou os animais causarem, salvo se provar que nenhuma culpa houve da sua parte ou que os danos se teriam igualmente produzido ainda que não houvesse culpa sua.

2. Quem causar danos a outrem no exercício de uma actividade, perigosa por sua própria natureza ou pela natureza dos meios utilizados, é obrigado a repará-los, excepto se mostrar que empregou todas as providências exigidas pelas circunstâncias com o fim de os prevenir. PORTUGAL. **Código Civil - Decreto Lei n.º47344/66, 25 de novembro**. **Código Civil**, 25 nov. 1966. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=775&tabela=leis. Acesso em: 13 jul. 2020.

a possibilidade de responsabilizar o detentor da coisa móvel - robô com reconhecimento facial como o Sanbot[143] - pelos danos que ela causou.

Para mais, é imperioso esclarecer que a conjetura delineada no número 2 do artigo 493.º do Código Civil português também poderá ser aplicado aos casos relacionados a peculiaridade da atividade comportamental dos robôs equipados com reconhecimento facial que fazem vigilância, a exemplo do robô da Spot da Boston Dynamics[144][145], visto que quem causar danos a outrem no exercício de uma atividade perigosa pela sua própria natureza ou pelos meios utilizados é obrigado a ressarcir a vítima do evento danoso.

Por está logica, aquele que tiver em seu poder o robô nos moldes do Spot poderá ser responsabilizado por potenciais danos causados, a terceiros, vez que se trata neste caso de tanto de atividade perigosa (vigilância de propriedade particular) tanto pelos meios utilizados (robô equipado com inteligência artificial de reconhecimento facial), assim, a depender do caso em concreto é possível a aplicação do artigo 493. º/2 do CC.

---

[143] Sanbot é um robô de serviço inteligente (humanóide) desenvolvido pela QIHAN Technology, uma empresa focada em inovações em robótica, inteligência artificial e análise de vídeo. Resultante de anos de pesquisa e desenvolvimento, a nova plataforma Sanbot irá liberar o poder da robótica habilitada para nuvem e IA para varejo, hospitalidade, saúde, educação, segurança e muitos outros setores orientados ao cliente para fornecer serviços mais inteligentes e personalizados.

Como um catalisador em inovações de serviço e produtividade de negócios, a Sanbot está levando a tecnologia de robótica para o mainstream. Com uma API aberta que permite que os desenvolvedores criem aplicativos Android que aproveitem os poderosos recursos de IA e aprendizado de máquina do Sanbot, as empresas oferecerão serviços mais ricos, inteligentes e interativos que aumentam a satisfação e a fidelidade do cliente.

Sanbot é o resultado da profunda colaboração da QIHAN com parceiros de tecnologia, apresentando soluções líderes de classe, incluindo baterias recarregáveis da Panasonic e sensores de imagem da Sony. Os recursos da QIHAN em robótica habilitada para nuvem e IA são construídos a partir de anos de pesquisa e colaboração com instituições, incluindo o Instituto de Tecnologia Harbin e a Universidade de Geociências da China. SANBOT THE ROBOT. [*S. l.*], [*s. d.*]. Disponível em: https://www.sanbot.co.uk. Acesso em: 28 out. 2021.

[144] Robot Spot da Boston Dynamics está ligado à rede privada europeia 5G SA e está responsável por complementar as tarefas de vigilância física do campus da Universidade de Vigo, em Espanha. (...) O robot pode ser equipado com inteligência artificial para tarefas de reconhecimento facial. SECURITYMAGAZINE. Robot ligado a rede privada 5G faz vigilância física na Universidade de Vigo. *In*: SECURITY MAGAZINE. 22 out. 2021. Disponível em: https://www.securitymagazine.pt/2021/10/22/robot-ligado-a-rede-privada-5g-faz-vigilancia-fisica-na-universidade-de-vigo/. Acesso em: 30 out. 2021.

[145] Nota explicativa: embora o robô Spot no recorde de reportagem trago a baila esteja sendo utilizado na segurança de uma instituição pública - Universidade de Vigo na Espanha - nada impede outros robôs da Boston Dynamics ou similares sejam utilizados no patrulhamento e segurança de propriedades particulares. Portanto, justifica-se a analise proposta, uma vez que a vigilância é uma atividade perigosa por sua própria natureza.

Sem embargo, é crível ressaltar que quando aquele que está na qualidade de vigilante provar que não ouve por sua parte violação do dever de cuidado ou culpa a julgar por comprovadamente ter tomado todas as precauções esperadas afasta-se, automaticamente, a aplicação do artigo 493. º do Código Civil.

5.2.2 Responsabilidade objetiva ou responsabilidade pelo risco

É de notório saber que a teoria clássica da responsabilidade baseada na culpa é revestida de caráter pedagógico e está presente no Código Civil como regra geral. Contudo, transpondo os fundamentos jurídicos a realidade provou-se que a teoria da culpa nem sempre proporcionou as soluções mais plausíveis, visto a incompatibilidade desta não comportar a ideia de que, por vezes, certos factos ilícitos não são comprováveis por imputação de culpa ao possível autor como, por exemplo, nos casos de caso fortuito ou de força maior.

Em vista disso, cria-se entre os operadores do direito a necessidade de moderar os pilares do pensamento clássico para melhor adequar a realidade jurídica presente no ordenamento ao plano de certas situações fáticas, assim, casuisticamente a culpa passa a ser intrínseca, em outras palavras, a lei passou a prever que em determinados comportamentos a aplicação da responsabilidade objetiva na qual não há necessidade de provar a culpa do agente devido ao risco envolvido, como ficou lecionado no artigo 483.º, n.º 2 do CC [146]

Como isso, cria-se no sistema jurídico civil português a tônica de que em certos casos o lesante será responsabilizado independentemente de averiguação culpa quando verificada a periculosidade da atividade e os proveitos obtidos com sua execução, quando há tutela especial de determinado bem jurídico ou há amparo aquele que sofreu o dano e que se

[146] Artigo 483.º
(Princípio geral)
1. Aquele que, com dolo ou mera culpa, violar ilicitamente o direito de outrem ou qualquer disposição legal destinada a proteger interesses alheios fica obrigado a indemnizar o lesado pelos danos resultantes da violação.
2. Só existe obrigação de indemnizar independentemente de culpa nos casos especificados na lei. (grifo nosso) *PORTUGAL, 1966.*

encontra em posição desfavorecida encontrando obstáculos para trazer a baila processual provas robustas da responsabilidade do autor do dano[147].

Nesse diapasão o legislador optou pela aplicação da responsabilidade objetiva aos danos causados por acidentes envolvendo veículos terrestres como dispõem o artigo 503.º[148] do Código Civil, uma vez que incidentes de viação aumentaram gradativamente com a acentuação do tráfego de veículos nas vias.

Curiosamente, quando se dedica a realização de uma análise meticulosa ao dispositivo destinado ao tema (artigo 503.º) descobre-se que o legislador português foge de uma linha de pensamento mais conservadora na qual limitaria a responsabilização ao dono veículo. Desta forma, assume-se certo vanguardismo ao englobar na esfera de responsabilização aquele que estiver na efetiva direção do carro ou estiver a utilizar o veículo para atender a seus interesses.

Nesse quesito é crível extrair o entendimento de que tal dispositivo tem por escopo abranger na esfera de responsabilidade o proprietário, o locatário, o usufrutuário, o comodatário, o adquirente e até mesmo o aquele que furtou o veículo, visto que se atribui a estes indivíduos o dever de cuidado para com toda e qualquer precaução essencial para a condução do carro sem causas danos, como anota precisamente Antunes Varela[149]. À vista disso, se firma o entendimento de que a responsabilidade será auferida ao detentor da direção concreta do veículo.

