



Universidades Lusíada

Guimarães, Eduarda Maria Santos

A inteligência artificial, a Internet das coisas e a proteção de dados

<http://hdl.handle.net/11067/7495>

Metadados

Data de Publicação

2023

Resumo

A rápida evolução tecnológica reduziu o mundo à distância de um clique. Possibilitou o acesso de qualquer cidadão a serviços, produtos e informação do outro canto do mundo. A tecnologia afeta não só o nosso quotidiano, mas também o trabalho, a saúde, as infraestruturas, as empresas, entre outras, modificando até a forma como nos relacionamos. A ligação das coisas à internet permitiu um maior desenvolvimento e controlo das ocorrências cotidianas, agilizando a vida do cidadão. A inteligência art...

The rapid technological evolution has brought the world together just a click away. Possibility of access by any citizen to services, products and information from the other corner of the world. The technology affects not only our daily lives, but also work, health, infrastructures, companies, among others, even changing the way we relate to each other. The connection of things to the internet allowed for better development and control of everyday occurrences, improving the lives of citizens a...

Palavras Chave

Direito, Inteligência artificial - Regulação, Proteção de dados

Tipo

masterThesis

Revisão de Pares

Não

Coleções

[ULP-FD] Dissertações

Esta página foi gerada automaticamente em 2024-11-11T22:12:02Z com informação proveniente do Repositório



UNIVERSIDADE LUSÍADA DO PORTO

**A INTELIGÊNCIA ARTIFICIAL, A INTERNET DAS
COISAS E A PROTEÇÃO DE DADOS**

Eduarda Maria Santos Guimarães

Dissertação para obtenção do Grau de Mestre

Porto, 2023



UNIVERSIDADE LUSÍADA DO PORTO

**A INTELIGÊNCIA ARTIFICIAL, A INTERNET DAS
COISAS E A PROTEÇÃO DE DADOS**

Eduarda Maria Santos Guimarães

Dissertação para obtenção do Grau de Mestre

Orientador: Prof. Doutor Alberto Ribeiro de Almeida

Porto, 2023

Agradecimentos

Desde logo, gostaria de agradecer ao meu orientador, Prof. Doutor Alberto Ribeiro de Almeida, por ter aceite ser orientador da minha tese. Agradeço ainda, toda a sua ajuda e disponibilidade no que concerne a partilha de conhecimentos, sugestões, rápida análise e correção do conteúdo da tese.

Agradeço ainda aos meus familiares, amigos e ao meu namorado, por todo o apoio neste arduo percurso até à conclusão da minha tese, que contribuíram de forma inegável para a conclusão da mesma.

Obrigada a todos pelo apoio, pela paciência e compreensão. Não existem palavras suficientes para agradecer todo o apoio que recebi.

Índice

Agradecimentos	I
Índice	II
Resumo	IV
Abstract.....	V
Palavras-chave	VI
Lista de siglas e abreviaturas	VII
1. Introdução	8
2. A inteligência artificial	9
2.1 Definição	9
2.2 Tipos de inteligência artificial.....	10
2.2.1 A inteligência artificial limitada (IAL)	10
2.2.2 A inteligência artificial geral (AIG)	11
2.2.3 A superinteligência (SIA).....	12
2.3. As vantagens da inteligência artificial	13
2.4. Desvantagens da inteligência artificial	14
3. A internet das coisas	14
3.1. Definição de internet das coisas (IoT)	14
3.2 Características da internet das coisas	16
3.3 Elementos da internet das coisas.....	17
3.4 A aplicação da internet das coisas.....	18
3.4.1 Aplicação da internet das coisas na habitação.....	18
3.4.2 A aplicação da internet das coisas na saúde	19
3.4.3 A aplicação da internet das coisas nas empresas.....	21
3.4.4 A inteligência artificial e o covid-19.....	22
3.5 Desafios da internet das coisas.....	24
4. A ligação entre a internet das coisas e a inteligência artificial	26
4.1 As aplicações da internet das coisas e da inteligência artificial.....	28

5. A afetação destas tecnologias no direito da privacidade e intimidade e a emergência na criação de uma regulação inteligente	29
6. A proteção constitucional da privacidade.....	35
7. A comissão nacional de dados	40
8. O problema da internet das coisas e da inteligência artificial na proteção da privacidade.....	42
8.1. A proteção de dados e o totalitarismo informático	50
8.2 Os problemas ético-jurídicos e as soluções dadas pela UE	51
8.2.1. A viés algorítmica	52
8.2.2 A transparência.....	52
8.2.3 A responsabilidade pelos danos causados por sistemas IA.....	54
8.2.4 A justiça e equidade	63
8.2.5. A proteção de dados	64
9. O ChatGpt, questões ético-jurídicas	65
9.1. O ChatGpt e a proteção de dados.....	74
10. O regulamento geral de proteção de dados.....	77
10.1 A proteção de dados na europa	77
10.2 O regulamento geral de proteção de dados	78
10.3 Os dados pessoais.....	80
10.4 Tratamento de dados pessoais.....	81
10.4.1. Princípios relativos ao tratamento de dados pessoais.....	84
10.4.2 O Consentimento e o direito à indemnização.....	89
10.4.3 O consentimento de menores	98
Conclusão	106
Bibliografia.....	108

Resumo

A rápida evolução tecnológica reduziu o mundo à distância de um clique. Possibilitou o acesso de qualquer cidadão a serviços, produtos e informação do outro canto do mundo.

A tecnologia afeta não só o nosso cotidiano, mas também o trabalho, a saúde, as infraestruturas, as empresas, entre outras, modificando até a forma como nos relacionamos.

A ligação das coisas à internet permitiu um maior desenvolvimento e controle das ocorrências cotidianas, agilizando a vida do cidadão. A inteligência artificial criou uma nova forma de obter respostas, de realizar cálculos e previsões, permitindo a redução de horas de trabalho, estudo e as decisões incorretas.

Os seres humanos estão a ser constantemente sugados por todas estas tecnologias o que afeta, não só a sua vida, mas também a forma de pensar, de julgar, de tomar decisões. A sede por informação transformou-se numa forma aliciante de permissão inconsciente de entrega de dados pessoais.

Face a esta nova realidade, tornou-se crucial encontrar fronteiras de equilíbrio entre o desenvolvimento tecnológico e a proteção dos dados pessoais e dos direitos pessoais com particular atenção ao princípio da privacidade.

Por isso, esta dissertação terá como objetivo principal desenvolver o tema sobre a inteligência artificial e a internet das coisas visto na perspetiva do Direito.

Irei ainda, enunciar algumas questões importantes deste tão vasto tema e, uma vez que, a aderência a estas novas tecnologias é tão incisiva, analisar as implicações que as mesmas têm na proteção de dados e na privacidade, retirando destas algumas conclusões.

Abstract

The rapid technological evolution has brought the world together just a click away. Possibility of access by any citizen to services, products and information from the other corner of the world.

The technology affects not only our daily lives, but also work, health, infrastructures, companies, among others, even changing the way we relate to each other.

The connection of things to the internet allowed for better development and control of everyday occurrences, improving the lives of citizens and companies. Artificial intelligence has created a new way of getting answers, making calculations and predictions, allowing the reduction of hours of work, study and incorrect decisions.

Human beings are constantly being sucked into all these technologies, which affects not only their lives, but also their way of thinking, judging, and making decisions. The thirst for information has turned into an attractive form of unconscious permission to hand over personal data.

Faced with this new reality, it has become crucial to find balance between technological development and the protection of personal data and personal rights, with particular attention to the principle of privacy.

Therefore, this dissertation will have as main objective the develop of the theme about artificial intelligence and the internet of things seen from the perspective of Law.

I will also enunciate some important issues of this vast subject, and since the adherence to these new technologies is so incisive, I will analyze the implications that these technologies have on data protection and privacy, drawing some conclusions from these.

Palavras-chave

Inovação tecnológica; Proteção de dados pessoais; Privacidade; Tratamento;
Mercado de dados

Lista de siglas e abreviaturas

Ac.	Acórdão;
Al/al)	Al), al);
Art.º art.º	Art., art.;
BD	BD;
CADH	Convenção dos Direitos Fundamentais da União Europeia;
CC	Código Civil;
CE	Comissão Europeia;
CEDH	Convenção Europeia dos Direitos do Homem;
CNPD	Comissão Nacional de Proteção de Dados;
CRP	Constituição da República Portuguesa;
CNPD	Autoridade Nacional de Controlo de Dados Pessoais;
IA	Inteligência Artificial;
IAG	Inteligência Artificial Geral;
IAL	Inteligência Artificial Limitada;
GT29	Grupo de Grupo de Trabalho do Artigo 29.º
LLMs	Large Language Models Large
N.º	N.º, n.º;
Proc.	Proc.;
SIA	Superinteligência;
Ss.	Seguintes;
TJUE	Tribunal Judicial União Europeia.

1. Introdução

As novas tecnologias vieram revolucionar as sociedades modernas e trouxeram mudanças para as pessoas na maneira de pensar, de agir e de se relacionar. Alteraram a forma de consumo, permitindo a realização de variadas tarefas, tornando o mundo próximo, à distância de um clique.

Pessoas de diferentes países, continentes, cidades e ruas podem efetuar compras, encomendar bens, realizar reuniões e trabalhar sem saírem de casa, precisando apenas de um equipamento ligado à internet.

Esta aproximação digital possibilitou ainda a partilha de variados dados, de computador para computador, colocando em perigo a proteção dos dados pessoais e consequentemente o direito à privacidade.

Tornamo-nos transparentes, vulneráveis, onde tudo sobre nós encontra-se na rede sem que nos apercebamos disso. Cada clique, escolha, preferência, ligação selecionada ou compra efetuada liberta uma ínfima quantidade de dados sobre nós. Permite a dedução de inclinações, vontades, necessidades e em alguns casos, nome, morada, entre outros dados.

Enfim, o pagamento para a inovação tecnológica é, sem sombra de dúvida os dados pessoais.

Por isso, é possível constatar que as tecnologias da informação têm comprometido não só a proteção dos dados pessoais, como também e consequentemente, a proteção ao direito à privacidade e à intimidade. Neste sentido, urge a necessidade de criação não só de uma legislação inovadora e protetora, de forma a controlar a difusão e o acesso a dados pessoais pelas entidades tecnológicas, como a de transmitir conhecimento às pessoas acerca deste tema, dos seus benefícios, mas também dos seus perigos.

Neste trabalho, propõe-se desenvolver a temática da inteligência artificial e da internet das coisas de uma maneira geral, enunciando as características e variadas utilizações e, posteriormente, referir os benefícios, mas também os perigos e consequências da utilização em massa destas tecnologias. Posteriormente, serão ainda mencionadas as soluções criadas pela Europa, apresentando ainda uma opinião crítica sobre as mesmas.

2. A inteligência artificial

2.1 Definição

Para que seja possível definir IA é necessário, em primeiro lugar, separar as palavras inteligência e artificial.

A palavra “inteligência” provém do latim *intelligentia*, oriundo de *intelligere* em que “enter” significa “entre” e *legere* significa escolha.

Neste sentido, a inteligência é uma capacidade intelectual pertencente ao indivíduo que compreende a possibilidade de avaliar as vantagens e desvantagens das hipóteses, pensar, interpretar e retirar soluções dessas interpretações. Assim, é a capacidade que o indivíduo tem de, perante várias possibilidades, escolher uma que acha mais adequada.

Para além disso, a inteligência não é igual em todos os seres humanos uma vez que, ela depende de outras faculdades como o uso da memória, do juízo, da abstração, da imaginação e da conceção.

A inteligência divide-se, segundo Hower Gardner, de acordo com a sua teoria de inteligências múltiplas, em três grupos: a inteligência psicológica (a capacidade cognitiva, de aprendizagem e relação), a inteligência biológica (a capacidade de adaptação perante novas situações) e a neurológica sendo estas faculdades aquelas que distinguem o ser humano dos restantes ser-vivos.¹

Já a palavra artificial significa que não é natural, que foi produzida artificialmente, o que, para Jacob Turner é relativamente incontroverso.

Posto isto, poder-se-ia acreditar que é fácil definir IA, no entanto isto está longe de ser verdade.

Segundo Jacob Turner, autor do livro *Robot Rules*, tentar definir IA é como perseguir o horizonte, pois assim que se alcança até onde ele estava, ela já se moveu para outro sítio.²

Por um lado, a falta de precisão na definição de IA acabou por ajudar na proliferação da mesma, permitindo o seu crescimento a todos os níveis. Certo é que, uma definição iria estabelecer um único caminho impedindo, desta forma, o desenvolvimento livre. Assim,

¹ GARDNER, Howard, *Inteligências Múltiplas*, 2005, pág. 9

² TURNER, Jacob. 2019. *Robot Rules. Regulating Artificial Intelligence*. London, England: Palgrave Macmillan Cham.

cientistas e pesquisadores podem estender a IA livremente e a mesma pode-se desenvolver sem qualquer objetivo pré-estabelecido.

No entanto, e ainda que não se pretenda colocar um ponto final na definição de IA, é possível depreender que a inteligência artificial é a faculdade de uma máquina de conhecer, compreender, raciocinar, pensar e interpretar.

Em suma, a inteligência artificial é um ramo da ciência da computação que elabora dispositivos que simulam a inteligência humana.³

2.2 Tipos de inteligência artificial

A inteligência artificial pode ser dividida em três tipos sendo eles, a Inteligência Artificial Limita (AIL), Inteligência Artificial Geral (AIG), Superinteligência (SIA).⁴

2.2.1 A inteligência artificial limitada (IAL)

Este tipo de inteligência artificial é conhecido como a IA limitada, porque apesar de proceder ao armazenamento de dados e realizar tarefas relativamente complexas, não tem capacidade para desempenhar tarefas além daquelas para as quais foi programada.

Neste sentido, estes equipamentos não são capazes de ir para além daquilo que estão programados, sendo incapazes de reproduzir o comportamento humano, apenas simula-lo. É utilizada para a execução de tarefas únicas, de forma completa e eficiente, sendo que essas tarefas são sempre orientadas para alcançar determinados objetivos.

Esta tecnologia é aplicada em sistemas de assistência virtual, de reconhecimento fácil, nos sistemas de condução autónoma dos veículos, jogos de xadrez, entre outros.

A IAL pode ser subdividida em duas subcategorias, sendo elas as máquinas reativas e as máquinas de memória limitada.

As máquinas reativas não possuem capacidade de armazenamento por isso, apenas realizam tarefas de acordo com a sua programação. Estas, como o nome indica, executam uma reação quando estimuladas para o efeito.

Acontece que, devido à impossibilidade de armazenar dados, estas não têm capacidade para realizar tarefas de aprendizagem.

³ Turner Jacob, Robot Rules, 2019, pág. 3

⁴ Catisha Nestor et al., 2020, Inteligência Artificial, Revista USP.

As máquinas de memória limitada já possuem, como o nome indica, capacidade de armazenamento. Estas também são reativas, no entanto, devido à possibilidade de armazenamento de uma pequena quantidade de dados, já conseguem aprender com os dados que armazenaram.

Desta forma, conseguem interpretar informações através de dados estatísticos presentes no banco de dados provenientes do seu histórico de interação.⁵

2.2.2 A inteligência artificial geral (AIG)

A IA geral é, de uma forma geral, a capacidade de uma máquina realizar qualquer tarefa intelectual da mesma forma de um humano. Isto implica a capacidade de reconhecimento, armazenamento e aprendizagem.

Esta distingue-se da IAL uma vez que, já tem a capacidade de, através da recolha de dados, aprender e, com base nisso, replicar comportamentos, identificar padrões, oferecer respostas e tomar decisões.

A esta competência é dado o nome de *machine learning*, uma tecnologia que permite que a máquina, através da recolha de dados, consiga decidir quais respostas mais adequadas aos comandos atribuídos. A característica principal da *machine learning* é a possibilidade da máquina se adaptar, apresentando soluções diferentes para variadas situações, sendo essa capacidade o que a aproxima do pensamento humano.

A IAG também se subdivide em duas subcategorias, as máquinas cientes e as autoconscientes.

Enquanto que as primeiras, são capazes de compreender estímulos e processar informações, as segundas, têm uma relativa consciência de si próprias e do mundo, o que facilita a compreensão dos estímulos externos.

Ainda que a IAG esteja mais avançada que a IAL esta ainda não se encontra ao nível da inteligência humana. Aliás, pesquisadores entendem que ainda existe um défice de desenvolvimento na criação de tecnologias que ultrapassem consideravelmente a o pensamento humano, uma vez que, entendem que estas tecnologias ainda operam confinadas a cenários para os quais foram programadas.⁶

⁵ Mialhe Nicolas & Hodes Cyrus, 2017, *The Third Age of Artificial Intelligence*, pág 9

⁶ Mialhe Nicolas & Hodes Cyrus, 2017, *The Third Age of Artificial Intelligence*, pág. 8

Acresce que, ainda que as mesmas sejam capazes de transferir informação e conhecimento, generalizar e criar padrões, ainda nos encontramos muito longe da versatilidade da mente humana.

A razão deste “atraso” no desenvolvimento do *machine learning* deve-se, desde logo, ao desconhecimento dos vários processos complexos do cérebro, da maneira como o consciente humano funciona e como se manifesta.⁷

2.2.3 A superinteligência (SIA)

Tem como objetivo ultrapassar a inteligência humana. Com esta tecnologia, pretende-se o armazenamento de dados e a tomada de decisões impossíveis à mente humana.

Tem como características a autonomia e consciência existindo quem acredite que esta será capaz de pensar de forma mais habilidosa que os humanos.

O cinema retrata esta tecnologia como aquela que criará robôs que irão dominar o mundo, o que se acredita que não acontecerá, não sendo a ideia de robôs inteligentes, no entanto, totalmente desprovida de sentido.

Uma característica desta tecnologia é a capacidade de as máquinas produzidas pela SIA possuírem emoções e vontades próprias.

No final, o objetivo principal da SIA é a construção de máquinas capazes de ser melhores que os humanos não só ao nível mental e motor, mas também ao nível emocional.

Assim, as máquinas tornar-se-ão melhores atletas, cientistas, médicos, etc.

Não obstante o dito, por muito que esta aposta seja promissora, existem várias preocupações que advêm do desenvolvimento da ASI, como o estudo das consequências da realização do raciocínio avançado.⁸

O uso do termo “superinteligência” deve-se à tentativa de criar um intelecto que ultrapasse as melhores mentes humanas em vários domínios. Acontece que, este entendimento é demasiado vago, pelo que, qualquer sistema, possuidor de qualquer característica da ASI, pode ser qualificado como superinteligente.

Desta forma, para que seja mais fácil a distinção ente as tecnologias com superinteligência e as demais pode-se subdividir em três formas: superinteligência rápida, coletiva e de qualidade.

⁷ Miailhe Nicolas & Hodes Cyrus, 2017, *The Third Age of Artificial Intelligence*, pág. 9

⁸ Bostrom, Nick, 2016, *Superintelligence*, pág.22.

2.3. As vantagens da inteligência artificial

A principal vantagem da IA resulta, inequivocamente, da intenção para o qual foi criada, ou seja, para facilitar a vida ao homem. É claro que, com a inovação da mesma as vantagens da criação destes mecanismos ficam a cada dia mais evidentes.

Outra vantagem, é a rapidez uma vez que, as máquinas são concebidas para operar ininterruptamente, contribuindo assim para a tomada rápida de decisões. Uma das principais vantagens é a taxa de erro mínima. Esta deve-se ao facto de as ações da IA serem reguladas por algoritmos.

Para além disso, a inteligência artificial, devidamente programada, tem como vantagem a imparcialidade e a taxa de erro mínima, o que torna a tomada de decisões mais lógicas e acertadas, diferente da eficiência humana, sujeita a alterações de estado de espírito.

A IA é muito vantajosa nos setores comercial e industrial, uma vez que contribui essencialmente para a diminuição de erros, aumento da eficiência, agilização de atividades repetitivas ou demasiado complexas. Esta é utilizada para analisar todo o tipo de informações, criar estatísticas e retirar as decisões mais assertivas alcançando, deste modo, os resultados desejados.⁹

Para além disso, esta ciência aliada à robótica pode ainda praticar atividades que possam ser uma ameaça para o ser humano.