---

[147] BARBOSA, A. M. C. N. de M. **Estudos a propósito da responsabilidade objetiva**. 1ªed. Cascais: Principia, 2014. , p. 44-45.

[148] Artigo 503.º

(Acidentes causados por veículos)

1. Aquele que tiver a direcção efectiva de qualquer veículo de circulação terrestre e o utilizar no seu próprio interesse, ainda que por intermédio de comissário, responde pelos danos provenientes dos riscos próprios do veículo, mesmo que este não se encontre em circulação.

2. As pessoas não imputáveis respondem nos termos do artigo 489.º

3. Aquele que conduzir o veículo por conta de outrem responde pelos danos que causar, salvo se provar que não houve culpa da sua parte; se, porém, o conduzir fora do exercício das suas funções de comissário, responde nos termos do n.º 1. PORTUGAL, 1966.

[149] VARELA, 2018. p. 656-658.

Todavia, diante de um acidente envolvendo um veículo totalmente autônomo como o Naru [150] pondera-se se é plausível aplicar as regras do artigo 503.º do CC com a finalidade de dar solução ao caso concreto.

E, embora anote Manuel Felício[151] que os ditos medos advindos da utilização da inovadora condução automatizada são iguais aos enfrentados pela introdução do veículo a motor nos primórdios, não vislumbra-se, *a priori*, solução com o emprego de referido dispositivo, uma vez que há muita variáveis que permeiam esta situação com saber de quem é "a direção efetiva do veículo é o *poder real (de facto) sobre o veículo*, mas não equivale à ideia grosseira de ter o volante nas mãos na altura em que o acidente ocorre."[152]

5.2.3 A responsabilidade do produtor

Neste ponto será abordada a responsabilidade do produtor, sem embargo com o intuito de tornar o estudo mais lógico e, por conseguinte, facilitado adota-se por produtor aquele que fabrica produto com reconhecimento facial e desenvolve *software* com sistema operacional via inteligência artificial. Tal feito tem por fim adequar-se as exemplificações explanadas no capítulo um e por entender que no mercado atual aqueles que ofertam a venda

---

[150] Nota explicativa: naru é um veículo totalmente autónomo de entrega que utiliza do reconhecimento facial para identificar o destinatário. SEM NEM SAIR DE CASA? STARTUP REVELA VEÍCULO AUTÔNOMO DE ENTREGAS [VÍDEO]. [*S. l.*], [*s. d.*]. Disponível em: https://www.tecmundo.com.br/mobilidade-urbana-smart-cities/126684-sair-casa-startup-revela-veiculo-autonomo-entregas-video.htm. Acesso em: 30 out. 2021.

[151] "[...] os receios suscitados com o advento dos sistemas de condução automatizada são comparáveis aos riscos e perigos idealizados pela comunidade aquando da introdução dos veículos a motor mais primitivos no meio rodoviário. Assistir-se-á, portanto ao alargamento de um conceito – o de riscos próprios do veículo – que por si só já é difícil de definir com precisão. Aos riscos do veículo, somam-se os riscos do software, subtraindo-se os riscos do condutor." FELÍCIO, M. Responsabilidade civil por acidente de viação causado por veículo automatizado. **Revista de Direito da Responsabilidade**, [*s. l.*], n. ano 1, p. 32, 2019. Disponível em: https://revistadireitoresponsabilidade.pt/2019/responsabilidade-civil-por-acidente-de-viacao-causado-por-veiculo-automatizado-manuel-felicio/ p.517.

[152] VARELA, 2018. p. 657.

de produtos como estes realizam ambos os papeis. Feita as devidas ressalvas passa-se a leitura do dispositivo legal.

Segundo consta a norma designada para tratar da responsabilidade decorrente de produtos defeituosos, Decreto Lei n.º 383/89[153], de 6 de novembro, proveniente da transcrição Diretiva n.º 85/374/CEE para o ordenamento jurídico pátrio, produto é "qualquer coisa móvel, ainda que incorporada noutra coisa móvel ou imóvel"[154] já produtor "é o fabricante do produto acabado, de uma parte componente ou de matéria-prima, e ainda quem se apresente como tal pela aposição no produto do seu nome, marca ou outro sinal distintivo."[155]

No nicho da inteligência artificial dedicado ao desenvolvimento de tecnologia de reconhecimento facial é imperioso esclarecer que é o *software*[156] instalado no sistema operacional que concede ao ente autônomo, como o robô da Sandot[157], a capacidade

---

[153] PORTUGAL. **Decreto Lei n.º383/89, de 06 de novembro**. Transpõe para a ordem jurídica interna a Directiva n.º 85/374/CEE, em matéria de responsabilidade decorrente de produtos defeituosos. 6 nov. 1989. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=729&tabela=leis&so_miolo=. Acesso em: 22 jul. 2020.

[154] Artigo 3.º
Produto
1 - Entende-se por produto qualquer coisa móvel, ainda que incorporada noutra coisa móvel ou imóvel.
2 – Revogado pelo DL n.º 131/2001, de 24 de Abril. *Ibid*.

[155] Artigo 2.º
Produtor
1 - Produtor é o fabricante do produto acabado, de uma parte componente ou de matéria-prima, e ainda quem se apresente como tal pela aposição no produto do seu nome, marca ou outro sinal distintivo.
2 - Considera-se também produtor:
a) Aquele que, na Comunidade Económica Europeia e no exercício da sua actividade comercial, importe do exterior da mesma produtos para venda, aluguer, locação financeira ou outra qualquer forma de distribuição;
b) Qualquer fornecedor de produto cujo produtor comunitário ou importador não esteja identificado, salvo se, notificado por escrito, comunicar ao lesado no prazo de três meses, igualmente por escrito, a identidade de um ou outro, ou a de algum fornecedor precedente. *Ibid*.

[156] [...] hardware (componente física do computador) e software (conjunto de instruções para a máquina" PINTO, I. F. T. **Patentes e Programas de Computador**. 118 f. 2016. Dissertação de Mestrado - Universidade do Minho. Escola de Direito, Braga-PT, 2016. p. 6.

reconhecer a os pontos nodais da face de um individuo por meio do aprendizado de máquina (*machine learning*[158]). Posto isto, ao tentar aplicar o disposto no artigo 3.º do Decreto-Lei n.º 383/89 ao caso em concreto depara-se com o seguinte paradoxo: o *software* deve ser classificado como bem incorpóreo ou bem imaterial[159]. Diante de tal incongruência resta considerar que o *software* não pode e não dever ser enquadrado exclusivamente como um produto, sendo assim passível de se encaixar na categoria de serviços a depender das circunstâncias fáticas com alinhava Calvão da Silva em sua tese de doutoramento intitulada *Responsabilidade civil do produtor*[160].

Todavia, embora não seja pensamento majoritário na doutrina que se dedica ao crivo dos temas que permeiam a ceara jurídica do Direito do Consumidor na literatura jurídico portuguesa é respeitável recordar as reflexões de Silva Conçalves[161] ao afirmar que um software consubstanciado e certo suporte material (exemplificando um *pen drive* ou *CD-ROM*) deve ser encarado como um produto. No mesmo diapasão deve ser adotado o entendido para com o software vendido *on-line*[162], uma vez que em decorrência dos riscos inerentes ao comércio de *software* se faz imprescindível buscar a responsabilização objetiva do produtor.