Os assistentes digitais (*chatbots*) são uma das principais vantagens criada pela IA no sentido que, possibilita às empresas responder a clientes em massa inexistindo a necessidade de recorrer a trabalhadores para o atendimento ao cliente. Neste momento, alguns dos *chatbots* são tão bem concebidos que já se torna quase impercetível a presença do robot no lado do assistente.

Por fim, a IA possibilita ainda, graças à grande capacidade de análise de dados, a deteção de fraudes, roubos e transações indevidas.¹⁰

A IA é uma revolução que veio para ficar, que vai nos expandir individualmente como pessoas contribuindo para as nossas atividades do dia-a-dia, no trabalho e nas atividades de lazer.

⁹ Bhbosale, Pujari, Multani. 2020. Advantages And Disadvantages Of Artificial Intelligence in National Seminar on Trends in Geography, Commerce, IT And Sustainable Development, 2020, pág. 227

¹⁰ Bhbosale, Pujari, Multani. 2020. Advantages And Disadvantages Of Artificial Intelligence in National Seminar on Trends in Geography, Commerce, IT And Sustainable Development, 2020, pág. 228

2.4. Desvantagens da inteligência artificial

É claro que, como tudo o que é criado, a IA também tem desvantagens, ainda que considere que, as mesmas não são suficientes para inviabilizar esta tecnologia.

Em primeiro lugar, esta tecnologia ainda é, na maior parte das vezes, muito dispendiosa, o que implica inúmeras despesas na criação e atualização das infraestruturas, energia elétrica e conectividade. Para além disso, são ainda dispendiosas as despesas com manutenções, reparações e profissionais altamente qualificados para lidar com os equipamentos e máquinas.

Acresce que, a IA acaba por eliminar determinados postos de trabalho. No entanto, esta também contribui para a criação de outros trabalhos ao nível do controlo e manutenção dos equipamentos inteligentes.

Acresce ainda que, esta tecnologia alimenta-se de um considerável número de dados para produzir decisões fidedignas, o que inicialmente atrasa o processo de criação. Para além disso, as máquinas inteligentes ainda operam para aquilo que foram programadas o que, por vezes, impede a inovação e as inviabiliza enquanto instrumentos inovadores.

Estes mecanismos, se colocados nas mãos erradas, podem provocar a destruição e a sua constante utilização contribui para a preguiça do ser humano que, cada vez mais, depende das tecnologias para realizar tarefas do dia a dia.

Por fim, é certo que estas tecnologias são indiscutivelmente superiores aos seres humanos no que toca à eficiência na realização de determinadas tarefas, no entanto, esta não é capaz de recorrer às relações e conexões humanas o que, por vezes, a impede de obter resultados diferentes ou mais adequados à situação. ¹¹

3. A internet das coisas

3.1. Definição de internet das coisas (IoT)

De uma forma simples, do conceito de IoT (Internet of Things) retira-se que, a IoT resulta de uma ligação entre as “coisas” e a “Internet”, sendo que, esta ligação, pode ser realizada em quase todos os objetos do dia a dia, desde fechaduras de portas a bolas de futebol. A cada um destes objetos é lhes inserido, através de um chip, um número de

¹¹ Bhbosale, Pujari, & Multani. 2020. Advantages And Disadvantages Of Artificial Intellegence in National Seminar on Trends in Geography, Commerce, IT And Sustainable Development, pág 229

identificação (UID) e um endereço eletrônico protocolado (IP) sendo que os mesmos conectam-se através de fio, wireless, e bluetooth.¹²

Este termo, foi referido pela primeira vez em 1999 por Kevin Ashton numa apresentação na empresa Procter & Gamble, uma corporação multinacional americana de bens de consumo. Segundo este, o termo foi criado com o objetivo de realçar a necessidade da integração da internet na venda de produtos.

Resumidamente, a questão surgiu quando um batom que, apesar de se encontrar em stock nos registos da empresa onde trabalhava, apresentava-se constantemente como esgotado nos revendedores, problema esse derivado à impossibilidade de se realizar eletronicamente uma ligação entre o revendedor e o stock da empresa.

Para solucionar o problema, o pioneiro da tecnologia, inspirado nos microchips presentes nos cartões de crédito que prosperavam na Europa à época decidiu, apresentar um projeto no qual se integrava uma antena RFID (identificação por radiofrequência) nas prateleiras desses produtos de forma a controlar a quantidade de produto disponível e assegurar as entregas dos mesmos atempadamente.

A expressão IoT surgiu assim, de forma acidental, criada com o intuito de realçar a importância da conexão das coisas à internet.¹³

A IoT é, tal como já referido anteriormente, caracterizada pela interconexão digital de objetos físicos com a internet. Tal conexão, é realizada por sensores que captam informações e enviam-nas para plataformas que tratam a informação de forma a que a mesma integre processos, serviços e aplicações. Através da conexão dos dispositivos inteligentes estes conseguem adquirir dados, permutar informações entre si e tomar decisões. Esta recolha de informação e interligação é realizada também através de aplicações como o Twitter, plataformas de comércio eletrónico, entre outras.¹⁴

A título exemplificativo, o smartphone tem diversos sensores que lhe indicam a localização, temperatura, pressão barométrica, entre outros e essa informação é partilhada na rede.¹⁵

Um exemplo desta interligação é a aplicação Uber que não poderia ser utilizada sem a interligação entre dispositivos. Ou seja, quando se pretende realizar uma viagem, o

¹² GREENGARD, Samuel, The Internet of Things, 2015, pág. 14

¹³ ASHTON, Kevin. 2017. The Internet of Things will disrupt transportation. Disponível na Internet em: https://youtu.be/PXncS2_63o4.

¹⁴ SANTOS, Pedro Miguel Pereira. 2016. Internet das Coisas: O desafio da privacidade, pág. 14.

¹⁵ FILHO, Nelson Belliconta, 2019. TRUMIT - Gerenciador de confiança para IoT, pág.16

smartphone do passageiro emite para a rede a sua localização e a pretensão de requerer uma viagem. Já o smartphone do motorista, emite a localização e a disponibilidade da realização da viagem.¹⁶

Outro exemplo do IoT é o GPS, Global Positioning System, tecnologia que funciona através do fornecimento, pelos dispositivos de localização, a localização aos satélites. Desta forma, é possível ao GPS indicar rotas, identificar congestionamentos e alterar rotas de acordo com a segurança e fluidez do tráfego em geral.¹⁷

3.2 Características da internet das coisas

Desde logo, uma das principais características da IoT, que deriva da própria noção, é a conexão digital entre aparelhos eletrônicos.

Para além disso, outra característica é a heterogeneidade, ou seja, a conexão à internet de uma grande quantidade de dispositivos IoT heterogêneos compostos por diferentes sensores ou atuadores. Esses dispositivos possuem, no entanto, para já, recursos limitados, ao nível da energia, memória, processamento e conexão.¹⁸

Mais, estes dispositivos interagem automaticamente à medida que se aproximam uns dos outros, gerando assim eventos. Esses eventos, aumentam com o crescimento da interação espontânea dos dispositivos tornando-se assim uma rede dinâmica e sem uma infraestrutura que suporte as operações.

Todos esses sensores geram uma grande quantidade de dados aleatórios que serão recolhidos, tratados, organizados e interpretados pela capacidade dos dispositivos inteligentes que agem de acordo com as circunstâncias.

O desafio será gerir a gigantesca quantidade de dados resultante destas imensas conexões e garantir a segurança dos mesmos.

A IoT tem múltiplas utilizações, quase qualquer coisa pode ser ligada à internet. Graças à IoT existem diversas aplicações que são utilizadas para diversos tipos de comodidades como por exemplo, transporte e logística, cuidados de saúde, indústria, entre

¹⁶ ASHTON, Kevin, 2017. The Internet of Things will disrupt transportation. Disponível na Internet em: https://youtu.be/PXncS2_63o4.

¹⁷ GPS - O que é, como funciona, Sofisica, consultável in <https://www.sofisica.com.br/conteudos/curiosidades/gps.php>

¹⁸ RAMASAMY, Lakshmana Kumar; KADRY, Seifedine, 2021 Blockchain in the Industrial Internet of Things, pág.4

outros, sendo que após a utilização dessas também esses dados são armazenados para possíveis utilizações.¹⁹

3.3 Elementos da internet das coisas

Os principais componentes da IoT são a *Hardware, Middleware e Presentation*. Contem ainda seis elementos básicos que contribuem para a interligação das coisas através da Internet. São eles, a identificação, o sensoriamento, a comunicação, a computação, os serviços e a semantics.

Em primeiro lugar, o elemento da identificação identifica os objetos de forma a conecta-los à internet, utilizando-se para o efeito tecnologias como RFID e NFC.

A RFID, (*Radio Frequency Identification*), é um sistema utilizado para identificar automaticamente qualquer dispositivo. Funciona através da transmissão das informações oriundas de ondas de rádio convertidas em informações digitais. Podem ser utilizadas na substituição do código de barras, no controlo de stock nos produtos, localização de animais, entre outros.

A NFC, (*Near Field Communication*), é uma tecnologia que possibilita a comunicação sem fios entre dois dispositivos relativamente próximos entre si. Funciona quando uma das partes é o Initiator, que inicia a ligação e controla a informação transmitida, e a outra parte, o Target, que se limita a responder à ação requisitada. Esta tecnologia é utilizada, a título exemplificativo, no cartão contactless.

Em segundo lugar, passa-se à fase do sensoriamento que ocorre quando os objetos recolhem os dados, armazenando-os ou encaminhando-os para a nuvem, sendo as informações recolhidas posteriormente analisadas com base nos serviços necessários.

A *Middleware*, (tecnologias intermediárias), é uma tecnologia que permite assegurar a manutenção, desenvolvimento e execução das aplicações munidas de sensor. Isto contribui para a formação de tarefas de sensoriamento complexas, coordenação entre sensores, fusão de dados e comunicação dos resultados.²⁰

Secure Data Aggregation, (agregação segura de dados), é essencial para assegurar a confiança na recolha de dados a partir dos sensores, protegendo o sistema de intrusos.

¹⁹ RAMASAMY, Lakshmana Kumar & KADRY, Seifedine, 2021. Blockchain in the Industrial Internet of Things, pág.4

²⁰ DHIVIYA, S.; MALATHY, S.; KUMAR, D. Rajesh, 2018. Internet of Things (IoT) Elements, *in* Journal of Computational and Theoretical Nanoscience, pág. 2.

Outro elemento da IOT, é o armazenamento de dados que tem de ser mantido em segurança para permitir uma confiança no sistema. Os dados presentes na IOT servem maioritariamente para a monitorização e inclinação para a tomada de decisões.

Um outro elemento da IOT é a visualização dos dados. Os dados são organizados de forma a que exista fácil acesso e compreensão dos mesmos. A organização contribui para uma melhor tomada de decisão. Por isso, a visualização deve conter os dados transformados e os dados obtidos inicialmente de forma a que a totalidade da informação seja sempre disponibilizada totalmente aos utilizadores.²¹

3.4 A aplicação da internet das coisas

3.4.1 Aplicação da internet das coisas na habitação

A IoT pode ser utilizada em vários dispositivos presentes nas habitações dos utilizadores. As chamadas *smart homes* permitem a conexão e o controlo de variados dispositivos possibilitando ao utilizador a demanda, o controlo e gestão de tarefas à distância, simplificando as atividades domésticas.

Estes dispositivos interligados permitem o controlo à distância do aquecimento da habitação, da eletricidade, da segurança e da limpeza e até da segurança da construção.

Estas construções inteligentes utilizam sensores para controlar a localização dos utilizadores no local. Desta forma, essa informação pode ser considerada no funcionamento das luzes, ventilação e segurança.

Possibilita ainda, a redução de custos e o auxílio na prática de atividades sendo variados os dispositivos dotados de sensores como máquinas de lavar, secar e de café, aspiradores, estores, televisões, aparelhos de ar condicionado, frigoríficos, entre outros.

Todos estes instrumentos procedem à recolha de dados, sendo os mesmos enviados guardados na base de dados ou transferidos para outros dispositivos via internet.

Pode-se considerar a título exemplificativo, uma portada inteligente, que pode ser programada para abrir e fechar a determinada hora ou até enviar uma notificação ao utilizador em caso de precipitação.

Ainda que estes dispositivos possam operar sem a ligação a outros dispositivos é possível realizar a ligação dos mesmos a um só controlador. Este controlador vai simplificar

²¹ DHIVIYA, S.; MALATHY, S.; KUMAR, D. Rajesh, 2018. Internet of Things (IoT) Elements, in Journal of Computational and Theoretical Nanoscience, pág. 8.

a tarefa, recebendo os dados dos dispositivos, controlando-os a partir da mesma fonte. Esta tecnologia é o resultado da simbiose entre a IoT e a IA.²²

A Domótica, pode-se definir como conjunto de métodos destinados a mecanizar uma habitação sem a ação do homem.

O controlador, ou *hub*, é ligado ao roteador doméstico através de um cabo *Ethernet*, um cabo de conexão que tem como objetivo distribuir internet aos equipamentos.

Posteriormente, o utilizador tem acesso aos dados armazenados na nuvem procedendo à realização dos comandos aos sensores, via internet, sendo notificado posteriormente das ações realizadas.²³

3.4.2 A aplicação da internet das coisas na saúde

A internet das coisas tem sido um grande contributo para o avanço no setor da saúde, especialmente no aumento da esperança média de vida, falando-se já na *Internet of Health Things (IoHT)*, em português, Internet das coisas na saúde, um conceito que resulta de uma extensão da internet das coisas à saúde.²⁴

Esta, utiliza sensores biomédicos e aplicações ligadas à internet que têm como objetivo melhorar tratamentos, técnicas e diminuir custos, contribuindo assim, para um aumento da esperança média de vida. Tudo isso, se deveu ao facto de existir a constante necessidade de monitorização do corpo e dos sinais vitais.²⁵

A IoT transformou a forma como um paciente é cuidado e diagnosticado. Através da conexão de aparelhos que os pacientes podem usar é possibilitado ao médico a monitorização real da informação e estado de saúde do paciente

No entanto, o desenvolvimento na área da saúde não se cinge apenas ao referido indo muito além disso. A título exemplificativo, há o avanço nos aparelhos digitais de diagnóstico, que armazenam os dados dos exames realizados, evitando o uso do papel, preservando o meio ambiente, permitindo o rápido acesso aos mesmos, a simplicidade no compartilhamento e correlação dos resultados, garantindo também a integridade dos exames.

²² DHIVIYA, S.; MALATHY, S.; KUMAR, D. Rajesh, 2018, Internet of Things (IoT) Elements, in Journal of Computational and Theoretical Nanoscience, pág. 3.

²³ BORGES, Paulo I. C., 2015. Internet-of-Things, An Arduino-based Domotic System for the Internet-of-Things, pág. 2.

²⁴ AROOSA, Ullah et al., 2021. Securing NDN-Based Internet of Health Things through Cost Effective Signcryption Scheme, 2021, pág. 1.

²⁵ DIAS, Carlos André Ferreira, 2019. A privacidade na era da internet das coisas, pág. 27.

Acresce que, a correlação destes sensores, entre o paciente e a maquinaria de suporte de vida, permite o acesso rápido a dados vitais, sintomas internos e alterações corporais, contribuindo para o rápido diagnóstico.

Outro exemplo dos benefícios da IoT na saúde é a implantação de aparelhos conectados nos pacientes, como por exemplo, os marcapassos inteligentes que monitorizam o sistema cardiovascular nos pacientes, armazenam e enviam dados em tempo real sobre a condição do paciente.²⁶

Assim, através da monitorização do indivíduo, os profissionais de saúde conseguem verificar a saúde do paciente à distância, podendo intervir quando necessário.

Acresce ainda que, hoje em dia, é ainda possível com a utilização de sensores supervisionar a realização de tarefas rotineiras por doentes que padeçam da Doença de Parkinson. Desta forma, esses dados são enviados para uma central permitindo assim aos pesquisadores assimilar o avanço da doença nos pacientes.²⁷

Esta tecnologia permitiu ainda, o desenvolvimento dos monitores contínuos de glicose, que enviam as informações dos níveis de glicose para os smartphones dos clientes para que estes se possam autorregular.

Para além disto, existem ainda nanocâmaras ou nanosensores que são utilizadas na realização cirurgias e de exames, criando alternativas a procedimentos invasivos.

Em suma, a IoT contribuiu não só para um melhor controlo das patologias dos doentes, mas também para uma melhor resposta em caso de alerta.

Além de que, contribui ainda para o armazenamento e controlo de dados dos pacientes permitindo o rápido acesso aos mesmos levando a um diagnóstico mais preciso.

A IOT tem, para além das já referidas, outras utilizações como a medição da pressão arterial, através da conexão entre um monitor de pressão arterial e um sensor de IoT. Também é utilizada em sistemas de reabilitação, monitorização de oxigénio, e até no controlo remoto de cadeiras de rodas.²⁸

²⁶ NEELAM, 2022. Sankeerthana, Internet of Things in Healthcare, pág. 11

²⁷ NEELAM, 2022. Sankeerthana, Internet of Things in Healthcare, pág. 13

²⁸ NEELAM, Sankeerthana, 2022. Internet of Things in Healthcare, pág. 14

3.4.3 A aplicação da internet das coisas nas empresas

Como já é possível constatar, a internet das coisas tem aplicação em quase todos os ramos, no entanto, onde a mesma tem tido uma crescente utilização é no ramo empresarial.

Tal utilização, não só contribuiu para o aumento da produtividade, devido à redução de erros operacionais, como também para o controlo de stocks e de vendas.

A interligação dos dispositivos numa empresa possibilita um controlo administrativo mais eficaz uma vez que, com a utilização dessa tecnologia a empresa consegue controlar a produção de acordo com a procura do produto.

Acresce que, a ligação entre os dispositivos possibilita a emissão de uma grande quantidade de dados que são utilizados pela empresa na realização de estudos que prevejam cenários futuros e permitam a tomada de decisões adequadas.

Claro está que, a informatização de todos os dados disponíveis e a constante utilização de dados necessita de profissionais experientes em controlo de dados e segurança cibernética, no entanto, as vantagens da utilização desta inovação compensam os gastos despendidos em profissionais e equipamentos.

O acesso em tempo real dos dados emitidos permite ainda, o controlo da situação à distância, o que possibilita o aumento de criação de sucursais.

Acresce ainda que, esta tecnologia é ainda utilizada nas lojas físicas, com a implementação de sensores que monitorizam a quantidade de clientes que entram na loja, a quantidade de produtos vendidos e ainda advertem quando há a necessidade de reposição de algum produto.²⁹

A utilização de sensores pode ainda beneficiar a eficiência energética uma vez que, através de sensores de movimento, é possível desligar luzes e dispositivos que não estejam em utilização.

Para além disso, através da recolha de dados, é possível ainda controlar os dispositivos ao nível energético, no sentido de que possam funcionar apenas a determinadas temperaturas e constatar quais os equipamentos ou setores que despendem de mais energia, permitindo à empresa o controlo na utilização dos mesmos, e, ou, até troca-los por equipamentos mais eficientes energeticamente.³⁰

²⁹ MÚLTIPLOS, 2020. The Internet of things: Applications for business. The economist Intelligence Unit, pág. 22

³⁰ MÚLTIPLOS, 2020. The Internet of things: Applications for business. The economist Intelligence Unit, pág. 13.

Mais, esta tecnologia, em conjunto com a inteligência artificial permite a ajuda de um *Intelligent Personal Assistant* (IPA), um programa que tem como função a realização de tarefas requeridas pelo utilizador.

A título exemplificativo, estes programas, aplicados ao interesse da empresa, respondem a perguntas sobre a produção, produtos, clientes, quantidade de vendas, lucro, entre outras.