Doravante as lucubrações até o momento esplanadas, reside ainda no âmbito da responsabilidade do produtor certa dificuldade probatória em atestar a existência de determinado defeito, pois a ideia de defeito está atrelada a expectativa de seguridade que certo produto oferece aquele que o consome. Concomitantemente, atrelado a esta linha de raciocínio o defeito para ser confirmado tem de ser verificado no momento da colocação do

---

[158] Ver nota de rodapé 141.

[159] Ver nota de rodapé 139.

[160] CALVÃO DA SILVA, J. **Responsabilidade civil do produtor**. Coimbra: Almedina, 1990. (Colecção teses).

[161] GONÇALVES, I. A. de A. e S. **Software, proteção, consumidor**. 83 f. 2012. Dissertação de Mestrado - Universidade de Coimbra, Coimbra/PT, 2012. p. 73.

[162] SILVA, J. C. da. **Compra e venda de coisas defeituosas: (conformidade e segurança)**. 5ªed. Coimbra: Almedina, 2008. (Monografias). p. 185.

produto no mercado, tendo em conta que o produtor não é responsável pelo risco do desenvolvimento, como extrai-se da leitura do artigo 4.º[163] do Decreto-Lei nº. 383/89.

E diante deste cenário torna-se difícil encaixar a realidade dos entes autônomos que se utilizam de sistemas reconhecimento facial a propositura dos ditames legais vigentes, pois há cenários em que os dados previamente programados no s*oftware* podem ser alterados quando ocorrer uma atualização mau sucedida, quando inserem informações biométricas incorretas ou ocorre comprometimento pelo mau funcionamento a tecnologia de *machine learning* ao interagir com o ambiente que o circunda e interagem.

Assim, vislumbra-se um possível enquadramento legal, vez que será considerada a falha sistémica ou operacional quando num robô equipado com sistema de reconhecimento facial quando ela for averiguada no momento da colocação dele no mercado. Com isso, exclusivamente poderá ser admitida a responsabilidade do produtor quando o defeito no sistema de reconhecimento facial foi detetado quando este é alocado no mercado de consumo.

Encerrando as reflexões acerca do tópico em análise resta esmiuçar as possíveis indenizações previstas na norma em comento. Dito isso, recorre-se ao artigo 8.º[164] do Decreto-Lei n.º 383/89, o qual determina quais são os tipos de danos indenizáveis. Portanto, são reparáveis: (1) os danos advindos da morte; (2) os danos qua culminaram em lesão pessoal; (3) e os danos em coisa diversa do produto defeituoso desde que seja normalmente destinado ao uso ou ao consumo privado e o lesado o tenha concedido esta destinação.

---

[163] Artigo 4.º
Defeito
1 - Um produto é defeituoso quando não oferece a segurança com que legitimamente se pode contar, tendo em atenção todas as circunstâncias, designadamente a sua apresentação, a utilização que dele razoavelmente possa ser feita e o momento da sua entrada em circulação.
2 - Não se considera defeituoso um produto pelo simples facto de posteriormente ser posto em circulação outro mais aperfeiçoado. PORTUGAL, 1989.

[164] Artigo 8.º
Danos ressarcíveis
São ressarcíveis os danos resultantes de morte ou lesão pessoal e os danos em coisa diversa do produto defeituoso, desde que seja normalmente destinada ao uso ou consumo privado e o lesado lhe tenha dado principalmente este destino. *Ibid*.

5.2.4 A responsabilidade do comitente

A comissão está elencada no artigo 500.º do Código Civil e percebe-se que o legislador optou por estabelecer que "aquele que encarrega outrem de qualquer comissão responde, independentemente de culpa, pelos danos que o comissário causar, desde que sobre este recaia também a obrigação de indemnizar", além de determinar no n.º 2 que "a responsabilidade do comitente só existe se o facto danoso for praticado pelo comissário, ainda que intencionalmente ou contra as instruções daquele, no exercício da função que lhe foi confiada."[165]

Como deslinda por Lino Diamvutu[166] a comissão, da forma como foi elaborada, assume sentido amplo englobando todo e qualquer serviço ou atividade executado por conta ou sob ordem de outrem.

Tendo por base que a relação de dependência entre comitente e comissário muito se assemelha a dinâmica "do motorista perante o dono do veículo."[167] Afirma Manuel Felício[168] que poderia este artigo servir de croqui para um eventual enquadramento normativo.

---

[165] Artigo 500.º
(Responsabilidade do comitente)
1. Aquele que encarrega outrem de qualquer comissão responde, independentemente de culpa, pelos danos que o comissário causar, desde que sobre este recaia também a obrigação de indemnizar.
2. A responsabilidade do comitente só existe se o facto danoso for praticado pelo comissário, ainda que intencionalmente ou contra as instruções daquele, no exercício da função que lhe foi confiada.
3. O comitente que satisfizer a indemnização tem o direito de exigir do comissário o reembolso de tudo quanto haja pago, excepto se houver também culpa da sua parte; neste caso será aplicável o disposto no n.º 2 do artigo 497.º PORTUGAL, 1966.

[166] "A comissão tem aqui o sentido amplo de serviço ou actividade realizada por conta e sob a direcção de outrem, podendo essa actividade traduzir-se tanto num acto isolado como numa função duradoura, ter carácter gratuito ou oneroso, manual ou intelectual." DIAMVUTU, L. Para uma melhor compreenção do aseguro obrigatório de responsabilidade civil automóvel: a questão do ressarcimento de danos resultantes de lesões corporais e materiais nos acidentes de viação. **Faculdade de Direito da Universidade de Lisboa**, [*s. l.*], [*s. d.*]. Disponível em: http://www.fd.ulisboa.pt/wp-content/uploads/2014/12/Damvutu-Lino-PARA-UMA-MELHOR-COMPREENSAO-DO-SEGURO-OBRIGATORIO-DE-RESPONSABILIDADE-CIVIL-AUTOMOVELi.pdf p. 5.

[167] LIMA, F. A. P. de; VARELA, J. de M. A. (org.). **Código civil anotado. Vol. 1: Artigos 1.º a 761.º**. 4. ed. rev. e atualizada. Reimpressãoed. Coimbra: Coimbra Ed, 2011. v. I p. 507-508

[168] FELÍCIO, 2019.

Entretanto, ao recordar que no próprio artigo 500.º prevê hipótese de culpa presumida do comissário, ou seja, sem que haja necessidade de qualquer juízo de responsabilidade, exigindo dele obrigação de indenização tal qual o comitente depara-se com ao cenário indefinido dos veículos autônomos de entrega que usam do reconhecimento facial para efetuar confirmação do destinatário final – a exemplo o Naru[169] - que, na atual conjuntura, não comportam personalidade jurídica, logo, são desprovidos da capacidade de agir por seus próprios termos e ,consequentemente, responderem pelos seus atos segundo os juízos éticos-normativos presentes do ordenamento jurídico contemporâneo.

5.2.5 A responsabilidade contratual

Sobre esta temática atesta Nuno Sousa e Silva que caso o objeto do contrato de compra e venda seja coisa guarnecida de inteligência artificial e está se mostrar defeituosa poder-se-á a disciplina que trata da compra e venda de coisas defeituosas, para mais entende o doutrinador que a mesma linha de raciocínio deve ser aplicada aos contratos de locação de produto e de empreitada quando são evidentemente defeituosos.[170]

Todavia, estas não são as únicas indagações suscitadas, visto que ainda na ceara da responsabilidade subjetiva provoca dúvida quando requer-se ponderar uma resposta quando estar-se-á diante de evento em que o cumprimento de uma obrigação se deu por meio da utilização de um robô, veículo autônomo ou qualquer ente dotado de inteligência artificial. Sobre este assunto alerta Mafalda Miranda Barbosa ao engendrar-se pela busca de uma resposta pode-se

> "[...] conseguir ilidir a presunção de culpa constante do artigo 799º CC, não se colocando, sequer, o problema de uma eventual responsabilidade por via do artigo

[169] SEM NEM SAIR DE CASA?, [*s. d.*].