Hoje em dia, os IPAs têm ainda a capacidade de interagir através de comandos por voz.³¹

Por fim, para além das diversas utilizações da IoT na segurança, esta inovação já é utilizada em sistemas de controlo de acesso a empresas. Esta tecnologia, de controlo de acesso, funciona através da definição no software de quais as horas, dias e que funcionários necessitam de entrar na empresa, sendo enviados convites de entrada para os smartphones dos trabalhadores.

Posteriormente, quando o convite é utilizado pelo trabalhador, fornecedor ou vendedor, é enviada uma notificação ao administrador de forma a garantir o controlo de entrada dos mesmos.³²

3.4.4 A inteligência artificial e o covid-19

O coronavírus, denominado por SARS-CoV-2, foi diagnosticado pela primeira vez em dezembro de 2019 na cidade de Wuhan, localizada na China.

Desde então, o mundo foi assolado por uma crise pandémica de repercussões inimagináveis.

Ora, perante tal catástrofe, surgiu a necessidade de aliar as novas tecnologias e a saúde, não só, ao nível da criação de vacinação e desenvolvimento de maquinaria avançada de suporte básico de vida, mas também, no desenvolvimento de aplicações de controlo epidemiológico.

Debruçando-me agora sobre as aplicações de controlo e vigilância epidemiológica, as mesmas foram recomendadas na Recomendação (UE) 2020/518 de 8 de Abril de 2020 da CE, nomeadamente no que concerne às aplicações móveis e à utilização de dados de mobilidade anonimizados.

³¹ CARDOSO, Donato 2019. O uso de aplicações IoT.

³² MÚLTIPLOS, 2020. The Internet of things: Applications for business. The economist Intelligence Unit, pág. 14.

Neste sentido, é necessário analisar se a utilização de dados com informações pessoais e o controlo e vigilância das pessoas pode ser justificada pela saúde pública e o bem-estar social.³³

Portugal utilizou a app *StayAway Covid* que utilizou o sistema GAEN (*Google/Apple Exposur Notification*) possibilitando assim, a compatibilidade da mesma com sistema Android e iOS.

A App tinha como função, sinalizar e rastrear os infetados pelo vírus evitando assim o contágio. Esta, utilizou um sistema de proximidade de dispositivos por Bluetooth, assim os dispositivos eram conectados quando ultrapassavam a distância permitida, possibilitando à app rastrear os contactos mantidos.³⁴

O risco eminente que estas aplicações acarretam é a possibilidade de facilitar a identificabilidade pessoal ou o rastreamento da localização através dos smartphones. Para além disso, criam a “tentação” das autoridades públicas, privadas ou até hackers terem acesso a dados privados e localização da população.

Os direitos fundamentais aqui em causa são o direito à liberdade (de reunião, deslocação), igualdade, intimidade da vida privada e dignidade humana.³⁵

A Comissão Europeia apresentou, em abril de 2020, algumas instruções que deveriam ser atendidas nessas aplicações, sendo entre elas, a necessidade de as mesmas garantirem o respeito pelos direitos fundamentais, de optarem por medidas que permitam evitar o tratamento de dados sobre a localização, de assegurarem a cibersegurança, de eliminar os dados pessoais até 90 dias e de utilizarem dados anónimos em caso de infeção e necessidade de alertar pessoas que tenham estado próximas da pessoa infetada.³⁶

Para que estas aplicações pudessem ser analisadas à luz da ética e segurança da privacidade um grupo de peritos em IA da União Europeia, desenvolveu um conjunto de 133 questões para avaliação da confiança da IA. Essas questões são divididas por 7 categorias de preocupações éticas:

- Ação e supervisão humanas;

³³ ARAGÃO, Alexandra, 2020. Questões ético-jurídicas relativas ao uso de apps geradoras de dados de mobilidade para vigilância epidemiológica da Covid-19. Uma perspetiva Europeia, pág. 1.

³⁴ MENDES, Pedro, 2022. StayAway Covid: como funciona a app, Deco Proteste, consultável in <https://www.deco.proteste.pt/tecnologia/telemoveis/noticias/stayaway-covid-como-funciona-a-app>.

³⁵ ARAGÃO, Alexandra, 2020. Questões ético-jurídicas relativas ao uso de apps geradoras de dados de mobilidade para vigilância epidemiológica da Covid-19. Uma perspetiva Europeia, pág. 7.

³⁶ ARAGÃO, Alexandra, 2020. Questões ético-jurídicas relativas ao uso de apps geradoras de dados de mobilidade para vigilância epidemiológica da Covid-19. Uma perspetiva Europeia, pág. 9.

- Solidez técnica e segurança;
- Privacidade e governação dos dados;
- Transparência;
- Diversidade, não discriminação e equidade;
- Bem-estar societal e ambiental e,
- Responsabilização.

Posto isto, a IA deve ser, em suma, legal (assegurando o respeito pela lei), ética (respeitando princípios e valores éticos) e sólida (tanto no sentido técnico e social).³⁷

O certo é que, no que concerne à criação destas aplicações, as mesmas apenas foram desenvolvidas devido à impossibilidade de controlo do avanço epidemiológico e contribuíram para o controlo e vigilância de infetados, evitando assim a transmissão.

Acresce que, ainda que estas *apps* realizem um certo controlo, o certo é que a adesão a estas é facultativa e, para além disso, é o utilizador que tem de consentir a utilização dos seus dados. Desta forma, utilizador tem de consentir, não só o armazenamento dos dados, como também o envio dos mesmos para a entidade competente.

Neste sentido, evita-se a utilização destas aplicações para outros fins que não aqueles para os quais foram desenvolvidas.³⁸

Para além disso, tal como a *app StayAway Covid*, estas aplicações são cuidadosamente protegidas e apenas funcionaram durante a pandemia, tendo as mesmas sido retiradas dos sistemas e os dados alegadamente sido apagados.

Posto isto, considero que, ainda que exista inegavelmente riscos na utilização destas aplicações, o certo é que, a utilização desta permitiu evitar contágios e, conseqüentemente, mortes.

3.5 Desafios da internet das coisas

O avanço da tecnologia irá permitir num futuro não muito distante, a criação de cidade inteligentes, veículos conectados entre si, sistemas sustentáveis ambientalmente, indústria mais produtiva, sistemas de saúde rápidos e precisos, entre outras possibilidades.

³⁷ ARAGÃO, Alexandra, 2020. Questões ético-jurídicas relativas ao uso de apps geradoras de dados de mobilidade para vigilância epidemiológica da Covid-19. Uma perspetiva Europeia, pág. 10-12.

³⁸ ARAGÃO, Alexandra, 2020. Questões ético-jurídicas relativas ao uso de apps geradoras de dados de mobilidade para vigilância epidemiológica da Covid-19. Uma perspetiva Europeia, pág. 13.

No entanto, para que a IoT consiga desenvolver de forma rápida, eficaz e segura é necessário que a mesma ultrapasse variados desafios.

Desde logo, é necessário reduzir o preço de custo de produção de sensores, melhorar a conectividade rapidez e flexibilidade.

Acresce que, um estudo em 2018 constatou que apenas 36% das organizações empresariais utilizam a IoT para otimizar operações internas, o que para os especialistas é um número demasiado baixo, tendo em conta o potencial da IoT. Para além disso, de acordo com a *IoT Business Index*, maior parte das empresas ainda se encontram em fases embrionárias e quase um terço dessas ainda na fase de aplicação.

Os principais obstáculos que a IoT terá de ultrapassar serão a segurança, privacidade, regulação e as infraestruturas digitais.

No que concerne à segurança, quantos mais objetos estiverem conectados com a internet, mais dados estarão em circulação, maior será a probabilidade de os *hackers* entrarem nos sistemas inteligentes.

Para se poder evitar isso, é necessário estabelecer normas de utilização e práticas entre utilizadores e vendedores de forma a existir constante informação e transparência.

Qualquer atividade de vigilância deve ser sempre evidente de forma a construir segurança e confiança entre o que vigia e o que é vigiado.

Outro conselho, é as empresas apostarem na segurança dos equipamentos e incentivarem os trabalhadores a alterar palavras-passe e dados de acesso regularmente.

Um outro desafio, é a criação de legislação que permita a segurança tanto dos utilizadores como dos manipuladores de dados da IoT.

A IoT não consegue ser subsumível em qualquer legislação devido ao facto de englobar variados produtos, serviços, práticas, processos e tecnologias.³⁹

Para que isso seja possível, é necessário assegurar a existência de legisladores especializados na área tecnológica, e que, a legislação criada seja virada para o futuro e harmonizada entre os vários países. Dessa forma, será possível a criação de legislação adequada aos desafios da IoT, permitindo o avanço e desenvolvimento desta, evitando assim a existência de “paraísos legislativos”.⁴⁰

³⁹ MÚLTIPLOS, 2020. The Internet of things: Applications for business. The economist Intelligence Unit, pág. 33

⁴⁰ MÚLTIPLOS, 2020. The Internet of things: Applications for business. The economist Intelligence Unit, pág. 35.

Por fim, um outro desafio é a necessidade de criação de infraestruturas preparadas para a IoT. Para que a IoT consiga se desenvolver necessita de upgrades à internet 4G de forma a que a utilização da mesma seja realizada forma mais rápida, eficaz, flexível e de baixa densidade.

Acresce que, o desenvolvimento da IoT implica um custo muito elevado na criação e manutenção de infraestruturas, o que impossibilita a implementação desta tecnologia em países de baixos recursos.

A solução para este problema passa, pelo governo e o setor privado, encetarem esforços para reduzir o custo da IoT e o alargamento da rede de 5G.

Para além disto, a IoT é uma tecnologia exigente ao nível cognitivo pelo que será ainda preciso o investimento, por parte do setor privado e até público, em profissionais capazes de lidar com tratamento de dados, hardware e segurança cibernética.⁴¹

4. A ligação entre a internet das coisas e a inteligência artificial

O avanço tecnológico está a alterar os novos padrões de comportamento e estes dois pilares da inovação são uma parte importante em todo o processo. É, através destas, que o mundo se encontra mais conectado e os dispositivos estão cada vez mais autónomos e interligados.

A internet das coisas é uma área relativamente recente enquanto que a IA já remonta aos anos 40 e 50.

A Internet das coisas, tal como já mencionado anteriormente, diz respeito à interligação de dispositivos com a rede e por isso preocupa-se com a questões de conectividade, concorrência, entre outros. Já a preocupação da inteligência artificial versa em questões analíticas de dados, linguagem, estatística e até mesmo um pouco de neurociência.

A IoT e a IA podem ser implementadas separadamente ou conjuntamente. Desta forma, há a possibilidade de os dados resultantes da IoT serem utilizados pela IA para análise de situações e a tomada de decisões. Esta simbiose dependerá do nível de inteligência do sistema de IoT. Se se tratar de um sistema não inteligente de IoT, este não será capaz de se adaptar ou desenvolver a partir dos dados recebidos. Por outro lado, se se tratar de um

⁴¹ MÚLTIPLOS, The Internet of things: Applications for business, The economist Intelligence Unit, 2020, pág. 36.

sistema de IoT inteligente, este irá conter IA e será capaz de aprender e desenvolver a partir dos dados recebidos. Os melhores exemplos desta junção são os assistentes de voz como a Alexa, Siri ou a Google e Robots⁴² como a Sophia, entre outros.⁴³

A análise preditiva é um exemplo da utilização conjunta da Iot e da IA. Consiste na utilização de dados, algoritmos estatísticos e técnicas de *machine learning* para identificar a probabilidade de resultados futuros, a partir de dados históricos.

O número de dados, o desenvolvimento tecnológico, a utilização facilitada dos softwares, e a competitividade empresarial torna esta tecnologia muito útil

Aliás esta tecnologia tem variadas utilidades como a detecção e prevenção de fraudes através da combinação de métodos analíticos, otimização de campanhas de marketing, melhoramento de operações económicas e empresariais e para a redução de risco na análise de possibilidade de atribuição de crédito.

Esta tecnologia, tem como finalidade a extração das decisões mais benéficas para o utilizador através de uma dedução do que poderá ocorrer no futuro.

Com o avanço da tecnologia e o aumento da competitividade empresarial a análise preditiva deixou de ser apenas utilizada por matemáticos e estatísticos e passou a ser utilizada por especialistas em linhas de negócios.

⁴² A robótica, é um ramo tecnologia que se dedica à construção de sistemas mecanizados. Esta ciência cria sistemas compostos por máquinas e partes mecânicas, controladas por circuitos integrados e circuitos eléctricos programados para a realização de determinados atos.

O início da construção de robôs remonta ao século XX quando George Devol começou a desenvolver robôs indústrias com o intuito de aumentar e melhorar a produtividade fabril.

Ainda no mesmo espaço temporal, Isaac Asimov, escritor e bioquímico, lançou a coletânea “Eu robô” com a obra “O mentiroso” onde cria o termo “robótica” e ainda expõe as Leis da Robótica no campo da ficção-científica:

“- Um robô não pode ferir um ser humano, ou por inação, permitir que um humano seja ferido.

- Um robô deve obedecer às ordens dadas por humanos, exceto quando isto conflitar com a Primeira Lei.

- Um robô deve proteger sua própria existência, a menos que isto conflite com a

Primeira ou a Segunda Lei.” OTTONI, André Luís Carvalho. 2010. Introdução à Robótica. Universidade São João Del-Rei, Brasil, pág. 2.

Este campo tecnológico começou a ser cada vez mais desenvolvido, fruto dos crescentes recursos tecnológicos possibilitando, não só, mas também, às empresas o aumento e desenvolvimento da produtividade, redução de custos e ainda a proteção de operariado em trabalhos de alto risco.

Para além disso, a robótica tem sido utilizada por todo o mundo, principalmente pelo Japão, para minimizar o risco e preservar o ser humano em atividades de risco, na reintegração de seres humanos com alguma deficiência ou redução de capacidades motoras, em sistemas de vigilância e até em testes operativos. OTTONI, André Luís Carvalho. 2010. Introdução à Robótica. Universidade São João Del-Rei, Brasil, pág. 1.

⁴³ GAYANTHA M.H.; KITHULWATTAB; W.M.C.J.T. RATHNAYAKA, R.M.K.T. 2022. The Interconnection of Internet of Things and Artificial Intelligence: A Review, pág. 59.

A IoT permite a obtenção de dados em massa sendo esses armazenados alimentando assim a BD⁴⁴. Estes dados, são sobretudo, informações genéricas sobre comportamentos humanos. Aí é possível descobrir tendências e inclinações humanas.⁴⁵

Combinando essas vertentes, o computador molda-se, aprendendo a inclinação das informações recolhidas e transformando a informação em benefício do seu programador.

Este processo de geração, análise e criação de *insights* pode ser aproveitado por diversos setores, como o industrial, tecnológico, comercial, entre outros.

Certas inovações apenas foram possíveis graças a estas tecnologias pois, essa combinação permitiu a realização de mecanismos interligados e automatizáveis.

4.1 As aplicações da internet das coisas e da inteligência artificial

Os principais setores derivados da junção destas duas tecnologias são o da agricultura, saúde e empresarial.

No setor da agricultura, os maiores desafios eram o controlo de água, pesticidas, ervas, e de doenças nas plantas. Todos estes problemas conseguem ser resolvidos através da simbiose destas tecnologias. A utilização da IoT permite a interligação entre os variados sensores e a IA possibilita a análise de gastos, a previsão de cenários futuros e o desenvolvimento de novas estratégias e ações mais benéficas. A automatização destas tecnologias contribui para a manutenção da fertilidade do solo.

No setor da saúde, a IA e a IoT têm sido um grande contributo para o diagnóstico e tratamento de doenças. O *deep learning*, aliado à IoT, possibilita a aprendizagem pela máquina de novos métodos de cura mais eficazes, reduzindo assim o tempo tanto de diagnóstico como de elaboração da cura.

No entanto, a utilização destas tecnologias pode consubstanciar um perigo ao nível da segurança uma vez que, a utilização de dados pessoais dos utentes constitui um grave perigo à privacidade dos mesmos.⁴⁶

⁴⁴ O termo BD na tradução literal da palavra significa grandes dados, ou seja, traduz-se num grande conjunto de dados. A utilização em massa de dispositivos tecnológicos levou a que uma grande quantidade de dados fosse produzida diariamente. Como resultado, tornou-se necessário desenvolver um modelo de armazenamento de dados que permitisse a organização e análise dos mesmos. Um exemplo de BD é, entre outros, o Youtube. STEPHENS-DAVIDOWITZ Seth, 2018 Everybody Lies, pág. 36.

⁴⁵ GAYANTHA M.H.; KITHULWATTAB; W.M.C.J.T. RATHNAYAKA, R.M.K.T. 2022. The Interconnection of Internet of Things and Artificial Intelligence: A Review, pág. 212.

⁴⁶ GAYANTHA M.H.; KITHULWATTAB; W.M.C.J.T. RATHNAYAKA, R.M.K.T. 2022. The Interconnection of Internet of Things and Artificial Intelligence: A Review, pág. 54

No setor empresarial, o maior objetivo é a utilização destas tecnologias no sentido do crescimento e desenvolvimento da empresa.

A análise preditiva e a facilidade de tomada de decisões possibilitam às empresas resolver problemas e desenvolver novas estratégias de crescimento. A recolha de dados de, por exemplo, stocks e vendas permite ao sistema deduzir quais as mercadorias que devem ou não ser vendidas, alterações de preços, entre outros. Para além disso e aliado à blockchain⁴⁷ será possível ao empresário prever comportamentos e padrões de forma a desenvolver o seu modelo de negócio ⁴⁸

5. A afetação destas tecnologias no direito da privacidade e intimidade e a emergência na criação de uma regulação inteligente

O termo “privacidade” é oriundo do latim “*privatus*” que significa privacidade, particular, próprio.⁴⁹

⁴⁷ A blockchain como o nome indica é uma corrente de blocos que contem dados. Trata-se de uma corrente uma vez que esses dados encontram-se correlacionados e presos entre si.

Ou seja, trata-se de um encadeamento de dados inseridos sendo criado um acesso direto aos mesmos entre duas partes, sem interferência de terceiros. Esta junção de blocos constitui uma forma rápida e segura na comunicação entre duas partes, contribuindo para a confiança e consenso nas transações realizadas por entidades.

À medida que novos blocos são incorporados, de forma linear e cronológica, a blockchain vai aumentando. A cada bloco adicionado é atribuído um “hash”, operação criptográfica que produz identificadores únicos e irrepetíveis a partir de uma determinada informação.

Estas funções têm como objetivo principal codificar dados para assegurar a autenticidade dos dados, armazenar senhas com segurança e até assinar documentos eletrónicos.

Uma característica importante na blockchain é que uma vez inserida informação (data), a mesma torna-se imutável, não podendo ser apagada. SHINO, K.; GANESH, D. C. 2020. Advanced Applications of Blockchain Technology, pág. 75.

Recentemente surgiu o interesse em aliar a Blockchain à IOT graças ao facto de a blockchain ser à prova de adulteração. Ou seja, o facto de os blocos serem ligados através de um “hash” isso contribui para uma permanente transação e comunicação dos dados de forma segura.

Acresce que, uma das características da Blockchain é a sua transparência, permitindo aos seus utilizadores verificarem facilmente o histórico das transações efetuadas.

Mais, a tecnologia presente na Blockchain permite que as transações sejam realizadas de forma anónima. Neste sentido, se cada transação for realizada com uma chave pública diferente, cada transação nova será ligada a um acesso diferente, tornando assim difícil localizar o criador do bloco.

Acresce ainda que, uma outra característica é a possibilidade da utilização da Blockchain na elaboração e desenvolver contratos. Estes contratos inteligentes “smart contracts” traduzem-se basicamente em condições predefinidas são aceites sem a necessidade de intermediários.

No entanto, apesar de parecer ser uma boa aposta a junção da Blockchain com a IOT a verdade é que, existem in.ºs problemas que dificultam a junção das mesmas. Alguns dos problemas associados são, para além de vários outros, o alto consumo de recursos, capacidade de expansão e o lento Proc. de transações. DEDEOGLU V. et al., 2020, The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms, p. 59.

⁴⁸ GAYANTHA M.H.; KITHULWATTAB; W.M.C.J.T. RATHNAYAKA, R.M.K.T. 2022. The Interconnection of Internet of Things and Artificial Intelligence: A Review, pág. 59

⁴⁹ VEIGA, Adélcia, 2020. Proteção de dados: O direito à privacidade na era digital, pág. 34.

Ora, desde logo, pode-se constatar que o significado de privacidade é muito amplo apresentando uma grande quantidade de significados. No entanto, autores como Samuel Warren e Louis Brandeis consideram a privacidade como “o direito à solidão, à intimidade da vida familiar e privada, ao anonimato e à distância em relação a estranhos.”⁵⁰

No mesmo sentido, Canotilho e Moreira definem privacidade como “o direito a impedir o acesso de estranhos a informação sobre a vida privada e familiar e o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem.”

Já Paulo Mota Pinto afirma que “a defesa da privacidade visa evitar ou controlar a tomada de conhecimento ou a revelação de informação pessoal, dos factos, comunicação ou opinião relacionados com o individuo, o que é razoável esperar que ele encare como íntimo ou pelo menos confidencial e que, por isso, queira excluir ou pelo menos restringir a sua circulação”⁵¹

Acresce que, a privacidade tem de ser entendida em dois sentidos, no sentido de interditar o acesso à vida privada e no sentido de impedir a divulgação sobre essa vida privada. Ora, hoje em dia, é necessário proteger de igual modo esta bidimensionalidade da privacidade.⁵²

Pelo exposto, é possível constatar que a privacidade é intrínseca à natureza da pessoa humana e que a sua definição remete tão só ao próprio individuo, sendo algo pessoal, de acesso interdito a terceiros.

Há quem utilize os conceitos privacidade e intimidade como sinónimos, no entanto, estes conceitos possuem definições diferentes.

Intimidade deriva do termo “intimus” e pode ser definido como aquilo é interior, alheio a terceiros.

Tércio Sampaio Ferraz Jr. refere que a “intimidade é o âmbito do exclusivo que alguém reserva para si, sem nenhuma repercussão social, nem mesmo ao alcance de sua vida privada, que, por mais isolada que seja, é sempre um viver entre os outros (na família, no trabalho, no lazer em comum (...)) Nestes termos, é possível identificá-la: o diário íntimo, o segredo sob juramento, as situações de pudor pessoal, o segredo íntimo cuja publicidade constrange.”⁵³

⁵⁰ VEIGA, Adélcia, 2020. Proteção de dados: O direito à privacidade na era digital, pág. 35.

⁵¹ VEIGA, Adélcia, 2020. Proteção de dados: O direito à privacidade na era digital, pág. 36.

⁵² CANOTILHO, J. G; MOREIRA, V, Constituição da República Portuguesa Anotada, 2007, pág.

⁵³ ÀVILA, Ana Paula Oliveira; WOLOSZYN, André Luís, 2017. A tutela jurídica da privacidade e do sigilo na era digital, in Revista de Investigações Constitucionais, pág. 174

Ora, a privacidade e a intimidade distinguem-se pela forma de comunicação, uma vez que, a privacidade, ao contrário da intimidade, pode ser caracterizada pela comunicação com terceiros.

Como forma de proteção da privacidade humana foram criadas algumas teorias de forma a se determinar o nível de proteção da privacidade.

Fazendo uma análise a todas as teorias e pensamentos criados, aquelas que suscitaram maior interesse foram a teoria das esferas e a teoria dos círculos concêntricos.

A teoria das esferas, segundo Marcelo Novelino, é dividida em quatro espécies, sendo a primeira a esfera da publicidade, a segunda a esfera pessoal, a terceira a esfera privada e a quarta a esfera íntima.⁵⁴

Na esfera da publicidade, o sujeito permite a publicidade de atos que pratica, seja expressamente, quando por exemplo, decide trabalhar como pivô televisivo, ou tacitamente quando atende a um local público. Nesta, estão incluídos os atos que o sujeito deseja praticar e tornar públicos.⁵⁵ Esta esfera, segundo esta teoria, não é alvo de proteção constitucional.

Já na esfera pessoal, encontram-se as relações com terceiros, sem que haja consentimento na divulgação como por exemplo, as relações comerciais do sujeito.

Por outro lado, na esfera privada já se encontram os factos de maior proximidade emocional cujo sujeito não pretende que se divulguem.

Por fim, a esfera íntima é a mais profunda de todas elas, aquela que retrata o ser mais íntimo da pessoa, o mundo intrapsíquico. São as informações mais restritas do indivíduo, aquelas cujo acesso é interdito.⁵⁶

A teoria dos Círculos Concêntricos, criada na Alemanha em 1950, com base na doutrina de Heinrich Hubmann e Heinrich Henkel, tem como objetivo a diferenciação entre o caráter público e privado, a intimidade e o segredo.

⁵⁴ CUNHA, Tiago Barros; FILHO, Adalberto Simão, 2017. A teoria dos círculos concêntricos e a preservação da privacidade humana no registo civil das pessoas naturais in V Congresso brasileiro de Proc. coletivo e cidadania, pág. 266.

⁵⁵ CUNHA, Tiago Barros; FILHO, Adalberto Simão, 2017. A teoria dos círculos concêntricos e a preservação da privacidade humana no registo civil das pessoas naturais in V Congresso brasileiro de Proc. coletivo e cidadania, pág. 267.

⁵⁶ CUNHA, Tiago Barros; FILHO, Adalberto Simão, 2017. A teoria dos círculos concêntricos e a preservação da privacidade humana no registo civil das pessoas naturais in V Congresso brasileiro de Proc. coletivo e cidadania, pág. 268.

Esta teoria possui três círculos, sendo que o maior inclui o direito à privacidade em sentido estrito (*privatsphäre*), o do meio o direito à intimidade (*vertrauenssphäre*) e o central o direito ao segredo (*geheimphäre* ou *vertraulichkeitssphäre*).

Esta teoria ganhou o nome de círculos concêntricos devido ao facto de ser representada em círculos. O da esfera privada encontra-se na ponta, o da esfera do segredo no núcleo, e o da esfera íntima entre os dois.

Tal como referido acima, a esfera da vida privada abrange as relações interpessoais, que se podem tornar públicas.

Neste sentido, Frota refere que “extremidade da vida particular mais perceptível ao observador externo e menos reveladora da personalidade de cada um, serve de palco à faceta material da esfera privada e às relações interpessoais perfunctórias, ilustradas pelas amizades circunscritas ao coleguismo. Nessa seara perfilam quer noções ligeiras sobre a rotina diária do indivíduo, quer os dados indicativos do seu património.”⁵⁷

Já na esfera da intimidade, existe uma necessidade de interditar o acesso de certas informações ao público, apenas sendo divulgadas algumas informações a pessoas mais próximas do sujeito.

Frota menciona ainda que, “No bojo da esfera privada está contida a esfera da intimidade (*Vertrauensphäre*) ou esfera confidencial (*Vertraulichkeitssphäre*.) Dela participam somente aquelas pessoas nas quais o indivíduo deposita certa confiança e com as quais mantém certa intimidade. Fazem parte desse campo, conversações ou acontecimentos íntimos, dele estando excluídos não apenas o público em geral, como é óbvio; bem assim, determinadas pessoas, que privam com o indivíduo num âmbito mais amplo”⁵⁸

Por último, existe a esfera do segredo, núcleo mais profundo da pessoa humana, cujo acesso a qualquer informação é vedada a terceiros.

Ora, pode-se referir que, para se conseguir distinguir a esfera privada da íntima é necessário verificar a quantidade de pessoas que tiveram acesso à informação e quais as suas relações com o sujeito.⁵⁹

⁵⁷ FROTA, Hidemberg Alves da, 2007. A proteção da vida privada, da intimidade e do segredo no Direito brasileiro e Comparado in *Anuário de Derecho Constitucional Latinoamericano*,, pág. 463.

⁵⁸ CUNHA, 2017. Tiago Barros & Filho, Adalberto Simão, A teoria dos círculos concêntricos e a preservação da privacidade humana no registo civil das pessoas naturais in *V Congresso brasileiro de Proc. coletivo e cidadania*, pág. 271.

⁵⁹ CUNHA, Tiago Barros; FILHO, Adalberto Simão, 2017. A teoria dos círculos concêntricos e a preservação da privacidade humana no registo civil das pessoas naturais in *V Congresso brasileiro de Proc. coletivo e cidadania*, pág. 272.

A teoria dos círculos concêntricos parece ser simples à primeira vista, no entanto, a sua aplicabilidade é complexa quando existe a necessidade de delimitar as esferas.

A privacidade e a tecnologia sempre andaram de “mãos dadas”, no entanto, hoje em dia, arrisco-me a afirmar que uma das mãos aperta a outra. O número de sensores tem aumentado significativamente e, tal como já mencionado acima, a ligação à rede de dispositivos do quotidiano permitiu a quase simbiose entre a vida humana e a tecnologia.⁶⁰

Ora, a pergunta que não quer calar será sempre a mesma: onde fica a privacidade do ser humano quando uma infraestrutura de milhares de milhões de sensores trata, armazena e transfere dados a todo o momento?⁶¹

Esta irá inevitavelmente afetar cada vez mais a privacidade dos indivíduos, através da utilização de dados pessoais, seja pela invasão não autorizada nos mesmos, seja pela utilização e partilha daqueles.

Ora, o desenvolvimento da era tecnológica acaba por desenvolver mais rápido que o processo de proteção dos direitos, o que cria esta desigualdade.⁶²

Claro que, a questão não se cinge apenas à IoT como principal ameaça à privacidade, uma vez que, a arma torna-se mais letal quando combinada com a inteligência artificial e, conseqüentemente, com o *machine learning* e o *BD*. Neste quadro, para além da recolha massiva de dados, dá-se ainda o tratamento e análise dos mesmos, o que possibilita a extração de informações privadas a partir de dados aparentemente “inofensivos”. Ou seja, com estas tecnologias dá-se a possibilidade de realizar a chamada “fusão de sensores”, um conceito que se caracteriza pela junção de variados dados de fontes diferentes de forma a possibilitar a aferição de novos dados que não seriam descobertos de outra forma.⁶³

⁶⁰ MILLER Michael, 2015. The internet of things - How Smart Tvs, Smart Cars, Smart Homes and Smart Cities are Changing the World, Pearson Education, Indianapolis, pág. 27 (versão e-book).

⁶¹ Neste sentido, GONÇALVES Maria Eduarda, quando afirma que, “a vida privada vai para além daquilo que cada indivíduo faz em casa, já que inclui também o direito à tranquilidade, à solidão, o direito de comunicar com os outros em segurança e confidencialidade” in Direito da Informação. 2023. Novos direitos e formas de regulação na sociedade da informação, Almedina, Coimbra, pág. 83.

⁶² Neste sentido, Paulo José Costa Júnior refere que a: “a revolução tecnológica promoveu um Proc. de corrosão das fronteiras da intimidade, que a devassa da vida privada tornou-se mais aguda e inquietante (...) avalia que esta revolução avança, muitas vezes, desprovida de diretrizes morais, acarretando uma progressiva desses direitos fundamentais numa escala de assédio crescente.” ÀVILA , A. O.; WOLOSZYN, A. L., 2017, A tutela jurídica da privacidade e do sigilo na era digital. Revista de Investigações Constitucionais, pág. 175.

⁶³ PEPPET R. Scott, in Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, pág. 120. Como explica este autor: "Put simply, in a world of connected sensors, “everything may reveal everything.” Sensor data are so rich, accurate, and fine-grained that data from any given sensor context may be valuable in a variety of - and perhaps all- other economic or information contexts.”

Uma das consequências desta fusão de dados é a dificuldade na anonimização dos utilizadores dos dispositivos IoT e agora também dos de AI.⁶⁴ Ou seja, ainda que os dados sejam inicialmente anonimizados é possível voltar a criar o perfil do indivíduo.⁶⁵ A conexão entre diversos dispositivos utilizados pelo utilizador permite a correlação de hábitos praticados pelo mesmo possibilitando, assim, a criação de um padrão de identificação.

A título exemplificativo, temos os smartphones que, ainda que possuam aplicações com dados encriptados, a não encriptação de uma outra, de utilização semelhante, permite por exemplo aferir a localização do utilizador.⁶⁶

Parece inofensivo, no entanto, atualmente, um dos negócios mais rentáveis tem como atividade o conhecimento de hábitos e comportamentos de pessoas. Daí a vulgarização de termos como *data mining*, *data analytics* e *data brockreage*⁶⁷, entre outros.

Estas ferramentas alimentam, por exemplo, o chamado *marketing* direcionado que permite a formatação de escolhas e comportamentos, sendo as mesmas orientadas nos interesses das empresas.

Para além do já enunciado, existe outra consequência da utilização descontrolada destas tecnologias que, conseqüentemente, significa uma violação do direito à privacidade, sendo ela a falta de segurança.

No que concerne à segurança é possível afirmar que, os dispositivos de IoT e IA apresentam variadas fragilidades de segurança, o que possibilita o ataque de hackers.

Neste sentido, é necessário a criação de mecanismos que ajudem a controlar esta introdução abrupta das novas tecnologias na vida privada do ser-humano.

⁶⁴ Neste sentido, Grupo de Trabalho do Artigo 29º para a Proteção de Dados, Parecer 05/2014 As principais técnicas de anonimização de dados pessoais são a aleatorização e ageneralização, A anonimização é um tratamento de dados que visa evitar a identificação. “As principais técnicas de anonimização de dados pessoais, designadamente a aleatorização – consiste na alteração da veracidade dos dados na intenção de eliminar a ligação com a pessoa – e a generalização, que passa pela alteração da escola ou ordem de grandeza dos atributos titulares dos dados.”

⁶⁵ Como afirma PEPPE R. Scott: “sensor data capture such a rich picture of an individual, with so many related activities, that each individual is a sensor-based dataset is reasonably unique” , *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, pág. 130.

⁶⁶ PEPPE R. Scott, “sensor data capture such a rich picture of an individual, with so many related activities, that each individual is a sensor-based dataset is reasonably unique”, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, pág. 131.

⁶⁷ Databrokers traduzem-se em corretores de dados que compram e recolhem informação dados de diferentes fontes de forma a desenvolver perfis de pessoas. Depois estes perfis são vendidos a empresas que queiram melhorar o direcionamento dos seus produtos e serviços. “Definição de perfis e decisões individuais automatizadas no Regulamento Geral sobre a Proteção de dados” in CORDEIRO Menezes A., PERESTRELO de Oliveira, D. Pereira Duarte, 2019. *Fintech – Novos estudos sobre a tecnologia financeira*, pág. 71.

Por isso, ainda que exista a tentativa de manter os dados em sigilo assegurada por textos constitucionais, europeus e internacionais, o certo é que, tal é uma tarefa cada vez mais difícil num sistema global digital.

6. A proteção constitucional da privacidade

A CRP consagra vários direitos pessoais, como o direito à identidade, livre personalidade, à reserva da intimidade privada e familiar, o direito à proteção contra quaisquer formas de discriminação, ao bom nome e reputação, imagem, palavra, entre outros. Tal consagração, demonstra a importância atribuída pelo Estado aos direitos pessoais e à sua proteção.

A consagração do direito à privacidade na CRP foi inicialmente concebida com base na proteção da violação desse direito na forma mais genérica.

Acontece que, com o avanço das eras e principalmente com o desenvolvimento da tecnologia, o direito à privacidade foi sofrendo mutações dificultando a tarefa ao legislador.

Uma vez que, se trata de um direito em constante mutação torna-o instável, o que levou a uma resistência por parte do legislador português em alterar a legislação.

Ainda que muitas constituições estrangeiras já consagrem direitos do indivíduo face à informática, a constituição portuguesa ainda se encontra com uma lacuna nesse aspeto.

O nosso ordenamento jurídico consagra a chamada “dicotomia protecional” da privacidade, o que se torna visível nos art. 26º e 35º da CRP.⁶⁸

O art. 26º constitui, para Jorge Miranda e Rui Medeiros, “expressão direta do postulado básico da dignidade humana que a Constituição consagra logo no art. 1º, como valor básico logicamente anterior à própria ideia de Estado de Direito democrático e que constitui a referência primeira em matéria de direitos fundamentais.”⁶⁹

Constitui ainda uma “pedra angular” na demarcação dos limites ao exercício dos outros direitos fundamentais”, como o direito à liberdade de expressão, informação, imprensa e meios de comunicação social, liberdade que só podem ser interpretadas tendo em atenção o art. em causa.

⁶⁸ MIRANDA, Jorge; MEDEIROS, Rui, 2010, Constituição Anotada Portuguesa, pág. 606.

⁶⁹ MIRANDA, Jorge; MEDEIROS, Rui, 2010, Constituição Anotada Portuguesa, pág. 607.

Ao se analisar o artigo supramencionado constata-se que, para além do direito à privacidade, também este artigo apresenta uma dicotomia.

Em primeiro lugar, este artigo inclui a proteção de setes direitos diferentes, o direito à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação.

Já em segundo lugar, na epígrafe do artigo, lê-se “Outros direitos pessoais”, o que parece remeter para os direitos à vida e à integridade física, presentes nos art. 24º e 25º. que antecedem ao artigo em causa.

Neste artigo, o legislador pretendeu a consagração ao desenvolvimento da personalidade, sendo considerado como um reflexo constitucional do direito à reserva da intimidade da vida privada.

O art. 26º implementa ainda, a obrigação ao Estado de respeitar os referidos direitos e criar leis que estabeleçam garantias efetivas contra o objetivo principal, a obtenção e utilização abusivas, ou contrárias à dignidade, de informações relativas às pessoas e famílias.

Concretamente o direito à reserva da intimidade da vida privada e familiar é um dos que tem maior alcance prático, ainda que essa abrangência não se compare à jurisprudência americana.

Neste caso, este direito engloba não só o direito à objeção à divulgação da vida privada, mas também o direito à oposição da investigação a vida privada.

No entanto, este direito hoje em dia encontra-se ainda na possibilidade de gestão pelo cidadão das informações que lhe dizem respeito, permitindo o controlo do acesso, utilização e divulgação de dados, quando se aperceba que o emprego dos mesmos não ocorreu nos moldes por ele consentidos, beneficiado ainda do direito ao conhecimento, retificação e eliminação dos dados.⁷⁰

Neste seguimento, o n.º 2 do art. 26º estabelece ainda as “garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.”

O problema que este direito suscita é, tal como referido no ponto anterior, delimitação da esfera privada, íntima e social. Para além disso, esta delimitação é muito volátil, diferindo de pessoa para pessoa, e de momento para momento.

⁷⁰ MIRANDA, Jorge; MEDEIROS, Rui, 2010, Constituição Anotada Portuguesa, pág. 621

A complexidade do juízo de proporcionalidade agravou-se com o facto de existirem cada vez mais dispositivos tecnológicos de obtenção de informação da vida privada das pessoas.

A solução passa por utilizar a autonomia pessoal como critério principal do princípio da proporcionalidade.⁷¹

A tutela das relações da esfera privada ocorre ainda, nas relações entre particulares, como por exemplo, nas relações laborais, e ainda para as pessoas coletivas, como por exemplo, no *know-how*, ajustando-se às relações comerciais da mesma.⁷²

Acresce que, este direito não é imutável principalmente quando se encontra em jogo a busca pela verdade material, encontrando-se constantemente em conflito com outras liberdades e garantias como o caso da liberdade de expressão e comunicação (37º e 38º da CPR) e o direito de informação (268º, n.º 1 e 2 CRP).⁷³

O art. 35º também procede à proteção do direito de privacidade, no entanto esta proteção é realizada com o intuito de criar uma barreira ao tratamento informatizado de dados, fazendo transparecer uma espécie de direito à autodeterminação informacional moderno.

Na sua versão originária, este artigo apenas retinha três números, sendo que o primeiro contemplava o direito à informação, o acesso do titular aos dados pessoais, o direito à retificação, e à atualização de dados.