[170] SILVA, N. S. e. Inteligência Artificial, Robots e Responsabilidade Civil: o que é que é diferente? **Revista de Direito Civil**, [*s. l.*], v. IV (2019), n. 4º, p. 691–711, 2019. Disponível em: https://doi.org/691-711 p. 702

> 800º CC, já que o mesmo pressupõe também a subjetivação do terceiro de que se lance mão para o cumprimento de uma obrigação."[171]

Segue o mesmo pensamento Nuno Sousa e Silva ao ponderar que a responsabilidade daqueles que utilizam tais entes para execução de uma obrigação "poderá existir culpa na conceção, escolha ou utilização do robot. No entanto, se não há culpa do ser humano que concebeu, escolheu ou utiliza o *robot*, mas este causou danos, então teremos de ponderar a responsabilidade objetiva por facto de terceiro."[172]

6 POSSÍVEIS REMÉDIOS

Após a digressão realizada dedica-se este tópico a apuração das possíveis soluções aventadas pelos estudiosos que se debruçaram sobre livros e normas com o intuito de provir remédios aos questionamentos levantados, vez que o futuro que se avizinha mostra uma sociedade profundamente integrada a convivência com estes agentes dotados de inteligência artificial voltada para o reconhecimento facial.

6.1 A PERSONIFICAÇÃO DOS ENTES AUTÔNOMOS

No ambiente forense, aqueles que se dedicam a estudar as relações jurídicas entre homem e máquina deparam-se com interrogação: devem os entes autônomos serem considerados como ferramentas ou serem enquadrados de alguma forma de ser ou dotado de capacidade volitiva. Nessa conjuntura, surge duas correntes doutrinárias: uma que enquadra tais agentes como *e-persons* e outra os reconhecem como *e-servents.*

---

[171] BARBOSA, A. M. C. N. de M. O Futuro da Responsabilidade Civil desafiada pela inteligência artificial: modelos tradicionais e caminhos de solução. **Revista de Direito da Responsabilidade**, [*s. l.*], n. ano 2, p. 47, 2020. Disponível em: https://revistadireitoresponsabilidade.pt/2020/o-futuro-da-responsabilidade-civil-desafiada-pela-inteligencia-artificial-as-dificuldades-dos-modelos-tradicionais-e-caminhos-de-solucao-mafalda-miranda-barbosa/ p. 291.

[172] SILVA, 2019., p. 703.

Aqueles que saem na defesa dos entes autónomos como *e-persons* associam-se a linha argumentativa de pensamento que concede personalidade jurídica a entes não humanos e justificam utilização desta com base na complexidade de tais agentes, assim, capazes de responder por toda e qualquer consequência jurídica proveniente de seus atos, assim, criando mais uma fonte de responsabilidade extracontratual com base na conduta de terceiro.[173]

Nesse sentido, a mencionada linha de pensamento abrandaria as discussões que cercam possíveis danos causados por entes autônomos de todas as sortes (veículos ou robôs) que em virtude do seu auto grau de inteligência artificial possui independência total. Deste modo, aquele que é dono ou está na posse deste ente seria totalmente excluído da averiguação do juízo de responsabilidade.

Entretanto, apresentam-se outros problemas como saber se seria cabível o direito de propriedade do homem sobre um *e-person*. Para além disso, também se descarta a possível catalogar os entes autônomos na figura de ente coletivo, haja vista necessidade de esse precisar, na sua constituição, da presença de pessoas físicas que legitime sua existência. Sobre este mote Mafalda Miranda Barbosa aponta que falta aos entes autônomos uma relação de cuidado para com o próximo e assentada na "pressuposição ética"[174] tão característica do ser humano.

Noutro diapasão, propõem Pagollo[175] a solução denominada *e-servant*, na qual a responsabilização do agente imbuído de inteligência artificial seria via contrato extensível,

---

[173] "[...] reconhecimento de *robots* enquanto seres dotados de personalidade jurídica, ou *e-persons* – com todas a consequências éticas, jurídicas, sociais e ontológicas que acarretaria – é pensada, acima de tudo, como um meio para evitar problemas como a litigiosidade decorrente do acidente ou a previsão de mais uma fonte de responsabilidade extra-contratual com base no comportamento de outrem – como é o caso de animais ou de mandatários." FELÍCIO, 2019. p. 500.

[174] BARBOSA, A. M. C. N. de M. Inteligência artificial, e-persons e Direito: desafios e perspectivas. **Revista Jurídica Luso-Brasileira (RJLB)**, [*s. l.*], v. 3, n. 6, p. 30, 2017a. Disponível em: https://blook.pt/publications/publication/6d03901f9052/ p. 1482.

[175] PAGALLO, U. Apples, oranges, robots: four misunderstandings in today's debate on the legal status of AI systems. **Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences**, [*s. l.*], v. 376, n. 2133, p. 16, 2018. Disponível em: https://doi.org/10.1098/rsta.2018.0168. Acesso em: 22 jul. 2020.

até mesmo, a responsabilização extracontratual segundo apuração do caso em concreto. Mas, afinal, o que é um *e-servant*?

Pagollo[176] cria a alegoria *e-servant* ao traçar comparações entre o papel desempenhado por estes entes autônomos – robôs, *selfdrive cars*, entre outros - a condição de escravo na Roma Antiga. Com isso, tal qual como os escravos de Roma o *e-servant* é objeto de direito de propriedade munido de inteligência, consciência e capacidade volitiva.

Assim, tal qual o proprietário de um escravo o dono do *e-servant* deve criar um patrimônio independente destinado exclusivamente a indenizar prováveis vítimas de determinado evento danoso causado pela capacidade volitiva deste agente. Embora soe como uma promissora resposta, tendo em vista a isenção de responsabilização do proprietário ainda reside falha ao perceber-se que o valor do alcance da pretensão indenizável será limitado ao máximo do pecúlio reservado com este escopo, o que eventualmente poderá se mostrar insuficiente para o alcance de uma indenização correspondente ao dano.

6.2 FUNDOS DE COMPENSAÇÃO E O SISTEMA DE SEGUROS OBRIGATÓRIOS

A atividade seguradora basicamente consiste em prestação de um serviço de cobertura de risco por parte do segurador mediante troca de prémio pelo segurado.[177] À vista disso, destaca-se que a finalidade do contrato de seguro é proporcionar segurança econômica aos segurados, uma vez que ficarão "cobertos" não tendo seus patrimônios afetados caso algum evento danoso ocorra.[178]

---

[176] *Ibid*.

[177] OLIVEIRA, L. I. G. A. da C. **Os carros autónomos e os novos desafios para o mercado de seguros**. 52 f. 2019. Dissertação de Mestrado - Universidade Católica Portuguesa, Lisboa, 2019. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/28412/1/OS%20CARROS%20AUT%C3%93NOMOS%20E%20OS%20NOVOS%20DESAFIOS%20PARA%20O%20MERCADO%20DE%20SEGUROS%20-%20Tese_Vers%C3%A3o%20Final.pdf P.9.