Já no n.º 2 estava presente, tal como agora, a proibição de tratamento de dados sensíveis, relativos a convicções políticas, fé religiosa e vida privada, tendo esta lista sido aumentada posteriormente.

Por fim, o n.º 3 continha a proibição de instituição de um único número nacional para cada cidadão.⁷⁴

Ao longo dos tempos, foram realizadas algumas alterações ao art. 35º despoletadas pelo avanço tecnológico.

⁷¹ MIRANDA, Jorge; MEDEIROS, Rui, 2010, Constituição Anotada Portuguesa, pág. 621.

⁷² MIRANDA, Jorge; MEDEIROS, Rui, 2010, Constituição Anotada Portuguesa, pág. 624.

⁷³ MIRANDA, Jorge; MEDEIROS, Rui, 2010, Constituição Anotada Portuguesa, pág. 625.

⁷⁴ CASTRO, Catarina Sarmiento e, 2016, 40 anos de “Utilização da Informática” - o artigo 35.º, pág.

Com a constituição deste artigo aprovado em 1976, a Constituição foi pioneira na consagração de direitos que, tal como a epígrafe indica, provenham da utilização informática.⁷⁵

Portugal, Suécia, Eslovénia, Hungria e Polónia são alguns países que consagram expressamente a proteção de dados pessoais, ao contrário Itália e Alemanha que consideram que a proteção de dados pessoais não deve de ter autonomia em relação à tutela concedida à intimidade da vida privada.⁷⁶

Não obstante o referido, o reconhecimento deste direito, o conteúdo e os limites transcendem a todos, fruto da subscrição da Convenção do Conselho da Europa sobre a proteção de dados, transpondo para as ordens internas o estabelecido pela Diretiva n.º 95/46/CE e, por fim o RGPD.

O direito constitucional alemão tem a organização dos dados construído à volta de um direito à autodeterminação informativa, a partir da consideração conjunta do direito geral de personalidade e do princípio da dignidade humana.

Esta autodeterminação informativa divide-se, segundo a jurisprudência alemã, em duas vertentes, uma delas referente à liberdade de movimentos do sujeito e a outra ao desenvolvimento da personalidade de cada pessoa no âmbito social.

O tribunal constitucional alemão considerou que, a tutela dos dados pessoais enquadra-se num direito à autodeterminação, existindo doutrina alemã que considera que este direito pertence à tutela do direito de imagem.

A previsão constitucional Italiana também não prevê uma previsão constitucional nesse sentido, contudo alguma doutrina do país tentou uma aproximação ao direito à reserva da vida privada em sentido amplo.

Tal como referido acima, o art. 35º consagra um direito à autodeterminação informativa, uma imprescindibilidade protecional projetada logo no final dos anos 60, pelo Conselho da Europa, uma vez que entenderam ser necessário uma maior proteção à defesa da vida privada através da CEDH, no seu art. 8º, ou a Declaração Universal dos Direitos do Homem com o art. 12º que refere que: “Ninguém sofrerá intromissões arbitrarias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra

46 ⁷⁵ CASTRO, Catarina Sarmiento e, 2016, 40 anos de “Utilização da Informática” - o artigo 35.º, pág.

⁷⁶ MIRANDA, Jorge; Medeiros, Rui, 2010, Constituição Anotada Portuguesa, pág. 784

e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei”.⁷⁷

Com a evolução tecnológica, “o alargamento das possibilidades de recolha e armazenamento de dados relativos ao cidadão (...) a facilidade e a velocidade de acesso e cruzamento de dados”, justificam mais que nunca a necessidade de tutelar a privacidade do indivíduo”.⁷⁸

O direito à autodeterminação informacional é a capacidade do indivíduo de controlar o acesso aos seus dados pessoais, mas também é, a possibilidade de o mesmo, querendo, dispor dos mesmos.

Este direito subdivide-se em três direitos, sendo um deles o direito ao não tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, religiosa, vida privada e origem étnica (n.º 3), o direito à interdição de acesso de dados pessoais a terceiros (n.º 4) e por fim o direito ao acesso aos dados informatizados.

Para além disso, o n.º 1 do art. 35º contém ainda outros direitos presentes como o direito de exigir a retificação e atualização de dados informatizados do cidadão e o direito de conhecer a finalidade a que se destinam os seus dados.

Ora, o art. supramencionado tem, por um lado, uma dimensão negativa no sentido em que permite a recusa por parte do cidadão ao tratamento de certos dados e, por outro, uma dimensão positiva na medida em que, é atribuído um controlo dos próprios dados ao cidadão constituindo assim o *Habeas Data*, “garantia de uma liberdade de natureza fundamental dos tempos modernos.”⁷⁹

O n.º 6 do art. 45º consagra o direito ao livre acesso às redes informáticas.

Foi implementada na revisão constitucional em 1997, mais uma demonstração da perceção da necessidade de acompanhar a evolução da tecnologia.

⁷⁷ CASTRO, Catarina Sarmiento e, 2016, 40 anos de “Utilização da Informática” - o artigo 35.º, pág. 50 Este direito à autodeterminação informacional é definido por Jorge Miranda e Rui de Medeiros como sendo o “direito de cada indivíduo dispor livremente dos respetivos dados e informações pessoais e, assim, determinar os tempos de acesso e utilização por terceiros desses mesmos dados e informações” e que tem como finalidade “evitar intromissões abusivas na vida privada das pessoas”, MIRANDA, Jorge; MEDEIROS, Rui, 2010, Constituição Anotada Portuguesa, pág. 784.

⁷⁸ MIRANDA, Jorge; MEDEIROS, Rui, 2010, Constituição Anotada Portuguesa, pág. 785.

⁷⁹ CASTRO, Catarina Sarmiento e, 40 anos de “Utilização da Informática” - o artigo 35.º in *Epública Revista de Direito*, 2016, pág. 52.

Ora, numa sociedade da informatizada, num mundo interligado numa rede mundial, os efeitos na sociedade são significativos ao nível da educação, cultura, relações pessoais, entre outros, ao que o direito não pode ignorar.

Este n.º 6 deve ser interpretado no sentido em que os cidadãos têm livre acesso à rede e infraestruturas tecnológicas e, para além disso, a possibilidade de ter um papel ativo no acesso aos mesmos, utilizando as funcionalidades que as tecnologias proporcionam, podendo realizar livremente tarefas como a utilização do correio eletrónico.

O uso generalizado da Internet “acarreta, nalguns casos, novas ameaças para velhos direitos, como o direito à honra, ao bom nome, à autodeterminação sexual, bem como à intimidade da vida privada, ou se é espaço virtual de incitação à violência e terrorismo, ou de emissão de mensagens racistas, ou pode, também, fazer perigar o direito à autodeterminação informativa, o seu uso também veio, ao invés, permitir novas formas, desmaterializadas e em rede, de exercício de velhos direitos do mundo analógico.”⁸⁰ (Castro, 2016, p. 53)

Este fenómeno, determina-se pelo facto de o direito ao acesso à Internet poder ser considerado um direito fundamental instrumental que engloba outros direitos e liberdades.

No entanto, este direito é ainda um direito fundamental de conteúdo próprio, um direito de ligação e interação numa rede informática, uma vez que esta utilização da rede e dos serviços de comunicação são hoje em dia indispensáveis ao ser cidadão.⁸¹

7. A comissão nacional de dados

O n.º 2 do art. 35º foi introduzido em 1997 na 4ª revisão constitucional da CRP e refere que: “a lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.”

Em 1976, a Assembleia Constituinte que aprovou a Constituição chegou a redigir um n.º para o art. 35º que referia que “em lei ordinária será assegurada a defesa dos cidadãos contra a utilização abusiva da informática e criada a comissão de inspeção de informática, cujas funções são definidas pela Assembleia Legislativa Popular”. Todavia, uma vez que se

⁸⁰ CASTRO, Catarina Sarmiento e, 2016. 40 anos de “Utilização da Informática” - o artigo 35.º *in* *Epública Revista de Direito*, 2016, pág. 52.

⁸¹ CASTRO, Catarina Sarmiento e, 2016. 40 anos de “Utilização da Informática” - o artigo 35.º *in* *Epública Revista de Direito*, 2016, pág. 53.

considerava que a sua definição deveria constar da Lei e não da Constituição, o mesmo foi eliminado, tendo o fenómeno se repetido novamente em 1989.⁸²

A CNPD foi criada pela Lei n.º 10/91 de 29 de abril e entrou em funcionamento em 1994.

A competências desta Comissão foi estabelecida pela Lei n.º 67/98, de 26 de outubro, revogada pela Lei n.º 58/2019, de 08 de Agosto, e a organização da mesma encontra-se determinada na Lei n.º 43/2004, de 18 de agosto.⁸³

A CNPD, também denominada de Autoridade Nacional de Controlo de Dados Pessoais, é uma entidade administrativa independente, com personalidade jurídica independente, de direito público e poderes de autoridade, dotada de autonomia administrativa e financeira e, que tem como objeto, o controlo e fiscalização do processamento ou tratamento de dados pessoais, com o objetivo de assegurar o respeito pelos direitos, liberdades e garantias do cidadão.

Esta entidade, tal como referido anteriormente caracteriza-se pela sua independência, não se encontrando subordinada a qualquer direção, superintendência ou tutela do poder político, “pautando a sua ação por critérios de natureza essencialmente técnica, e assegurando o estatuto dos seus membros a independência e imparcialidade da sua atuação, em virtude de lhes serem atribuídas garantias de inamovibilidade e de irresponsabilidade, e a sujeição a um especial regime de incompatibilidades.”⁸⁴

De acordo com o art. 8º da Lei n.º 58/2019, de 08 de agosto as entidades públicas e privadas devem prestar a sua colaboração à CNPD, facultando-lhe todas as informações que por esta lhes sejam solicitadas, no exercício das suas atribuições e competências.

Esta cooperação ocorre quando existe uma necessidade de examinar o sistema informático e ficheiros de dados pessoais, bem como todos os dados pessoais em causa.

Mais, de acordo com os n.º 3, 4 e 5 todos os membros da CNPD, assim como todos os intervenientes que cooperem com esta entidade estão obrigados ao dever de sigilo profissional, durante e após a realização das funções, relativamente aos dados pessoais,

⁸² CASTRO, Catarina Sarmento e, 2016. 40 anos de “Utilização da Informática” - o artigo 35.º in *Epública Revista de Direito*, pág. 52.

⁸³ CASTRO, Catarina Sarmento e, 2016.40 anos de “Utilização da Informática” - o artigo 35.º in *Epública Revista de Direito*, pág. 53.

⁸⁴ CASTRO, Catarina Sarmento e, 2016. 40 anos de “Utilização da Informática” - o artigo 35.º in *Epública Revista de Direito*, pág. 54.

segredo profissional, industrial e comercial ou informações confidenciais a que tenham acesso no exercício das suas funções.

Em relação às competências desta entidade, o art. 6º da supramencionada lei, atribui à mesma a capacidade de pronunciar-se sobre medidas legislativas e regulamentares relativas à proteção de dados e fiscalizar o cumprimento das disposições do regulamento de proteção de dados e demais disposições regulamentares, bem como, disponibilizar uma lista de tratamentos sujeitos à avaliação do impacto sobre a proteção de dados, apresentar projetos de acreditação de organismos de monitorização de códigos de conduta e dos organismos de certificação, e ainda, cooperar com o Instituto Português de Acreditação, para a acreditação de organismos de certificação em matéria de proteção de dados.

Atualmente, equaciona-se a necessidade de uma nova legislação, que concerne à proteção de dados que clarifique as novas competências da autoridade nacional de proteção de dados. Com a mudança resultante do Regulamento, o modelo de supervisão passou de preventivo para reativo, deixando a função verificativa e passando à responsabilização dos responsáveis pelo tratamento de dados.

É certo que, o novo modelo contém vantagens ao nível do controlo de dados uma que, esse controlo ainda evita burocracias administrativas lentas, permitindo às empresas iniciar atividade sem muitos entraves. Não obstante, essa falta de zelo será um preço a pagar no futuro.

8. O problema da internet das coisas e da inteligência artificial na proteção da privacidade

Tal como já anteriormente referido, a nova era digital, afeta e afetarà cada vez mais a privacidade.

Aliás, esta afetação da vida privada inclui todo o quotidiano do cidadão, o direito à tranquilidade, à solidão, o direito de comunicar com os outros em segurança e em confidencialidade.

A utilização de dados pessoais pelos softwares, seja na invasão não autorizada dos mesmos, seja pela partilha ou utilização, afeta e afetarà cada vez mais a privacidade dos indivíduos, pelo que é e será sempre necessário a criação de mecanismos que ajudem a controlar esta introdução abrupta das novas tecnologias na vida privada do ser humano.

Este processo de corrosão das fronteiras da intimidade, ainda que exista uma tentativa de manter o sigilo dos dados por textos constitucionais, europeus e internacionais, torna-se cada vez mais difícil, uma vez que nos encontramos num sistema global digitalizado.

O mundo diminuiu à distância de um clique, contribuindo para o rápido acesso a pessoas e dados pessoais.

O problema surge quando nos apercebemos que, para que seja possível aceder a qualquer informação, é necessário abdicar de dados pessoais, interferindo com o direito à privacidade do cidadão. Por isso, hoje mais que nunca é necessário encetar todos os esforços para protegê-los.

Hoje em dia não existe serviços ligados à internet que dispensem o armazenamento e tratamento de dados pessoais e, como nos encontramos numa sociedade informação, o cidadão prefere abdicar dos seus dados de forma a não perder a informação que procura.

Acresce que, hoje em dia o problema não passa só pela cedência de dados à internet, mas também pela incapacidade de manter o sigilo sobre os mesmos.

Todos os dias são realizados inúmeros ataques cibernéticos cujo objetivo é, muitas vezes o acesso aos dados privados.

Ora, as entidades ainda não têm capacidade suficiente para prever, prevenir ou evitar esses ataques informáticos, encontrando-se à mercê dos mesmos.

Acresce ainda que, para além dos ataques generalizados a websites e redes sociais, outro problema é o *phishing*, tentativa fraudulenta de obter informações privadas das contas dos utilizadores.⁸⁵

Através desta ação, o *hacker* tem acesso a dados como ao nome, email, senha da conta do utilizador, morada, dados de cartões de crédito, entre outros.

Na atual era digital, a intromissão dos dados pessoais abrange o acesso a emails, dados de contas bancárias, dados sobre convicções religiosas e políticas, arquivos eletrónicos guardados, entre outros.⁸⁶

⁸⁵ CANCELIER, Mariela, 2020. Hackers são nova ameaça no Instagram com avisos falsos de direitos autorais in Mundo Conectado, consultável in <https://mundoconectado.com.br/noticias/v/14339/hackers-sao-nova-ameaca-no-instagram-com-avisos-falsos-de-direitos-autorais>.

⁸⁶ VEIGA, Adélcia, 2020. Proteção de dados: O direito à privacidade na era digital, 2020, pág. 41. Neste sentido, o ransomware, ocorre quando dados privados como identidade, email, entre outros, são sequestrados e bloqueados aos seus utilizadores por um software que depois requer um resgate com o objetivo de os devolver - JÚNIOR, Francisco Gomes, A proteção dos dados pessoais e os hackers, Migalhas, 2021, consultável in <https://www.migalhas.com.br/depeso/344504/a-protecao-dos-dados-pessoais-e-os-hackers>

Estes episódios têm sido cada vez mais frequentes e surgem em qualquer aplicação, emails anónimos, redes sociais, telemóvel entre outros.

Afeta não só, utilizadores individualizados, mas também, empresas bloqueando-lhes o acesso a dados e sistemas, vendendo os dados e comprometendo negócios, sistemas.

Para além disso, ainda que liquidado o preço do resgate nem sempre isso dá lugar à transferência total dos dados para a posse do lesado, ou até à eliminação permanentemente dos dados na conta do infrator.⁸⁷

Para que este problema fosse resolvido a solução passaria por um reforço na segurança cibernética das empresas, pela criação de mecanismos guia de proteção e ainda através do sancionamento àquelas que não respeitassem tais instruções no caso de vazamento de dados.

O problema é que, esses mecanismos de proteção e as coimas aplicadas pela “permissão” do ataque são muito dispendiosos levando a que pequenos empresários prefiram correr o risco e, eventualmente, negociar com o *hacker* para que o resgate seja inferior à sanção.

Os problemas da informatização de dados e de mecanismos rudimentares de segurança vai muito para além de acessos a contas individualizadas.

No passado dia 30 de Janeiro de 2022, hackers pertencentes ao Lapsus\$ Group, que também atacaram o Grupo Impresa, grupo de comunicação social em Portugal, tendo divulgado uma mensagem no qual referiam ter hackeado o site do Parlamento Português, tendo acesso a aplicações da Microsoft, IIS srv, SOAP apis, DLL,⁸⁸

Apesar de as autoridades judiciárias ainda se encontrarem a apurar se existiu realmente um ataque informático e, no caso afirmativo, se foram furtados dados sensíveis, a verdade é que a rapidez e perícia destes ataques conseguem que só sejam analisados os dados posteriormente ao ataque.

⁸⁷ SOPRANA, Paula, Internet das Coisas impõe desafios de segurança, privacidade e conectividade, *Época*, 2017, consultável in <https://epoca.oglobo.globo.com/tecnologia/experiencias-digitais/noticia/2017/10/o-risco-da-internet-das-coisas.html>.

⁸⁸ E, segundo Franco Hugo, “(...)a uma grande quantidade de bases de dados que contém informação sensível do Governo relacionada com informações pessoais de políticos e de partidos políticos, muitos documentos, emails, passwords(...)”. Referiram ainda que, “(...) os sistemas têm tecnologia Microsoft antiga e sem manutenção, aplicações fracas, má programação e más práticas de segurança”, Hackers do Lapsus\$ Group anunciaram ter roubado informações do site do Parlamento. Site esteve em baixo durante cinco minutos, PJ está a investigar. *EXPRESSO*, 30 de Janeiro de 2022, consultável in <https://expresso.pt/sociedade/hackers-do-lapsus-group-anunciaram-ter-roubado-informacoes-do-site-do-parlamento-site-esteve-em-baixo-durante-cinco-minutos-pj-esta-a-investigar/>.

Os nossos sistemas de segurança cibernética são tão deficitários que não conseguem impedir um ataque, limitando-se à investigação posterior e à verificação de possíveis danos.

Grupos como os do Lapsus\$ Group entram nos dispositivos, vendem a informação ou o acesso aos mesmos, ou até, por simples diversão, destroem os ficheiros permanentemente. O intuito é demonstrar a sua imponente e intangibilidade e ainda obter lucro com a venda de informações.

O mesmo ocorreu no ciberataque à operadora de telecomunicações Vodafone, que na noite de dia 07 de fevereiro de 2022 foi alvo de um ciberataque com o objetivo de causar danos e perturbações na rede, que bloqueou todos os serviços da operadora por um determinado tempo.⁸⁹

Ora, esta situação afetou, não só, utilizadores regulares, mas também, empresas, multibancos e inclusive o Inem que, devido ao sucedido, implantou um plano de contingência de forma a assegurar a ininterruptão das chamadas de emergência.

A operadora, logo após se aperceber do putativo problema, procedeu de forma imediata à identificação e reposição dos serviços tendo o CEO da Vodafone Portugal afirmado não existirem indícios que o hacker tenha acedido a dados de clientes. Todavia, o mesmo não pode confirmar o não acesso aos mesmos.⁹⁰

Tal situação, aconteceu também aos laboratórios Germano de Sousa que, na sequência de um ataque a 10 de fevereiro de 2022 não realizaram análises ou exames por um tempo determinado.⁹¹

Tal ataque não aparenta, dizem, ter afetado bases de dados com registos de informação de clientes, no entanto, interferiu nas intercomunicações com parceiros, hospitais e centro de análises.

Ora, tal situação suscita uma questão: Se o atacante conseguiu entrar no sistema informático e bloquear comunicações, o que garante que as informações privadas de utentes

⁸⁹ DIÁRIO DE NOTÍCIAS, PJ investiga ataque informático à Vodafone, Diário de Notícias, 8 de Fevereiro de 2022, consultável in <https://www.dn.pt/sociedade/servicos-de-voz-movel-da-vodafone-registam-recuperacao-progressiva-14568590.html>.

⁹⁰ DIÁRIO DE NOTÍCIAS, 8 de Fevereiro de 2022, PJ investiga ataque informático à Vodafone, Diário de Notícias, consultável in <https://www.dn.pt/sociedade/servicos-de-voz-movel-da-vodafone-registam-recuperacao-progressiva-14568590.html>.

⁹¹ RTP, 14 de Fevereiro de 2022, Ciberataque. Laboratórios Germano de Sousa adiam reabertura, consultável in https://www.rtp.pt/noticias/pais/ciberataque-laboratorios-germano-de-sousa-adiam-reabertura_n1384288.

não tenham sido acedidas da mesma forma? Aliás, cinco minutos de acesso a um sistema informático é o suficiente para que seja possível copiar milhares de ficheiros.

O que é certo é que, estes ataques são cada vez mais frequentes e os hackers que outrora entravam em sistemas operativos alheios por mera diversão, hoje em dia conseguem ter uma atividade lucrativa através da venda de dados sensíveis ou importantes.

Acresce ainda que, mesmo as criações feitas pela simbiose da internet das coisas e da inteligência artificial padecem de problemas de segurança.

A AI e a IoT necessitam de uma grande quantidade de dados de forma a poder obter uma decisão correta ou um banco de dados uniformizado. Dessa forma, os algoritmos são beneficiados pela maior quantidade de dados possível para a realização de uma tarefa.

Toda esta recolha de dados permite a formação de algoritmos, ou seja, os dados são organizados e armazenados permitindo a previsão de determinados padrões de comportamento.

Claro está que, os dados utilizados são ainda armazenados dentro do sistema para fins históricos, de forma a se realizar previsões sobre decisões a tomar futuramente.

Através dos mesmos, a máquina, aliada à inteligência artificial, irá conduzir o indivíduo para o fim pretendido por esta, sem que o mesmo se aperceba.

“O algoritmo é a arma dos gigantes da internet para controlar o ser humano sem que este se aperceba.”⁹²

A questão está, no controlo de fornecimento dos dados, que não é de todo realizado uma vez que, quanto maior a quantidade de dados, melhor será a resposta dada pelo sistema.

Poder-se-ia reduzir o tempo de armazenamento dos dados, no entanto isso implicaria a redução na taxa de sucesso das previsões efetuadas, o que também não é pretendido.

Hoje em dia, a recolha de dados para fins de inteligência artificial ainda é realizada sem muito controlo o que coloca em risco a privacidade do cidadão.⁹³

Para além disso, ainda que os sistemas de inteligência artificial sejam extremamente vanguardistas o certo é que, os mesmos não são impenetráveis, pelo contrário, uma vez que,

⁹² SHULZE, Alberto de Franceschi Reiner, 2019. Digital Revolution - New Challenges for Law, pág. 109.

⁹³ JULIANA, 2021 Proteção de dados e Inteligência Artificial: desafio da LGPD, Neuralmind, consultável in <https://neuralmind.ai/2021/02/10/protecao-de-dados-e-inteligencia-artificial-o-desafio-da-lgpd/>.

a grande parte dos mesmos é criada para um determinado objetivo sendo a segurança dos mesmos realizada por outro sistema.

Ou seja, o risco encontra-se não só pela simples utilização da rede, mas também pelos instrumentos criados pela IA e pela IoT.

A título exemplificativo, o marcapassos que, tal como referido no ponto 4.4.2, permite a monitorização do sistema cardiovascular nos pacientes.

Este aparelho, no final de agosto de 2017 sofria de variadas falhas de segurança, o que levou à notificação de 465 mil americanos com fim à atualização do instrumento sob o risco de verem o seu coração *hackeado* por estranhos.

Ora, a interligação de todo o tipo de objetos com cidadãos, empresas e governos é, para a repórter Paula Soprana “como um campo de petróleo recém-descoberto: pode gerar riqueza para a população ou ser corrompido para o interesse de poucos. Junto às duas possibilidades, também existe o risco de o petróleo vazar.”⁹⁴

As vantagens da utilização de sensores na agricultura e indústria não apresenta aparentemente qualquer ameaça, no entanto, a quantidade de informação que é recolhida pela maquinaria permitirá, no caso de *hakeamento*, a venda de informações para outras empresas possibilitando, por exemplo, a concorrência desleal entre empresas.

Acresce que, quando os chips são implantados no ser humano e utilizados no quotidiano do mesmo a resposta não será certamente a mesma.

O acesso à localização, ao microfone, à camara do telemóvel e computador do cidadão pode e potencializa um risco para o mesmo.

Falamos de uma “*bomba atómica*” cuja destruição é surpreendentemente superior à grandiosidade da sua criação.

Encontramo-nos numa época em que o acesso à informação tem como pagamento o acesso a dados pessoais.⁹⁵

O Wi-fi público, aliado a uma parceria privada, requer para o seu acesso a entrega de dados pessoais e, até as aplicações que são instaladas o telemóvel requerem a cedência de determinados dados como email e identidade.

⁹⁴ SOPRANA, Paula, 2017. Internet das Coisas impõe desafios de segurança, privacidade e conectividade, *Época*, consultável in <https://epoca.oglobo.globo.com/tecnologia/experiencias-digitais/noticia/2017/10/o-risco-da-internet-das-coisas.html>.

⁹⁵ SOPRANA, Paula, 2017. Internet das Coisas impõe desafios de segurança, privacidade e conectividade, *Época*, consultável in <https://epoca.oglobo.globo.com/tecnologia/experiencias-digitais/noticia/2017/10/o-risco-da-internet-das-coisas.html>.

Jaron Lanier afirma que, estamos a perder a nossa liberdade de escolha e a nossa privacidade, uma vez que, nos encontramos constantemente a ser vigiados e monitorizados sem nos apercebermos. Afirma ainda que “Apple ouve tudo, Google vê tudo, e a NSA sabe tudo.”⁹⁶

O constante uso de redes sociais permite a recolha de dados por parte do algoritmo permitindo assim a criação de um perfil do utilizador sem ser necessário sequer o seu consentimento. O acesso a serviços alegadamente gratuitos pelo utilizador permite que o mesmo, sem que se aperceba pague esse acesso com os seus dados pessoais. Depois, o mesmo é facilmente redirecionado para publicidade de produtos alegadamente do seu interesse.

Esta forma aliciante permite que os utilizadores estejam cada vez mais “amarrados” às redes sociais levando a um número mais evidente de viciados, os chamados “Sticky cosumers”. Quanto mais viciado nas redes sociais, ou internet no geral, estiver um utilizador mais fácil será a sua manipulação.⁹⁷

Frank Schirmacher chama a este problema totalitarismo tecnológico, no sentido de demonstrar que nos encontramos numa era de controlo tecnológico que coloca em grande risco a liberdade pessoal.

Apesar de a expressão parecer um pouco bruta, certo é que não existe melhor para descrever o presente fenómeno tecnológico. A única diferença entre os dois é que um é obtido através da violência e opressão e o outro através da omissão de informações e esquemas ardilosos.⁹⁸

Richard David Prech, filósofo alemão afirma que, existe quase que uma pressão da sociedade para a utilização das redes apenas para o ser humano demonstrar que é social.

Por isso, ao contrário de Lanier, este filósofo entende que, ainda que esteja visível os perigos da constante utilização das redes não há outro caminho possível porque qualquer recusa ao mesmo será um ideal irrealista.⁹⁹

100. ⁹⁶ SHULZE, Alberto de Franceschi Reiner, 2019. Digital Revolution - New Challenges for Law, pág.

101. ⁹⁷ SHULZE, Alberto de Franceschi Reiner, 2019. Digital Revolution - New Challenges for Law, pág.

102. ⁹⁸ SHULZE, Alberto de Franceschi Reiner, 2019. Digital Revolution - New Challenges for Law, pág.

103. ⁹⁹ SHULZE, Alberto de Franceschi Reiner, 2019. Digital Revolution - New Challenges for Law, pág.

Todavia o filósofo considera que é possível recuperar a autonomia ainda que seja um caminho difícil. Caso contrário, o mundo irá se tornar num lugar completamente frio, sem qualquer imperfeição humana, completamente controlado por máquinas.¹⁰⁰

Em suma, é possível constatar que, sem sombra de dúvidas a liberdade dos indivíduos está a ser posta em causa. Neste momento, a liberdade dos indivíduos está a ser comprimida e o mesmo já não faz parte do comando, mas sim do objeto de interesses comerciais e políticos.

Isto é um claro ataque às sociedades democráticas e como Lanier refere “The one that owns the data, will decide our destiny”.¹⁰¹

Aqui a solução passaria talvez, por um reforço legislativo ao nível da segurança cibernética. A criação de uma lei de proteção de dados direcionada para a proteção cibernética primeiramente ao nível empresarial e posteriormente ao nível pessoal.

Essa legislação deveria conter normas de carácter obrigatório e facultativo, sendo que a quantidade de dados obtidos pela empresa seria o ponto de referência.

As obrigações passariam pela criação de departamentos de cyber segurança, de planos de segurança, contingência e proteção de dados, de forma a evitar ataques ou, ainda que estes ocorram, diminuir as suas consequências.

Para além das normas obrigacionais, a existência de normas sancionatórias no caso de vazamento de dados iria criar um maior cuidado por parte das empresas detentoras dos dados em evitar o *hackeamento* dos sistemas.

Essas normas deveriam ser realizadas de forma a que empresas com acesso a um número mínimo de dados não fossem prejudicadas com custos acrescidos às suas atividades.

Claramente, o que foi criado até aqui não foi capaz de resolver o prolema, então a solução ideal passaria pela criação de um programa único para recolha, armazenamento e proteção de dados (à semelhança da icloud) direcionado para dados empresariais.

A criação de um programa universal de recolha de dados em IoT iria permitir o vasto armazenamento e tratamento de dados pelas empresas nunca refutando

O programa, ainda que geral, deveria ser individualizado a cada empresa impedindo o cruzamento de dados indevidos.

100 SHULZE, Alberto de Franceschi Reiner, 2019. Digital Revolution - New Challenges for Law, pág. 104.

101 SHULZE, Alberto de Franceschi Reiner, 2019. Digital Revolution - New Challenges for Law, pág. 108.

Desta forma, o controlo do programa seria sediado pelo Estado, (tal como o Saft).

8.1. A proteção de dados e o totalitarismo informático

Manuel Castells, sociólogo, no final dos anos 90, afirmou que, a internet iria revolucionar as décadas seguintes, referindo que o mundo iria estar todo interligado.

Refere ainda que, ao contrário das eras anteriores cujo acontecimentos e alterações surgiram e alteraram a sociedade moderadamente, esta iria transformar por completo a nossa cultura material.

O desenvolvimento tecnológico começou a sua expansão a partir das últimas décadas do século XX, fruto da capacidade de criar uma interface entre campos tecnológicos através de uma linguagem digital comum fornecida pelo tratamento de dados.¹⁰²

A rápida evolução tecnológica reduziu o mundo à distância de um clique. Hoje em dia, qualquer cidadão pode aceder facilmente a serviços, produtos e informação do outro canto do mundo porque tudo está interligado.

A tecnologia afeta, não só, o quotidiano das pessoas, mas também, o seu trabalho, a sua saúde, as infraestruturas, as empresas, entre outras.

A ligação das coisas à internet permitiu um melhor desenvolvimento e controlo das coisas agilizando a vida do cidadão e a inteligência artificial criou uma nova forma de obter respostas, de realizar cálculos e previsões, permitindo a redução de horas de estudo e de decisões infundadas.

A ligação do ser humano a estes dispositivos está tão enquadrada na sociedade que já não se estranha a constante utilização dos mesmos. Os seres humanos estão a ser constantemente sugados por todas estas tecnologias o que afeta, não só a sua vida, mas também a forma de pensar, de julgar, de tomar decisões.

A sede por informação transformou-se numa forma aliciante de permissão inconsciente de entrega de dados pessoais.

O ser humano permite o acesso aos seus dados privados apenas para obter uma informação e o seu consciente está tão concentrado no acesso à informação que não lhe dá qualquer aviso.

¹⁰² Neste sentido, CASTELLS, Manuel afirma que: “Vivemos num mundo que segundo Nicholas Negroponte, se tornou digital”,2002, A sociedade em rede, pág.68.

Quando a questão é o acesso à informação, a irracionalidade do ser humano despoleta transformando-se como num animal com fome em frente à sua presa.

O animal ataca a presa pela necessidade de se alimentar, o ser humano cede dados porque tem fome de informação.

O motivo é diferente, mas o desejo é o mesmo, o acesso, um à alimentação, outro à informação.

O direito à proteção de dados tem particular relevância no controlo da recolha, utilização e partilha de dados.

As informações pessoais recolhidas, utilizadas e armazenadas colocam os seres humanos numa posição fragilizada, tendo o RGPD colocado o tratamento de dados pessoais no centro das preocupações jurídicas e empresariais.¹⁰³

8.2 Os problemas ético-jurídicos e as soluções dadas pela UE

É verdade que a IA e a IoT são ferramentas de ajuda para o desenvolvimento da humanidade. Mas, do que têm de maravilhoso, têm de perigoso.

Para além dos inúmeros problemas enunciados no ponto anterior, existem ainda alguns problemas que devem ser enumerados no campo da ética e do direito.

Claro que, não é só sobre estes problemas que esta tese versa, todavia, os mesmos são intransigentes a qualquer sistema IA, inclusivé sistemas que necessitam de dados pessoais para funcionar.

Por isso, será realizada uma pequena enunciação dos mesmos e mencionados quais os mecanismos que a UE definiu para a resolução, ou no mínimo diminuição, destes problemas.

Ora, antes de mais, é importante referir que sim, a IA encontra-se a evoluir a olhos vistos e consegue realizar muitas tarefas, algumas melhores que um ser humano. Afinal, é uma tecnologia que não é afetada pelo cansaço, desejo de ajudar um amigo ou até por ter tido um mau dia. Mas, mesmo assim os algoritmos não são, nem perto, mais objetivos que os humanos. Os resultados podem ser incorretos ou discriminatórios se no treino do sistema o mesmo tenha recebido dados nesse sentido.¹⁰⁴

¹⁰³ CORDEIRO A. Barreto Menezes, 2020, Direito da Proteção de dados, pág. 29.

¹⁰⁴ THE NORWEGIAN DATA PROTECTION AUTORITHY, 2018, Artificial intelligence and privacy, pág. 15, consultável em <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>.

8.2.1. A viés algorítmica

Um dos problemas que pode surgir com a utilização destas novas tecnologias é a discriminação ou viés algorítmica.

Uma vez que, estas tecnologias são treinadas com base numa grande quantidade de dados históricos, isso pode levar a um agravamento ou perpetuamento de alguns vieses na sociedade. Ou seja, estas tecnologias podem levar à criação ou continuação de estereótipos e discriminação.

O grupo independente de peritos de alto nível sobre a inteligência artificial afirma que, os dispositivos com IA devem ser concebidos de forma a assegurar o respeito igualitário do valor moral e da dignidade de todos os seres humanos.

O objetivo é que exista igualdade no sistema, ou seja, o sistema não pode gerar resultados injustamente tendenciosos, pelo que os dados utilizados para treinar os sistemas de IA devem ser o mais inclusivos possível, representando diferentes grupos, etnias, religiões, entre outros, de toda a sociedade, possibilitando desse modo, o respeito por determinadas pessoas e grupos potencialmente vulneráveis.¹⁰⁵

Todavia, de acordo com as estatísticas, o viés algorítmico tem uma percentagem baixa, o que significa que ainda que seja um problema, não é dos que gera maior preocupação.

8.2.2 A transparência

Outro problema que a utilização destas tecnologias leva é a falta de transparência. Ora, quando um dispositivo IA cria um output¹⁰⁶ não demonstra como chegou a essa conclusão.¹⁰⁷

Isto torna a tecnologia de IA e o *machine learning* inatingíveis, o que preocupa a sociedade. Desde logo porque, em variados sistemas não é possível verificar quais os componentes, informações e dados utilizados pelo sistema até à criação da resposta, nem sequer, de onde os mesmos foram retirados. Este fenómeno é chamado de *black box* porque tudo o que está dentro é obscuro, inatingível e indecifrável.

¹⁰⁵ Grupo independente de peritos de alto nível sobre a inteligência artificial, Orientações éticas para um IA de confiança, pág. 13.

¹⁰⁶ Output significa saída.

¹⁰⁷ Colóquio Tribunais e inteligência artificial – uma odisséia no século XXI, 12 de maio de 2023, 01:29:15 até 03:49:05, consultável em <https://www.stj.pt/?p=17432>.

Esta situação, cria uma sensação de insegurança por parte dos utilizadores e principalmente por parte dos Estados e é chamada o problema da intangibilidade do *machine learning*.

O requisito da transparência traduz-se na indicação de que deve haver transparência e revelação de informações pelo responsável dos sistemas de inteligência artificial, para assegurar a possibilidade aos utilizadores de entender o seu funcionamento e possam ainda os contestar.

Nestas situações, considera-se que os governos devem, por um lado, intensificar a fiscalização de forma a assegurar o cumprimento deste princípio e, por outro lado, facilitar os investimentos na criação e desenvolvimento de sistemas de IA confiável, com infraestruturas digitais acessíveis e transparentes. Devem ainda, assegurar um ambiente propício à proliferação e desenvolvimento, nacional e internacional, destas tecnologias confiáveis.¹⁰⁸

O requisito da transparência está ligado ao princípio da explicabilidade, rastreabilidade e comunicação.

O grupo independente de peritos de alto nível refere que, os conjuntos de dados e processos que criam a decisão de IA e os processos de recolha dos dados, bem como os algoritmos utilizados, devem ser sustentados de forma a possibilitar a rastreabilidade e um aumento da transparência. Tal também se deve aplicar às decisões tomadas pelo sistema de IA, dessa forma será possível rastrear os motivos pelos quais o sistema IA produziu uma resposta errada e evitar possíveis erros.¹⁰⁹

No que concerne à explicabilidade, o grupo independente de peritos de alto nível demonstra que a explicabilidade diz respeito à faculdade de esclarecer todos os processos técnicos de um sistema IA como as decisões humanas com eles relacionadas.

Tal como a rastreabilidade, a explicabilidade técnica exige a possibilidade da rastreabilidade e compreensão das decisões tomadas pelos sistemas. Acresce que, a explicação em causa deverá ser adequada ao nível de especialização da parte interessada.

¹⁰⁸ MARTINS, José Eduardo Figueiredo de Andrade, 14 de maio de 2020, Dilemas éticos e jurídicos do uso da inteligência artificial na prática jurídica, CIDP - Centro de Investigação de Direito Privado, pág. 14, disponível em https://www.cidp.pt/revistas/rjlb/2021/4/2021_04_0919_0952.pdf

¹⁰⁹ Grupo independente de peritos de alto nível sobre a inteligência artificial, Orientações éticas para um IA de confiança, pág. 21.

No caso da comunicação, o grupo determina que os utilizadores devem ser informados que estão a interagir com um sistema IA não devendo ser-lhes omitida essa informação.

Por isso, os sistemas de IA devem ser identificáveis como tal. Deve ainda ser permitida a escolha, por parte do utilizador, da interação humana ou da interação por sistema IA. Acresce ainda que, os programadores de IA devem ainda informar sobre as capacidades e limitações do sistema de IA.¹¹⁰

8.2.3 A responsabilidade pelos danos causados por sistemas IA

Um outro problema é o da responsabilidade pelos danos causados pela IA.

A IA tem evoluído de forma galopante ao longo dos anos encontrando-se inserida em variados sistemas e dispositivos, evoluindo através das instruções dos seus programadores ou através de si própria. O problema ocorre quando, esse sistema ou dispositivo comete algum erro que crie lesão ao utilizador.