[178] Tradução livre de "El seguro de responsabilidad civil tiene como objetivo cubrir el riesgo de amenazar los activos del asegurado debido a un evento futuro, incierto y dañino, independientemente de su voluntad, un accidente de tráfico, que causará daños a la propiedad material o moral terceros o personas

E em virtude da lógica de funcionamento dos seguros e sua ampla aplicabilidade já no âmbito automobilístico há quem defenda que o sistema de seguros obrigatórios seja a solução mais plausível para os carros autónomos, isso pois

> "o seguro de responsabilidade civil automóvel tem por finalidade cobrir o risco que consiste na ameaça do património do segurado em razão de acontecimento futuro, incerto e danoso, independente da sua vontade – um acidente de trânsito – , que causará prejuízos nos bens materiais ou morais de terceiros ou pessoas transportadas no veículo"[179]

Contudo, afirma Carla Castro que a forma como o seguro de automóveis hoje está delineada

> "[...] não cobre os mesmos riscos que cobria no passado, existem novas automatizações, tecnologias de deteção e proteção que a indústria automóvel está a desenvolver e que alteram o comportamento dos veículos em circulação. Temos a realidade dos veículos autónomos que vai constituir uma verdadeira mudança de paradigma."[180]

Assim, a maior mudança no contrato de seguro será n âmbito da responsabilidade civil, haja vista que as seguradoras deverão desvendar como atribuir o risco do sinistro e a quem imputar em situações envolvendo veículos autônomos nos quais quanto maior o grau de automação mais visível a ausência do condutor nos moldes tradicionalmente conhecidos.[181] Sem contar que ao segurar um carro autônomo a marca, o modelo e o ano venham assumir papel destaque, tendo em vista que atualmente somente algumas marcas investem neste nicho do mercado automobilístico o que pode ocasionar seguros mais elevados.[182]

Este mesmo raciocínio pode ser para os robôs, pois assim como os veículos autónomos varia-se de marca, modelo, funcionalidades e riscos advindos da utilização dos

---

transportadas en el vehículo". ELGUERO Y MERINO, J. M. **El contrato de seguro**. Madrid: Mapfre, 2004. p. 1.

[179] LOPES, M. C. **Seguro Obrigatório de Responsabilidade Civil Automóvel**. [*S. l.*]: Imprensa Nacional - Casa da Moeda, 1987. p. 20.

[180] Carla Castro apud OLIVEIRA, 2019. p.26.

[181] *Ibid*. p.27.

[182] VANSO, T. **A iminência dos carros autônomos e os desafios propostos ao mercado de seguros**. [*S. l.*], [*s. d.*]. Disponível em: https://talitavanso.jusbrasil.com.br/artigos/499245124/a-iminencia-dos-carros-autonomos-e-os-desafios-propostos-ao-mercado-de-seguros. Acesso em: 23 jul. 2020.

mesmos para exercer alguma tarefa, seja ela de segurança ou de administrar o remédio a um paciente num hospital, etc.

Em contrapartida, como bem define Mafalda Miranda Barbosa o cenário dos fundos de compensação podem ser traçados de duas maneiras: a primeira em que todos os cidadãos contribuam para o fundo, assim, desaparecendo a necessidade de aferir responsabilidade a alguém que é substituída por uma saída de segurança social; e a segunda, baseada no esquema securitário, em que a vítima de um dano causo por um ente dotado de inteligência artificial terá acesso a uma compensação advinda de um fundo formado pela contribuição de um maior ou um menor grupo de pessoas sem que seja apontado o responsável por tal ente vez que eles, direita ou indiretamente, retiram benefícios da utilização desta coisa guarnecida de inteligência artificial.[183]

Observa-se que o legislador na proposta de regulamento para harmonização das normas de inteligência artificial em território europeu recomenda no artigo 33. º/8 que "os organismos de notificação devem subscrever um seguro de responsabilidade civil adequado para suas atividades de avaliação"[184], podendo ser descartada essa sugestão em caso de o Estado-Membro assumir esse papel.

Feitas as elucubrações pertinentes, averigua-se nos dois cenários de seguros obrigatórios e fundos de compensação que, embora possam ser o caminho para uma possível resposta as demandas impostas pelos tanto veículos autônomos quanto pelos robôs, ainda esbaram com a necessidade regulatória para passarem ser postas a prova.

---

[183] BARBOSA, 2020. p. 294-295.

[184] Artigo 33.o Organismos notificados

[...]

8. Os organismos notificados devem subscrever um seguro de responsabilidade civil adequado para as suas atividades de avaliação da conformidade, a menos que essa responsabilidade seja assumida pelo Estado-Membro em causa nos termos da legislação nacional ou que esse Estado-Membro seja diretamente responsável pela avaliação da conformidade. UNIÃO EUROPEIA. **Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados).**

6.3 *AUTOMATED AND ELECTRIC VEHICLES ACT*

O *Automated and Electric Vehicles Act 2018*[185] trata-se de lei, promulgada pela Rainha Elizabeth do Reino Unido no dia 17 de julho de 2018, que tem por fim regular e prever soluções às ocorrências envolvendo veículos autônomos ou carros elétricos em solo britânico.

Em linhas gerais, este documento determina a criação de uma lista de veículos autônomos que fica a cago da Secretaria de Estado para o Transporte (cláusula primeira); define a responsabilização da seguradora quando este ente autônomo se conduza e verificar-se no momento do evento que o veículo está segurado e que averigua-se danos ao beneficiário do seguro ou a terceiros (cláusula segundo); ademais antevê a possibilidade de concurso de comportamento culposo do lesado limitando, assim a *strict liability* da seguradora e do dono do automóvel quando dá-se por certo a conduta negligente do lesada (cláusula terceira); quanto ao funcionamento do software não é previsto defeitos de programação, mas sim fica permitido ficar estabelecido na apólice delimitação ou isenção de responsabilidade da seguradora por danos sofridos pelo segurado quando comprova-se que o facto danoso foi ocasionado por alterações feitas no *software* pelo próprio proprietário ou com o conhecimento deste (cláusula quarta).[186]

Ainda cumpre asseverar que nos casos em que não haja celebração de contrato de seguro e o controle do veículo, no momento do sinistro, estava em modo de condução autônoma ter-se-á acesso a responsabilidade do proprietário. Ademais, no diploma em análise a ideia de danos engloba-se os danos o dano proveniente da morte, dos danos pessoais (físicos e morais) e os danos patrimoniais à exceção dos danos patrimoniais a bem de terceiro transportados no veículo "bens de terceiro transportados no veículo ou em atrelado ou em

[185] REINO UNIDO. **Automated and Electric Vehicles Act 2018**. n Act to make provision about automated vehicles and electric vehicles. Queen's Printer of Acts of Parliament, 19 jul. 2019. Disponível em: https://www.legislation.gov.uk/ukpga/2018/18/contents/enacted. Acesso em: 22 jul. 2020.
[186] FELÍCIO, 2019. p. 519-520.

bens submetidos à vigilância da pessoa segurada ou da pessoa que circule no veículo autónomo"[187].

Logo, observa-se que este diploma legal vanguardista tem por fim resolver os conflitos jurisdicionais advindos de acidentes envolvendo veículos autônomos fundado também na sistemática organizacional do direito securitário admitindo-se, é claro, pontualmente em casos específicos na responsabilidade objetiva do condutor/proprietário do veículo. Em vista disso, é precipitado afirmar que esta norma logrou êxito pleno em terras britânicas o que a tornaria um modelo a ser seguido, assim, resta aguardar a sua real eficácia quando for a juízo casos nos quais questiona-se aplicabilidade na norma em comento.