Ora, quanto maior a introdução destas tecnologias, maior será a quantidade de danos criados pois, a IA terá sempre a necessidade de se aperfeiçoar, o desejo de ser racional, a procura pela preservação da utilidade das suas funções e a vontade de adquirir novos recursos de forma a poder evoluir.¹¹¹

Para a resposta a essa questão é necessário, desde logo, discutir-se a questão da atribuição de personalidade jurídica, ou um sistema semelhante, a um sistema de IA.

Existe um entendimento doutrinário que defende que, a partir do momento em que uma entidade alcança um certo grau de autonomia, à mesma será passível de lhe ser conferida personalidade jurídica.

Outra vertente doutrinária defende que, deve ser atribuída personalidade jurídica à semelhança do que sucede com as pessoas coletivas. A chamada técnica da personificação, possibilita lidar com a incerteza, sendo definida consoante ficções que equiparam o “personificado” ao “humano”.¹¹²

¹¹⁰ Grupo independente de peritos de alto nível sobre a inteligência artificial, Orientações éticas para um IA de confiança, pág. 22.

¹¹¹ SILVA, Bárbara Jénifer Paz de Abreu da, 2020, Inteligência artificial e as suas implicações etico-jurídicas, pág. 42.

¹¹² Ramos, Nuno André Novo, 2020. Responsabilidade civil em dano causado por mecanismo dotado de inteligência artificial, pág. 46.

Neste sentido, a atribuição de personalidade aos robots seria um meio de evitar conflitos decorrentes da atribuição de responsabilidade ao detentor do mesmo.

Se, a título exemplificativo, esta última teoria fosse adotada, o primeiro passo seria determinar qual o momento de atribuição da personalidade jurídica.

No nosso ordenamento jurídico, segundo o n. 1 do art. 66º do CC, “(...) a personalidade adquire-se no momento do nascimento completo e com vida.” e, nos termos do n.º 1 do art, 68º do mesmo diploma legal, “A personalidade cessa com a morte”.

Ora, esta personalidade, ainda que pareça abrangente, encontra-se intimamente ligada ao ser humano, pelo que não se considera que se possa aplicar esta personalidade jurídica aos robots.

Não será, no entanto por esse motivo que o robot não possa ser responsabilizado, aliás, as pessoas coletivas também são possuidoras de personalidade jurídica, mesmo não tendo adquirido a mesma de forma biológica.

Todavia, a atribuição de personalidade jurídica às pessoas coletivas foi necessária para dar resposta à possibilidade de as mesmas serem responsabilizadas no âmbito da responsabilidade civil.

Então questiona-se: se existe personalidade jurídica para uma empresa porque não existe para um robot completamente autónomo? Ou seja, existindo a capacidade por parte do robot de proceder à tomada de decisões e realização de atos de forma totalmente autónoma, não deveria de ser diferenciado das pessoas coletivas.

Ora, ainda que fosse realizado o teste de Turing e fosse atribuída autonomia ao robot, seria necessária uma decisão de reconhecimento jurídico da existência de uma espécie de personalidade digital, onde se verificaria se, para além do programado pelo seu detentor, o robô teria a capacidade de decidir autonomamente.

Não seria impeditivo o mesmo ser, pelo menos, julgado nas decisões que tivesse tomado, mesmo que tivesse sido programado por terceiros.

Acontece que, pelo menos para já, o robot não consegue ir muito para além da sua programação, o que significa que, ainda que o mesmo tome decisões “autonomamente”, o mesmo foi programado para a aferição dessas. A questão apenas se colocaria, num cenário já não tao apocalíptico, a título exemplificativo, se o robot desenhado para cozinhar decidisse que ia limpar. E, mesmo nestes casos, o programador teria de demonstrar que, pelo menos 90% do ato realizado, teria sido decidido livremente pelo robot.

Para além disso, o robot, ainda que fosse detentor de personalidade jurídica, nunca iria ser possuidor de liberdade e até de consciência.

Seria apenas livre para ser responsabilizado, todavia, seria sempre propriedade de alguém, o que levanta inúmeras questões éticas.

A responsabilidade civil das pessoas coletivas está conectada às ações dos seus representantes legais por isso, necessitam de um elemento pessoal, desta forma, no concerne às ações praticadas, serão sempre realizadas por humanos.

Assim, permitir a atribuição de personalidade jurídica a atos praticados por sistemas IA seria evitar que o seu programador não fosse responsabilizado pela criação de um mecanismo que alegadamente não tem controlo.

Posto isto, entendo que, pelo menos para já, este entendimento não deve ser aplicado.

É certo que, em dez anos a minha resposta possa ser outra, todavia, ainda não considero que os sistemas de IA sejam autónomos o suficiente para serem dotados de personalidade jurídica ou qualquer responsabilidade pelos atos praticados.

Ainda que não seja uma parte essencial na presente tese, considero que, antes de abordar este tema, deve ser realizada uma breve enunciação dos requisitos para aplicação da responsabilidade civil, de forma geral.

Ora, para existir responsabilidade civil é necessário um facto, um dano, a ilicitude, o nexo de causalidade entre o facto e o dano e a culpa.

Ocorrendo um dano praticado por um sistema IA, cria-se na esfera jurídica do lesado um direito a ser ressarcido do dano pelo responsável da criação.

Transpondo para o caso em questão, tal ato não tem necessariamente de consistir numa ação, bastando uma conduta para que lhe possa ser imputada responsabilidade. Essa conduta, no caso em concreto, é a conceção, o controlo do robô ou até a omissão de, por exemplo, proceder a atualizações ou correções no mesmo.

No que concerne à ilicitude e à culpa, a primeira significa que, a conduta deverá consubstanciar numa violação de um dever imposto pela ordem jurídica, a segunda trata-se de um juízo de censura, de desvalor, em relação à ação do agente.¹¹³

O nexo de causalidade, entre o dano e a omissão, ocorre no sentido que, o primeiro não se iria verificar se não houvesse o segundo.

¹¹³ NETO, Filipe Teixeira. 2017. A ilicitude enquanto pressuposto da responsabilidade civil delitual: um exame em perspectiva comparada (luso-brasileira). Review for CIDP revistas.

A culpa,¹¹⁴ que pressupõe que o agente tenha agido com culpa, necessitaria de um padrão de conduta que qualificasse o ato do agente como reprovável. Todavia, as exclusões previstas no nosso ordenamento jurídico não poderiam ser utilizadas em danos provocados por sistemas IA.

O dano, resultante do ato ou omissão do programador, é condição essencial para a existência de responsabilidade civil.¹¹⁵

Por fim, e de forma a finalizar o tema da responsabilidade civil em geral, é necessário distinguir a responsabilidade extracontratual da contratual, do qual, a primeira resulta da violação de direitos e deveres presentes em normas elaboradas para a proteção de terceiros, e a segunda, resulta da violação de uma relação contratual.

Aqui chegados, é necessário analisar de forma mais concreta a responsabilidade civil em caso de dano provocado por sistemas IA.

Um exemplo que ilustra a necessidade de regulação da responsabilidade de danos provocados por sistemas IA é o caso do robô Gaak, que saiu sozinho do centro de pesquisa e acabou sendo atropelado por um carro. O robô agiu de forma autónoma e sem qualquer comando nesse sentido.¹¹⁶

Outro exemplo, tendo esse até resultado na morte do seu ocupante, Joshua Brown, o caso do tesla, semiautónomo, que em piloto automático, não travou e se enfaixou no atrelado de um camião.¹¹⁷

Por isso, a questão que aqui se coloca, nestes casos, é de quem é a responsabilidade?

¹¹⁴ Segundo o n.º 1 do artigo 483º do CC: “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.”

¹¹⁵ O dano, é, tal como a ilicitude, um tema controverso e longo, todavia, não são temas essenciais para a presente tese pelo que irão ser tratados de forma gera. Neste sentido, deve-se distinguir o dano em sentido real, do qual se subsume à afetação de um determinado objeto, do dano no sentido patrimonial, do qual corresponde à afetação do património do lesado.

Para além disso, existe ainda os danos emergentes, presentes, futuros, patrimoniais, e futuros, patrimoniais e não patrimoniais.

¹¹⁶ O exemplo do robô Gaak ilustra essa circunstância da IA de aprender e desenvolver muitas vezes sem o controlo do seu programador. Este, utilizou a experiência e inteligência para sobreviver num ambiente mutável. Desta forma, o robô conseguiu do centro de pesquisa tendo sido atropelado por um carro.

O comportamento do mesmo surpreendeu até o seu criador pois o robô decidiu escapar do centro de pesquisa de forma independente. Neste sentido, o que se logra saber é quem é o responsável pelos danos causados. SILVA, Bárbara Jénifer Paz de Abreu da, 2020, Inteligência artificial e as suas implicações ético-jurídicas, pág. 42.

¹¹⁷ EXPRESSO, 9 de julho de 2016. Uma morte não vai parar os carros autónomos. Disponível na Internet em: <https://expresso.pt/sociedade/2016-07-09-Uma-morte-nao-vai-parar-os-carros-autonomos>.

- Do programador ou fabricante? Que procedeu à criação e não foi capaz de assegurar a segurança da sua criação ou de prever alterações de comportamento da mesma.

- Do sistema em si, que não foi capaz de proceder da forma predefinida, ou seja, como foi programado.

- No caso de terem sido comercializados, do vendedor dos robots e sistemas de IA.

- Ou, dos utilizadores do sistema.

Estas problemáticas tratavam-se, há poucos anos atrás, apenas de exemplos hipotéticos e académicos, todavia, estes acidentes estão a ocorrer com cada vez mais frequência.

A responsabilização pelos danos provocados por sistemas IA pode ser dividida em, pelo menos, quatro teorias.

A primeira posição é a que resulta que, a responsabilidade deve ser assumida e gerida pelos fabricantes dos modelos artificiais. Isto poderá ser alcançável através do estabelecimento de uma presunção ilidível que preveja que, em caso de dúvida, os fabricantes serão considerados responsáveis.

Este modelo já é adotado pelo regulamento sobre a IA, que atribui a responsabilidade aos criadores dos modelos salientando a importância da criação de sistemas de IA confiáveis.

Existe, por isso, uma responsabilidade objetiva por parte do criador que, deve ser responsabilizado pelos danos causados por produtos defeituosos, nos termos já enunciados acima.

No caso de a responsabilidade ser atribuída ao produtor, poder-se-ia dizer que tal iria culminar numa redução do desenvolvimento e produção destas tecnologias. Ora, embora seja uma questão pertinente considero que tal não iria acontecer devido ao carácter extremamente lucrativo destas inovações e há vontade nefasta dos produtores criarem sistemas cada vez mais avançados.

Todavia, responsabilizar o produtor seria a resposta fácil, o problema surge quando, da produção à distribuição, o sistema IA passa por diversas entidades.

Mas, no caso de existir essa responsabilização estaríamos perante um produto defeituoso, tratado no DL 383/89 de 6 de novembro.¹¹⁸

¹¹⁸ DL 383/89 de 6 de novembro - Responsabilidade Decorrente de Produtos Defeituosos. “O presente diploma transpõe para a ordem jurídica interna a Directiva n.º 85/374/CEE, do Conselho, de 25 de Julho de 1985, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados membros em matéria da responsabilidade decorrente de produtos defeituosos.”

De acordo com o art. 2º do mencionado diploma legal, o conceito de produtor estende-se a outras pessoas que, importem produtos da Comunidade Europeia e que, forneceram produtos anónimos, caso não comuniquem à vítima, a identidade do produtor comunitário, do importador ou de algum fornecedor.

Esta definição permite o chamamento de todos os participantes na criação do sistema IA.

A definição de defeito, enunciada pelo art. 4º, permite considerar um produto defeituoso quando este não oferece a segurança com que legitimamente se pode contar, o que, para o caso em apreço, é a consideração mais importante.

O DL em causa tinha como propósito, unir os campos da responsabilidade contratual e extracontratual do qual, o lesado deveria provar o dano, o defeito e o nexo de causalidade entre ambos e ao produtor bastava recorrer à exclusão da responsabilidade, previstas nos art. 5º, 7º, 11º e 12º do mencionado diploma legal.

No que concerne ao caso aqui em apreço, poder-se-ia levantar a questão de saber se a responsabilidade pelos defeitos ao nível da programação, ou de sensores defeituosos comprados para inserir no dispositivo, ou pela invasão de um sistema por um hacker ou vírus poderia ser, na mesma, imputada, tão só e apenas, ao produtor. O art. 6º do DL em análise determina que, tal responsabilidade iria ser solidária entre todos os intervenientes na cadeia de produção.

Ora, o problema que surge nestas situações é, sem sombra de dúvidas a prova, uma vez que existem sistemas de IA extremamente complexos e, no caso de um acidente em que o sistema fique inoperacional, será difícil verificar a origem do problema e os componentes que levaram ao mesmo.

Certo é que, a decisão de responsabilizar o produtor é o entendimento mais consciencioso uma vez que, desta forma, assegura-se a responsabilização daquele que tem, não só o dever, mas a melhor capacidade para suportar as despesas inerentes dos danos.

No meu humilde entendimento considero que, essa presunção da responsabilidade nos casos de sistemas de IA defeituosos, apenas deveria de ocorrer durante uma quantidade determinada de anos.

Ou seja, os produtos teriam, com base em níveis de autonomia, um número determinado de anos de garantia. Essa garantia asseguraria a responsabilização do produtor,

no entendimento acima descrito, durante o decurso desses anos. Após o término do prazo de garantia, o produtor deixaria de ser responsável pelos danos causados do sistema IA.

Isto porque, não seria justo, no meu entender, para o produtor, ser “ad eterno” responsável por um produto que foi produzido por si há 20 anos, ainda que o mesmo tivesse um defeito pré-existente.

A título exemplificativo, não podemos responsabilizar um produtor de uma máquina de lavar, utilizada durante vinte anos, que começa a deteriorar a roupa, ainda que essa máquina tivesse um problema pré-existente e que, esse problema apenas tivesse se despoletado agora.

Essa garantia serviria, por um lado, para ressarcir o utilizador do produto de quaisquer danos provocados pelo sistema desde que, o mesmo tivesse sido utilizado corretamente e não existisse a intervenção de terceiros e, por outro lado, proteger o produtor de uma responsabilização eterna.

Para além disso, permitiria ainda ao produtor, por um lado, a criação de um fundo de precaução para eventuais conflitos e, por outro, a possibilidade de evoluir e despender mais recursos na produção de novos produtos sem estar preocupado com as produções, criadas por si, há vinte anos atrás.

E se, a responsabilidade fosse atribuída ao proprietário utilizador do sistema de IA?

A segunda teoria é a que considera que, a responsabilidade deve recair sobre o utilizador do sistema.

Neste entendimento, a atribuição da responsabilidade ao proprietário ou utilizador pelos danos provocados pelo sistema IA assentaria na teoria que, este é que teria o maior proveito dessa fonte de risco e, como tal, deveria ser responsabilizado. Seria como a responsabilização de um dono pelo seu animal de estimação.

O terceiro entendimento baseia-se na divisão da responsabilidade entre o fabricante e o utilizador, tendo cada um deles uma cota-parte de responsabilidade, o primeiro pela criação defeituosa e o segundo pelo proveito que retira da utilização do sistema.

Neste sentido, e a título exemplificativo, no caso dos carros autónomos, Jeffrey K Gurney entende que, o produtor seria responsabilizado na totalidade dos danos se o veículo

se encontrasse em modo autónomo e transportasse um condutor com capacidades diminuídas e, parcialmente responsável, no caso de um condutor distraído.¹¹⁹

Este tipo de responsabilização não pode ser adotado desde logo porque, e abraçando já as novas tecnologias, reconhecendo a capacidade dos carros autónomos, não é por uma pessoa ter capacidades diminuídas que isso a impede de, por exemplo, escolher rotas perigosas. Para além disso, limitar a responsabilização de um condutor distraído levaria à criação de uma desresponsabiliza

O prolema deste sistema de responsabilidade iria ser a dificuldade na resolução e na prova da responsabilidade de cada um e, no caso de existir mais intervenientes, essa indecisão iria ser ainda maior.

Entendo que, o regime da responsabilização deveria ser tratado ao nível do regime da culpa do lesado do qual, quando um facto culposo do lesado tiver concorrido para a produção ou agravamento dos danos, a sua responsabilização dependeria da gravidade das culpas de ambas as partes e nas consequências que delas resultaram.

A quarta posição, atribui a responsabilidade à tecnologia em si. A questão é que, se a responsabilidade é da tecnologia então, primeiro deveria ser-lhe concedida personalidade jurídica, entendimento esse que, tal como já mencionado supra, não considero viável.

Em 2015, o Parlamento Europeu adotou uma resolução a convidar a Comissão a permitir a criação de um estatuto jurídico para robôs. Desta forma, iria ser possível responsabilizar robôs mais avançados pelos danos provocados.

Esta teoria foi rejeitada em 2020 pela CPE que adotou três resoluções sobre os aspetos éticos e legais dos sistemas de software de IA, a Resolução 2020/2012, na qual são enquadrados aspetos éticos na IA, robótica e tecnologias, A Resolução 2020/2014, sobre o regime de responsabilidade civil para a IA e, por fim, a Resolução 2020/2015, sobre direitos de propriedade intelectual para o desenvolvimento de tecnologias de IA. Estas resoluções reconheceram que a IA trará benefícios para variados setores, todavia, existem preocupações que o atual quadro jurídico europeu pode já não ser adequado para enfrentar eficazmente os riscos colocados pela IA, robótica e tecnologias relacionadas.¹²⁰

¹¹⁹ Ramos, Nuno André Novo, 2020. Responsabilidade civil em dano causado por mecanismo dotado de inteligência artificial, pág. 64.

¹²⁰ PANAGOPOULOU, Fereniki; PARPOULA, Christina; KARPOUZIS, Kostas, 2023, Legal and ethical considerations regarding the use of ChatGpt in education, pág. 5.

A proposta da Diretiva 2022/0303 (COD relativa à adaptação das regras de responsabilidade civil extracontratual à IA de 28 de setembro de 2022, criou uma presunção de causalidade refutável para eliminar a necessidade de prova por parte das vítimas, que caso contrário, teriam a obrigação de comprovar o nexo de causalidade entre a atividade do sistema IA e os danos ocorridos.¹²¹

Tem como objetivo o estabelecimento de uma base legislativa eficaz de forma a pedir uma indemnização relacionada com o facto culposo que consiste no incumprimento de um dever de diligência nos termos do direito da União ou do direito nacional.

Desta forma, a Diretiva elimina a dificuldade de prova por partes dos demandantes do nexo de causalidade entre o incumprimento e o resultado produzido pelo sistema de IA.

Neste sentido, o n.º 1 do art. 4.º, estabelece uma presunção de causalidade ilidível seletiva no que diz respeito a este nexo de causalidade. “Esta presunção é a medida menos onerosa para dar resposta à necessidade de uma indemnização justa da vítima.”¹²²

Os n.º 2 e 3 do supramencionado artigo distinguem as ações que são intentadas contra o fornecedor de um sistema de IA de risco elevado daquelas das que não são de risco elevado.

No caso de sistemas de IA de risco elevado o artigo 4.º, n.º 4 estabelece uma exceção à presunção de causalidade, que ocorre se, o demandando demonstrar que, estão razoavelmente acessíveis aos demandantes elementos de prova e conhecimentos especializados suficientes para provar o nexo de causalidade.

Esta obrigação leva ao incentivo do cumprimento das obrigações de transparência por parte dos produtores, assegurando um elevado nível de transparência da IA.

No caso de sistemas de IA que não são de risco elevado, o n.º 5 do art. 4.º, “estabelece uma condição para a aplicabilidade da presunção de causalidade, segundo a qual esta última depende de uma determinação do tribunal em como é excessivamente difícil para o demandante provar o nexo de causalidade. Tal dificuldade deve ser apreciada à luz das características de determinados sistemas de IA, como a autonomia e a opacidade, que, na prática, tornam muito difícil explicar o funcionamento interno do sistema de IA, afetando

¹²¹ Proposta de Diretiva do Parlamento e do Conselho 2022/0303 (COD) relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial, 28 de setembro de 2022, (Diretiva Responsabilidade IA).