6.4 EM QUE MEDIDA O CONTROLLER PODE SER OU NÃO O OPERADOR DO SISTEMA DE INTELIGÊNCIA ARTIFICIAL

A simples violação dos dados por ato de terceiro não basta para o *controller* ser responsabilizado. Desta forma, para que haja a real responsabilização do *controller* é preciso que ele também viole deveres de cuidado para com terceiro, somente assim, se tem a recondução da lesão. Nesse diapasão, cabe ao *controller* – e, por conseguinte, ao *processor* – adotar medidas de segurança adequadas, que devem levar em consideração as técnicas mais avançadas, os custo de sua aplicação, os riscos envolvidos e a natureza dos dados quê serão tratados.[188]

Destaca-se que quanto ao quesito risco é importante lembrar que para calcula-se com base em avaliação na estimativa de impacto que proteção de terminados dados gerara, sendo isso relevante para a escolha de quais parâmetros estabelecer. Entretanto, caso chegue-se a conclusão de que o tratamento de determinados dados seja eivado de alto risco teme-se que as medidas ditas adequadas sejam insuficientes, assim, deve-se realizar consulta a comissão

[187] *Ibid*. p. 520.
[188] BARBOSA, 2018.P. 212

nacional de proteção de dados de cada Estado- Membro antes mesmo que seja iniciado o tratamento de tais dados, com afirma o Considerando n. º 83 do RGPD. [189]

Esta consulta deve ser realizada assim que percebe-se que o ocorreu a violação de dados via notificação a comissão pertinente. Como também deve-se informar ao titular dos dados para que possa, na medida do possível, tomar as providências que lhe cabem. Logo a maculação de um desses deveres do *controller* convertendo-os em *liability* o que torna-os passiveis de imputação legal. [190]

Outra possibilidade também de se auferir se o *controlle*r é ou não operador do sistema de inteligência artificial reside no facto que avaliar-se ele é responsável ou não pelo ato de terceiro que, embora não esteja previsto no RGPD, pode ser avocado via responsabilidade extracontratual tendo em vista os deveres esquecidos por ele nota-se se os deveres lesionados podem ou não lhe ser imputados.[191]

[189] UNIÃO EUROPEIA. **Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados).**
[190] BARBOSA, 2018.P. 212-213.
[191] Ibid. P. 214.

CONCLUSÃO

Após todas as elucubrações feitas, no último capítulo, além de confrontar o direito de responsabilidade civil e os regulamentos objetos centrais desta dissertação e ao final traz a baila, em tópico exclusivo, os possíveis remédios aventados pelos estudiosos para responder os questionamentos vislumbrados durante a elaboração desta dissertação.

Com isso em mente, primeiro trabalhou-se a hipótese de personificação dos entes autônomos e verificou-se que se dividem entre aqueles que defendem os entes dotados de inteligência artificial como sendo *e-persons* (que possuem efetivamente personalidade jurídica) e aqueles que o reconhecem como *e-servents* (associados a figura do escravo nos tempos de Roma).

Entretanto, ambos apresentam problemas desde questionar se após conferida personalidade jurídica caberia falar em direito de propriedade sobre o *e-person* visto as questões éticas envolvidas até imbróglios montantes indemnizatórios insatisfatórios, pois valor do alcance da pretensão indenizável será limitado ao máximo do pecúlio reservado.

Já quando examinou-se a possibilidade a aplicação dos fundos de compensação ou sistemas de seguros obrigatórios averiguou-se que no primeiro, embora recomendável, deve sofrer alterações para melhor adaptar a nova realidade imposta por esse entes dotados de inteligência artificial, pois a forma em que se encontra os seguros não comporta os diversas aceções que envolvem a dinâmica de tais dotados de tanta independente e de multifacetadas funções. Ademais, no tocante ao fundo de compensação e aos seguros obrigatórios, embora possam ser remédios plausíveis ainda carece de regularização normativa em solo português para poderem se tornar realidade.

Logo após, esmiúça-se o documento legal *Automated And Eletric Vihicles Act*, vigente no Reino Unido, constata-se ser um diploma legal vanguardista que tem por fim solucionar os possíveis conflitos jurisdicionais envolvendo veículos autônomos que merece ser acompanhado visto que a sua real eficácia será posta em prática quando for questionada em juízo sua aplicabilidade.

Por fim, analisou-se em que medida o controller pode ser o não responsabilizado por atos de terceiros auferindo se ele é ou não operador do sistema de inteligência artificial. E percebe-se que a depende duas situação a qual ele está inserido podendo a maculação de um desses deveres do *controller* convertendo-os em *liability* o que torna-os passiveis de imputação legal ou via responsabilidade extracontratual tendo em vista os deveres esquecidos por ele nota-se se os deveres lesionados poderiam ou não lhe ser imputados.

Com isso, conclui-se que existem possíveis remédios, entretanto, todos esbarram em algum impeditivo legal, assim, para os tornar mais efetivos cabe o legislador debruçar-se sobre o tema seja criando lei em apartado para tratar exclusivamente os casos envolvendo inteligência artificial e reconhecimento facial ou seja apontando na miríade legal que compõem o ordenamento jurídico português quais normas são aplicáveis. Enquanto, tal feita não se concretiza cabe somente realizar análises hipotéticas até que o legislador se de conta que as situações não são mero fruto da imaginação, mas sim parte da realidade que nos circunda.

REFERÊNCIAS BIBLIOGRÁFICAS

ALGORITMO: O QUE É, COMO FUNCIONA E QUAIS SÃO OS PRINCIPAIS EXEMPLOS. *In*: ROCK CONTENT - BR. 7 fev. 2019. Disponível em: https://rockcontent.com/br/blog/algoritmo/. Acesso em: 14 maio 2021.

ANDRION, R. Você sabe o que é o QR Code?. *In*: OLHAR DIGITAL. 14 set. 2019. Disponível em: https://olhardigital.com.br/2019/09/14/seguranca/voce-sabe-o-que-e-o-qr-code-a-gente-explica/. Acesso em: 22 maio 2021.

BARANAUSKAS, J. A.; MONARD, M. C. Capítulo 4 - Conceitos sobre Aprendizado de Máquina. *In*: SISTEMAS INTELIGENTES-FUNDAMENTOS E APLICAÇÕES. 1ªed. Barueri/SP: Manoele Ltda, 2003. p. 89–114. *E-book*.

BARBOSA, A. M. C. N. de M. Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil. **Instituto de Direito Bancário, da Bolsa e dos Valores**, [*s. l.*], n. 3, REVISTA ONLINE BANCA, BOLSAESEGUROS, p. 147–214, 2018.

BARBOSA, A. M. C. N. de M. **Estudos a propósito da responsabilidade objetiva**. 1ªed. Cascais: Principia, 2014.

BARBOSA, A. M. C. N. de M. Inteligência artificial, e-persons e Direito: desafios e perspectivas. **Revista Jurídica Luso-Brasileira (RJLB)**, [*s. l.*], v. 3, n. 6, p. 30, 2017a. Disponível em: https://blook.pt/publications/publication/6d03901f9052/

BARBOSA, A. M. C. N. de M. **Lições de responsabilidade civil**. 1ªed. Parede: Principia, 2017b.

BARBOSA, A. M. C. N. de M. O Futuro da Responsabilidade Civil desafiada pela inteligência artificial: modelos tradicionais e caminhos de solução. **Revista de Direito da Responsabilidade**, [*s. l.*], n. ano 2, p. 47, 2020. Disponível em: https://revistadireitoresponsabilidade.pt/2020/o-futuro-da-responsabilidade-civil-desafiada-pela-inteligencia-artificial-as-dificuldades-dos-modelos-tradicionais-e-caminhos-de-solucao-mafalda-miranda-barbosa/

BING, J. Transnacional Data Flows and the Scandinavian Data Protection Legislation. **Stockholm Institute for Scandinavian Law**, [*s. l.*], n. 24, Scandinavian Studies in Law, p. 65–96, 1980.

CAENEIRO DA FRADA, M. A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana. *In*: CONTRATO E

DEVERES DE PROTECÇÃO, SEPARATA DO BOLETIM DA FACULDADE DE DIREITO DA UNIVERSIDADE DE COIMBRA. Coimbra/PT: [*s. n.*], 1994.

CALVÃO DA SILVA, J. **Responsabilidade civil do produtor**. Coimbra: Almedina, 1990. (Colecção teses).

CARNEIRO DA FRADA, M. A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana. *In*: DIREITO E JUSTIÇA. Lisboa: [*s. n.*], 1998. (Volumes Comemorativos dos 30 anos da Universidade Católica Portuguesa e dos 20 anos do seu Curso de Direito).v. II, p. 297–311.

COMISSÃO EUROPEIA. **Livro Branco sobre a inteligência artificial - uma abordagem europeia virada para a excelência e a confiança**. [*S. l.*: *s. n.*], 2020. Disponível em: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_pt.pdf.

COMISSÃO EUROPEIA. **Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos**. Bruxelas, 23 abr. 2021.

CONSELHO EUROPEU. **Conclusões da Presidência – A Carta dos Direitos Fundamentais no contexto da inteligência artificial e da transformação digital**. Bruxelas/BE: [*s. n.*], 2020.

CONSELHO EUROPEU. **Reunião extraordinária do Conselho Europeu (1 e 2 de outubro de 2020) – Conclusões**. Bruxelas/BE: [*s. n.*], 2021.

CORDEIRO, A. B. M. **Direito da proteção de dados: à luz do RGPD e da Lei no. 58/2019**. Coimbra: Almedina, 2020.

DALSENTER, T. **Reconhecimento Facial: laissez-faire, regular ou banir? - Migalhas**. [*S. l.*], 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/330766/reconhecimento-facial--laissez-faire--regular-ou-banir. Acesso em: 15 maio 2021.

DIAMVUTU, L. Para uma melhor compreenção do aseguro obrigatório de responsabilidade civil automóvel: a questão do ressarcimento de danos resultantes de lesões corporais e materiais nos acidentes de viação. **Faculdade de Direito da Universidade de Lisboa**, [*s. l.*], [*s. d.*]. Disponível em: http://www.fd.ulisboa.pt/wp-content/uploads/2014/12/Damvutu-Lino-PARA-UMA-MELHOR-COMPREENSAO-DO-SEGURO-OBRIGATORIO-DE-RESPONSABILIDADE-CIVIL-AUTOMOVELi.pdf

ELGUERO Y MERINO, J. M. **El contrato de seguro**. Madrid: Mapfre, 2004.

FELÍCIO, M. Responsabilidade civil por acidente de viação causado por veículo automatizado. **Revista de Direito da Responsabilidade**, [*s. l.*], n. ano 1, p. 32, 2019. Disponível em: https://revistadireitoresponsabilidade.pt/2019/responsabilidade-civil-por-acidente-de-viacao-causado-por-veiculo-automatizado-manuel-felicio/

FINALLY, FACIAL RECOGNITION FOR COWS IS HERE. [*S. l.*], [*s. d.*]. Disponível em: https://gizmodo.com/finally-facial-recognition-for-cows-is-here-1822609005. Acesso em: 22 maio 2021.

FRANCE FINES GOOGLE €50 MILLION USING GDPR PRIVACY LAW. [*S. l.*], 2019. Disponível em: https://www.euronews.com/2019/01/21/france-fines-google-50-million-using-eu-s-transparency-and-consent-law. Acesso em: 17 out. 2021.

GONÇALVES, I. A. de A. e S. **Software, proteção, consumidor**. 83 f. 2012. Dissertação de Mestrado - Universidade de Coimbra, Coimbra/PT, 2012.

HERING | ROUPAS FEMININAS E MASCULINAS E INFANTIS. [*S. l.*], [*s. d.*]. Disponível em: https://www.hering.com.br/. Acesso em: 22 maio 2021.

HIJMANS, H. Lee A. Bygrave, Data Privacy Law, an International Perspective, Oxford University Press, Oxford, 2014, 272 pages, 234 x 156 mm, 75, ISBN 978-0-19-967555-5. **International Data Privacy Law**, [*s. l.*], v. 5, n. 1, p. 88–90, 2015. Disponível em: https://doi.org/10.1093/idpl/ipu031. Acesso em: 18 out. 2021.

HILL, K. The Secretive Company That Might End Privacy as We Know It. **The New York Times**, [*s. l.*], 18 jan. 2020. Technology. Disponível em: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. Acesso em: 16 maio 2021.

HISTÓRIA DA INTERNET: ORIGEM, QUEM INVENTOU E TUDO SOBRE O ASSUNTO!. *In*: ROCK CONTENT - BR. 27 jan. 2020. Disponível em: https://rockcontent.com/br/blog/historia-da-internet/. Acesso em: 15 maio 2021.

HODGES, C. Delivering data protection: Trust and Ethical Culture. **The Legal Publisher Lexxion**, [*s. l.*], v. 4, n. 1, European Data Protection Law Review, p. 65–79, 2018. Disponível em: https://doi.org/10.21552/edpl/2018/1/9

HUNTON ANDREWS KURTH LLP. **Centre for information policy leadership**. [*S. l.: s. n.*], 2019. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_paper_-_learning_from_the_eu_gdpr_-_what_elements_should_the_us_ado....pdf.

INFORMÁTICA BÁSICA: O QUE SÃO HARDWARE E SOFTWARE? [*S. l.*], [*s. d.*]. Disponível em: https://edu.gcfglobal.org/pt/informatica-basica/o-que-sao-hardware-e-software-/1/. Acesso em: 14 maio 2021.

IRAMINA, A. RGPD V. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**, [*s. l.*], v. 12, n. 2, Brasil, p. 91–117, 2020. Disponível em: https://doi.org/10.26512/lstr.v12i2.34692. Acesso em: 25 maio 2021.

LIMA, F. A. P. de; VARELA, J. de M. A. (org.). **Código civil anotado. Vol. 1: Artigos 1.º a 761.º**. 4. ed. rev. e atualizada. Reimpressãoed. Coimbra: Coimbra Ed, 2011. v. I

LOPES, M. C. **Seguro Obrigatório de Responsabilidade Civil Automóvel**. [*S. l.*]: Imprensa Nacional - Casa da Moeda, 1987.

MAGRANI, E. **A internet das coisas**. 1ªed. Rio de Janeiro, RJ, Brasil: FGV Editora, 2018.

MENA. Verbete Draft: o que é Reconhecimento Facial. *In*: PROJETO DRAFT. 30 maio 2018. Disponível em: https://www.projetodraft.com/verbete-draft-o-que-e-reconhecimento-facial/. Acesso em: 13 maio 2021.

MONICA, 1776 Main Street Santa; CALIFÓRNIA 90401-3208. **The RAND Tablet: iPad Predecessor**. [*S. l.*], 2018. Disponível em: https://www.rand.org/blog/rand-review/2018/09/the-rand-tablet-ipad-predecessor.html. Acesso em: 22 maio 2021.

MULTISTAKEHOLDER EXPERT GROUP. **CONTRIBUTION FROM THE MULTISTAKEHOLDER EXPERT GROUP TO THE STOCK-TAKING EXERCISE OF JUNE 2019 ON ONE YEAR OF GDPR APPLICATION**. Europa: União Europeia, 2019. Disponível em: https://ec.europa.eu/info/sites/default/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf. Acesso em: 24 maio 2021.

O QUE É A INTELIGÊNCIA ARTIFICIAL E COMO FUNCIONA? | ATUALIDADE | PARLAMENTO EUROPEU. [*S. l.*], 2020. Disponível em: https://www.europarl.europa.eu/news/pt/headlines/society/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona. Acesso em: 22 maio 2021.

OLIVEIRA, L. I. G. A. da C. **Os carros autónomos e os novos desafios para o mercado de seguros**. 52 f. 2019. Dissertação de Mestrado - Universidade Católica Portuguesa, Lisboa, 2019. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/28412/1/OS%20CARROS%20AUT%

C3%93NOMOS%20E%20OS%20NOVOS%20DESAFIOS%20PARA%20O%20MERCADO%20DE%20SEGUROS%20-%20Tese_Vers%C3%A3o%20Final.pdf

PAGALLO, U. Apples, oranges, robots: four misunderstandings in today's debate on the legal status of AI systems. **Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences**, [*s. l.*], v. 376, n. 2133, p. 16, 2018. Disponível em: https://doi.org/10.1098/rsta.2018.0168. Acesso em: 22 jul. 2020.

PARLAMENTO EUROPEU. **Regime de responsabilidade civil aplicável à inteligência artificial**. 20 out. 2020.

PAULO MOTA PINTO. **A. Pinto monteiro, Cláusulas limitativas e de exclusão da responsabilidade**. Coimbra/PT: Almedina, 2003.

PINTO, C. A. da M. **Cessão da posição contratual**. Reimpred. Coimbra: Livraria Almedina, 2003. (Colecção teses).

PINTO, I. F. T. **Patentes e Programas de Computador**. 118 f. 2016. Dissertação de Mestrado - Universidade do Minho. Escola de Direito, Braga-PT, 2016.

PISA, P. **Como funciona o reconhecimento facial**. [*S. l.*], 2012. Site. Disponível em: http://www.techtudo.com.br/artigos/noticia/2012/04/como-funciona-o-reconhecimento-facial.html. Acesso em: 15 maio 2021.

PORTUGAL. **Código Civil - Decreto Lei n.º47344/66, 25 de novembro**. **Código Civil**, 25 nov. 1966. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=775&tabela=leis. Acesso em: 13 jul. 2020.

PORTUGAL. **Decreto Lei n.º383/89, de 06 de Novembro**. Transpõe para a ordem jurídica interna a Directiva n.º 85/374/CEE, em matéria de responsabilidade decorrente de produtos defeituosos. 6 nov. 1989. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=729&tabela=leis&so_miolo=. Acesso em: 22 jul. 2020.

RAVIV, S. The Secret History of Facial Recognition. **Wired**, [*s. l.*], v. 28, n. 2, p. 56–65, 2020. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&AuthType=cookie,ip,shib,uid&db=edb&AN=141229925&lang=pt-pt&site=eds-live&authtype=sso. Acesso em: 14 maio 2021.

REINO UNIDO. **Automated and Electric Vehicles Act 2018**. n Act to make provision about automated vehicles and electric vehicles. Queen's Printer of Acts of Parliament, 19 jul. 2019. Disponível em: https://www.legislation.gov.uk/ukpga/2018/18/contents/enacted. Acesso em: 22 jul. 2020.

ROCHFELD, J. Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet. **Law, State and Telecommunications Review**, [*s. l.*], v. 10, n. 1, p. 61–84, 2018. Disponível em: https://doi.org/10.26512/lstr.v10i1.21500. Acesso em: 28 maio 2021.

SANBOT THE ROBOT. [*S. l.*], [*s. d.*]. Disponível em: https://www.sanbot.co.uk. Acesso em: 28 out. 2021.

SECURITYMAGAZINE. Robot ligado a rede privada 5G faz vigilância física na Universidade de Vigo. *In*: SECURITY MAGAZINE. 22 out. 2021. Disponível em: https://www.securitymagazine.pt/2021/10/22/robot-ligado-a-rede-privada-5g-faz-vigilancia-fisica-na-universidade-de-vigo/. Acesso em: 30 out. 2021.

SEM NEM SAIR DE CASA? STARTUP REVELA VEÍCULO AUTÔNOMO DE ENTREGAS [VÍDEO]. [*S. l.*], [*s. d.*]. Disponível em: https://www.tecmundo.com.br/mobilidade-urbana-smart-cities/126684-sair-casa-startup-revela-veiculo-autonomo-entregas-video.htm. Acesso em: 30 out. 2021.

SILVA, J. C. da. **Compra e venda de coisas defeituosas: (conformidade e segurança)**. 5ªed. Coimbra: Almedina, 2008. (Monografias).

SILVA, N. S. e. Inteligência Artificial, Robots e Responsabilidade Civil: o que é que é diferente? **Revista de Direito Civil**, [*s. l.*], v. IV (2019), n. 4º, p. 691–711, 2019. Disponível em: https://doi.org/691-711

SOBRE DARPA. [*S. l.*], [*s. d.*]. Disponível em: https://www.darpa.mil/about-us/about-darpa. Acesso em: 22 maio 2021.

THE STOCKHOLM PROGRAMME — AN OPEN AND SECURE EUROPE SERVING AND PROTECTING CITIZENS. : NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES. Official Journal of the European Union: Concelho Europeu, 2010.

VANSO, T. **A iminência dos carros autônomos e os desafios propostos ao mercado de seguros**. [*S. l.*], [*s. d.*]. Disponível em: https://talitavanso.jusbrasil.com.br/artigos/499245124/a-iminencia-dos-carros-

autonomos-e-os-desafios-propostos-ao-mercado-de-seguros. Acesso em: 23 jul. 2020.

VARELA, A. **Das obrigações em geral**. 7ª (reimpressão)ed. Coimbra/PT: Almedina, 2001. v. II

VARELA, A. **Das obrigações em geral**. 10.ª ed. rev. e actualiz.:15ªed. Coimbra: Almedina, 2018. v. I

VAZ SERRA, A. Responsabilidade do devedor pelos actos dos auxiliares, dos representantes legais ou dos substitutos. **Boletin n. º72**, [*s. l.*], n. 2, [*s. d.*].

VERBETE DRAFT: O QUE É RECONHECIMENTO FACIAL. *In*: PROJETO DRAFT. 30 maio 2018. Disponível em: https://www.projetodraft.com/verbete-draft-o-que-e-reconhecimento-facial/. Acesso em: 14 maio 2021.

LEIS E NORMAS

PORTUGAL. **Constituição da República Portuguesa**. Publicada em: 2/04/1976.

PORTUGAL. **Lei da Proteção de Dados Pessoais**. 8 ago. 2019.

UNIÃO EUROPEIA. **Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu 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 (Regulamento Geral sobre a Proteção de Dados).**

UNIÃO EUROPEIA. **Tratado Sobre o Funcionamento da União Europeia (Versão Consolidada)**. Publicada em: 20/06/2016