¹²² Proposta de Diretiva do Parlamento e do Conselho 2022/0303 (COD) relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial, 28 de setembro de 2022, (Diretiva Responsabilidade IA).

negativamente a capacidade do demandante em provar o nexo de causalidade entre o facto culposo do demandado e o resultado da IA.”¹²³

Este tema sempre foi muito controverso, todavia, o grupo de peritos de alto nível afirma que, para que seja criada uma IA de confiança, é necessário criar mecanismos para assegurar a responsabilidade e a responsabilização pelos sistemas de IA dos seus resultados, tanto antes como depois, da sua adoção.¹²⁴

Uma das soluções para alcançar esta avaliação da responsabilização é a auditabilidade, que implica que, seja possibilitada a avaliação de algoritmos dados e processos de criação. É claro que, tal não implica a constante publicação de informações sobre os modelos de negócios e a propriedade intelectual relacionadas com o sistema IA. Apenas significa, o fácil acesso por auditores a esses relatórios de criação.

Deve ainda ser minimizado e comunicado os impactos negativos de determinado sistema IA devendo-se ainda, proteger os denunciadores que denunciem preocupações legítimas de determinado sistema IA.

Outra solução, é a criação de soluções de compromisso no sentido que devam ser identificados os interesses e valores envolvidos naquela criação de IA e avaliados os seus riscos para os princípios éticos.

Por fim, quando ocorrer um impacto adverso injusto deverão ser definidos mecanismos acessíveis para assegurar vias de recurso adequadas.¹²⁵

8.2.4 A justiça e equidade

Uma outra questão que a utilização de sistemas IA suscita é a da justiça e equidade. Ora, os sistemas de IA são muitas vezes utilizados para a tomada de decisões inclusive escolha de candidatos, projetos, entre outros.

O certo é que, estas decisões automatizadas são tomadas tão só e apenas com base nos dados puramente estatísticos ou factuais, o que poderá levar a decisões injustas ou desiguais. Aliás, tal desigualdade poderá ser, tão só e apenas, realizada pelo próprio programador que procedeu à inserção dos dados de forma a proporcionar a escolha de

¹²³ Proposta de Diretiva do Parlamento e do Conselho 2022/0303 (COD) relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial, 28 de setembro de 2022, (Diretiva Responsabilidade IA).

¹²⁴ PANAGOPOULOU, Fereniki; PARPOULA, Christina; KARPOUZIS, Kostas, 2023, Legal and ethical considerations regarding the use of ChatGpt in education, pág. 6.

¹²⁵ Grupo independente de peritos de alto nível sobre a inteligência artificial, 2019, Orientações éticas para um IA de confiança, pág. 27 e 28.

determinado candidato ou ação. Para além disso, podem ainda comprometer o respeito pela democracia e do Estado de direito.¹²⁶

Considera o grupo independente de peritos que, os sistemas de IA devem servir para manter os processos democráticos, não os devendo comprometer seja de que forma for respeitando os valores e escolhas¹²⁷ dos indivíduos.

Não devem ainda, comprometer os compromissos basilares do Estado de direito, bem como a legislação, regulamentação e compromissos fundamentais do mesmo.

8.2.5. A proteção de dados

Por fim, o problema pela utilização de sistemas IA, interesse desta tese é o da privacidade e proteção de dados.

Não esquecendo o já mencionado em todo este trabalho, importa mencionar algumas questões sobre este problema que assola a sociedade mundial, e quais as direções mencionadas pela EU nesse sentido.

O historiador e filósofo Yuval Harari levantou a seguinte questão: “O que acontecerá com a sociedade, a política e a vida cotidiana quando algoritmos não conscientes, mas altamente inteligentes, nos conhecerem melhor do que nós mesmos?”¹²⁸

Ora, já sabemos que para que um sistema possa aprender necessita de experiência, e o mesmo obtém-na através da informação que o alimentamos. Depois, dependendo daquilo que o sistema produz será escolhido o tipo de dados que o mesmo irá utilizar

Dados pessoais significam, tal como veremos mais à frente, qualquer informação que identifique, ou que torne identificável, uma pessoa. Os dados podem ser ligados a uma pessoa diretamente (nome, morada) ou indiretamente, o que significa que com a combinação de mais de um dado seja possível identificar a pessoa (cultura, genética, características físicas).¹²⁹

O direito à privacidade, tal como já enunciado ao longo deste trabalho, é um direito fundamental que é particularmente afetado pelos sistemas de IA. Está interligado

¹²⁶ Colóquio Tribunais e inteligência artificial – uma odisséia no século XXI, 12 de maio de 2023, 01:29:15 até 01:49:05.

¹²⁷ Grupo independente de peritos de alto nível sobre a inteligência artificial, 2019, Orientações éticas para um IA de confiança, pág. 16.

¹²⁸ HARARI, Yuval Noah, 2017, Homo Deus: A Breaf History of Tomorrow.

¹²⁹ The Norwegian Data Protection Authority, 2018, Artificial intelligence and privacy, pág. 15.

diretamente ao princípio da prevenção de dados, uma vez que, é sobretudo sobre a necessidade de utilização de dados pelos sistemas de IA que a privacidade é afetada.

O grupo independente de peritos entende que, desde logo, é necessário um controlo adequado dos dados para que assegurem a qualidade e a integridade dos dados utilizados, seja por forma de protocolos de acesso, de eliminação de dados, entre outros.

Por isso, os sistemas de IA devem ser concebidos de forma a garantir a privacidade e a proteção de dados, incluindo informações fornecidas pelo utilizador, quem a título inicial, quer durante a utilização do sistema.

Tudo o que seja, ou leve, a informações dos utilizadores deve ser protegido, tais como, as preferências dos indivíduos, mas também a sua orientação sexual, idade, convicções religiosas, entre outras. Acresce que, para que seja possível confiar nos sistemas IA é necessário assegurar-se o respeito pelos dados recolhidos, para evitar discriminações ou injustiças e manter a qualidade e integridade dos dados.

A ideia é que, quando são recolhidos dados e os mesmos contenham enviesamentos socialmente construídos, inexatidões, erros e enganos esses problemas sejam resolvidos antes de treinar o sistema com um determinado conjunto de dados. O mesmo se aplica a dados maliciosos.

Acresce ainda que, o processo de aprendizagem durante a criação do sistema IA deve ainda ser documentado por fases para que todo o processo de treinamento seja conhecido.

Por fim, qualquer empresa de criação de sistemas de IA deve adotar protocolos de governação de acesso aos dados. Esse acesso apenas deverá ser permitido a pessoal devidamente qualificado. ¹³⁰

9. O ChatGpt, questões ético-jurídicas

O *ChatGPT* é uma tecnologia, criada pela *OpenIA* de Elon Musk, que utiliza técnicas avançadas de inteligência artificial para gerar conversas e aprender com a informação recebida.

É um protótipo de um *chatboot*, ou seja, é um robot com inteligência artificial especializado em diálogos virtuais.

¹³⁰ Grupo independente de peritos de alto nível sobre a inteligência artificial, 2019, Orientações éticas para um IA de confiança, pág. 24.

Embora esta tecnologia seja extremamente inovadora, levanta várias questões sobre possíveis impactos que possa ter, não só em *ciber* segurança, mas também nas escolas, trabalhos, informação e principalmente na proteção de dados.¹³¹

Esta tecnologia funciona através de um modelo de linguagem baseado em *machine learning*, um sistema de conversação inteligente que usa a tecnologia de processamento de linguagem natural para entender o que é pedido e responder de forma a que seja compreendida pelo utilizador.

O *ChatGPT* é composto por várias camadas de transformadores, cada transformador é concebido para processar sequencialmente dados de forma a criar um diálogo natural. Para que este chat evolua é necessário a inserção uma grande quantidade de dados, de forma a que o mesmo absorva a informação e aprenda padrões, relações entre palavras e frases.

O processo de aprendizagem, *deep learning*, é realizado constantemente sempre que o chat absorve mais dados. Uma vez predefinido, o chat pode ser utilizado em variadas tarefas e fins. Mais, como procede ele mesmo à constante aprendizagem, o mesmo quase não necessita de intervenção direta para se desenvolver, procedendo à busca e recolha das informações.

O processo de aprendizagem do *ChatGpt* pode ser dividido em três passos. No primeiro passo encontra-se o modo de utilização base do chat, no sentido em que são adicionados dados básicos para ensinar o modelo. Já no segundo, os dados são acumulados para treinar o mesmo. E, por fim, no terceiro o próprio modelo utiliza o *self learning* para evoluir.¹³²

Uma vez que, este chat realiza conversas e responde a questões considereí que nada seria melhor do que perguntar ao próprio chat como ele aprende.

O mesmo respondeu que aprende através de um processo chamado *pre-training* e *fine-tuning*, o que necessita de uma grande quantidade de dados de texto e de algoritmos complexos.

Na fase de *pre-training*, o mesmo é alimentado por uma grande quantidade de dados de texto da internet. Após isso, o chat prevê as palavras seguintes com base no contexto das anteriores e assim, aprende gramática, factos, habilidades, entre outros.

¹³¹ DINESH Kalla; NATHAN Smith, 2023, Study and Analysis of Chat GPT and its Impact on, pág. 327.

¹³² DINESH Kalla; NATHAN Smith, 2023, Study and Analysis of Chat GPT and its Impact on, pág. 327.

Após isso, passa para a fase do fine-tuning, onde revisores inserem novos dados, mais específicos, de forma a aprimorar e moldar as respostas do mesmo.

O chat adverte, no entanto, que aprende de forma padronizada, que não tem consciência, compreensão ou pensamento independente, pelo que, as respostas do mesmo são baseadas em padrões.¹³³

Ora, a verdade é que, este chat há três meses atrás já detinha mais de 100 milhões de utilizadores, o que significa que, a aderência ao mesmo é avassaladora.

O facto de possibilitar respostas rápidas, coerentes e, na sua grande maioria, corretas, permitiu a rápida aderência a esta tecnologia.

Resultado de tudo isto, é a criação de uma tecnologia com conteúdo complexo que imita a criatividade humana.

É certo que, na maioria das vezes este chat consegue desempenhar melhor as tarefas que um ser humano, o que não surpreende, tendo em conta a capacidade de memorização e avaliação característica do mesmo.¹³⁴

O *ChatGPT* serviu de base para a criação de variados chats para inúmeros fins como por exemplo, e no âmbito do direito, o *LawGPT*.

Este chat, já utilizado na justiça portuguesa, utiliza um processador de linguagem natural e algoritmos de *machine learning* para ajudar na criação de documentos legais online.

Basicamente, o chat funciona através da inserção de específicas informações e instruções para o documento que desejam que o chat crie. Depois, o sistema processa o pedido e cria um documento adequado às necessidades do utilizador. Este sistema pode criar, em apenas alguns segundos, variados tipos de documentos legais, incluindo contratos, cartas, pesquisas legais entre outras.

Os modelos GPT têm potencial de realização de variadas tarefas jurídicas tais como:

- Procura Jurídica: neste caso, podem ser utilizados para realizar pesquisas nas bases de dados legais, podendo ainda, pesquisar outros recursos relevantes como doutrinas, jurisprudência e fornecer ainda informações relevantes sobre determinados temas jurídicos;

- Análise de contratos: estes modelos são utilizados na análise de contratos e outros documentos legais, podendo identificar cláusulas-chave certas ou erradas e termos;

¹³³ ChatGpt, OpenAI, consultável em <https://chat.openai.com/>.

¹³⁴ Colóquio Tribunais e inteligência artificial – uma odisseia no século XXI, 12 de maio de 2023, 1:08:40, consultável em <https://www.stj.pt/?p=17432>.

- Análise preditiva: podem ser usados para analisar grandes documentos jurídicos de forma mais rápida e precisa que um humano, conseguindo prever resultados prováveis de um caso.

- Redação de documentos legais: são ainda utilizados para a realização de documentos jurídicos como contratos, petições e peças processuais, ajudando a que os documentos contenham linguagem precisa e clara.

- *Chatbots* jurídicos: foram criados com o intuito de responder precisa e corretamente a questões jurídicas, direcionando os utilizadores para os recursos jurídicos adequados.¹³⁵

A título exemplificativo, inscrevi-me no LawGPT com o intuito de verificar se, mesmo com a informação mais básica, o mesmo era capaz de criar um texto.

Por isso, nos variados campos para a colocação de informação coloquei que pretendia o texto em português (existindo a possibilidade da criação do mesmo em variadas línguas), e apenas as seguintes palavras: pagamento a prestações, emprestei 5.000€, falta de pagamento.

O chat, em questão de segundos criou o seguinte:

“[Cabeçalho do seu escritório de advocacia]

[Data]

[Informações de contacto do destinatário]

Assunto: Exigência de pagamento de prestação em atraso

Estimado/a [Nome do Destinatário],

Escrevo-vos em representação do meu cliente [Nome do Cliente], referente a uma disputa pelo não pagamento de prestação financeira, a qual, desafortunadamente, você está em atraso.

Os factos da disputa são os seguintes: o meu cliente emprestou a quantia de 5000€ a você, com o entendimento que se procedesse ao pagamento de forma prestacional de acordo com o contrato estabelecido entre ambas as partes.

Contudo, apesar dos lembretes múltiplos e dos avisos, o meu cliente não recebeu nenhum pagamento até ao momento presente. Esta situação gerou danos significativos, financeiros e de confiança, para o meu cliente.

¹³⁵ Law Chat GPT <https://lawChatGpt.com/>

A resolução que solicitamos é bastante simples: proceder ao pagamento imediato de todas as prestações em atraso. Caso contrário, estaríamos forçados a prosseguir com acções legais para assegurar os direitos do meu cliente.

Com esta carta, esperamos chamar a vossa atenção para a gravidade da situação e vossa obrigação em resolver a mesma imediatamente.

Solicito assim, a vossa atenção para este assunto com a maior brevidade possível. Para quaisquer questões adicionais ou esclarecimentos, sinta-se à vontade para entrar em contacto com o nosso escritório.

Atenciosamente,

[Seu nome]

[Suas Informações de Contacto]

[Apelido, Endereço, Telefone, Email]

Por favor, considere esta carta uma advertência formal e um pedido para resolver o assunto pendente.

Este é o último recurso do meu cliente antes de levar o assunto aos tribunais. Gostaríamos de resolver este problema de forma amigável, mas se o pagamento não for efectuado dentro de um prazo razoável, teremos que defender os direitos do nosso cliente da única maneira que nos restará.

Agradeço a vossa pronta ação neste assunto.

Atenciosamente,

[Seu nome]¹³⁶

O certo é que, esta tecnologia consegue criar textos explicando contextos e muitas vezes inserindo a legislação adequada. E pergunta-se: é totalmente precisa? Não, mas já tem um começo.

Qualquer um pode ter acesso a esta tecnologia e, através do machine learning a mesma melhora a cada interação.

Para a utilização inteligente desta tecnologia é fundamental, desde logo, ter um conhecimento básico da língua em que se deseja comunicar. Para além disso, as perguntas a realizar devem ser concisas, diretas e claras para que não haja divergência na análise da informação pelo *chatboot*.

¹³⁶ Law Chat GPT <https://lawChatGpt.com/>

Acresce que, o *chatboot* apenas consegue dar uma informação ou criar uma peça de forma correta se o contexto inserido contenha informações suficientes para que o modelo possa fornecer uma resposta precisa.

Por fim, é necessário ter sentido crítico e analisar as respostas oferecidas por este *chatboot* avaliando as mesmas com base na experiência e no conhecimento e, utilizar o mesmo com responsabilidade ética, evitando questões que possam prejudicar outros. Por exemplo, no que concerne aos chats jurídicos, geram, de certa forma, uma sociedade desigual no sentido de que, apenas os especialistas conseguirão tirar proveito dos mesmos uma vez que o cidadão comum não vai ter sentido crítico e desta forma, averiguar se a informação se encontra correta¹³⁷

No entanto, o que estes chats têm de maravilhoso e inovador, têm de perigoso.

Quando estes chats são utilizados por empresas para o atendimento ao cliente. O que acontece é que, na maioria das vezes, o cliente não faz a mínima ideia de que se contra a comunicar com um robô.

Para além disso, os utilizadores dos chats não são informados de como os primeiros chegaram àquela conclusão.

É necessário, portanto, que estes chats sejam desenhados para conseguir demonstrar como chegaram a determinada conclusão, o que muitas das vezes não ocorre.

Ao nível da privacidade, a inserção de dados pessoais ou análise de documentos legais representa um risco para a privacidade, uma vez que o chat, ainda que por breves segundos, absorve toda a informação inserida incluindo dados pessoais dos utilizadores. Para além disso, os chats, ainda que garantam a não memorização das conversas, o certo é que os mesmos não se responsabilizam por fugas de informação.

Ao nível da responsabilidade, a utilização deste chat não é capaz de criar assumir uma responsabilidade legal pelas informações e peças que fornece.

Ora, isso levanta problemas também ao nível da responsabilidade civil, na medida em que, o chat poderá dar informações incorretas ou criar até, no caso do direito, peças processuais inadequadas ao cliente, o que pode provocar lesões ao mesmo.

¹³⁷ Colóquio Tribunais e inteligência artificial – uma odisséia no século XXI, 12 de maio de 2023, 01:29:15 até 03:30:05, consultável em <https://www.stj.pt/?p=17432>.

O certo é que, qualquer um destes chats não se responsabiliza por todo e qualquer erro por ele praticado. Ou seja, tudo o que seja repostas erradas ou inadequadas a responsabilidade pela utilização das mesmas vai recair tão só e apenas ao utilizador.

Por isso, existe a controvérsia de saber a quem recai a responsabilidade pela entrega de respostas erradas pelo ChatGpt, tema discutido no ponto 8.2.3 do presente trabalho.

As quatro teorias continuam a ser aplicadas sendo apenas alterada a base pelo qual lhe é atribuída a responsabilidade.

Neste caso, sobre a primeira posição, que atribui a responsabilidade aos criadores dos chats, o fundamento de responsabilidade será, de forma igual, o já enunciado no ponto 8.2.3. Ou seja, a responsabilidade poderá ser alcançável através do estabelecimento de uma presunção ilidível que preveja que, em caso de dúvida, os fabricantes serão considerados responsáveis.

Todavia, aqui não se poderia utilizar a questão da garantia uma vez que, a propriedade do chat não seria transferida para cada um dos utilizadores. Neste caso, o chat, munido de sistemas IA, seria uma exceção a este entendimento.

A segunda teoria é a que considera que, a responsabilidade deve recair sobre o utilizador do chat. Este entendimento considera que, deve ser o utilizador a verificar se a proposta recebida é a adequada ao caso em concreto. Aqui, adotar-se-ia o entendimento que o julgamento humano prevalece sobre a decisão do algoritmo em caso de dúvida.

Esta teoria não está, no meu entender, completamente errada, uma vez que, o utilizador tem conhecimento que se encontra a utilizar uma tecnologia que, afirma não ser precisa ou 100% correta. Pelo que, o mesmo deve fazer uso do seu sentido crítico de forma a confirmar a veracidade da informação transmitida pelo chat. Se não o faz, corre o risco de ser responsabilizado pelo dano provocado na utilização das informações transmitidas pelo chat.

Todavia, considero que, a não responsabilização do controlador do chat levaria a uma impunibilidade pela criação de uma tecnologia defeituosa e incompleta.

O terceiro entendimento baseia-se na divisão da responsabilidade entre o fabricante e o utilizador, tendo cada um deles uma cota-parte de responsabilidade, o primeiro pela criação defeituosa e o segundo por não verificar a veracidade dos casos em apreço. O prolema deste sistema de responsabilidade iria ser a dificuldade na resolução e na prova da

responsabilidade de cada um e, no caso de existir mais intervenientes, essa indecisão iria ser maior.

A quarta posição atribui a responsabilidade à tecnologia em si. A questão é que, se a responsabilidade é da tecnologia então primeiro deveria ser-lhe concedida personalidade jurídica, questão já discutida no ponto 8.2.3 e que, mesmo neste assunto, considero que não se deva aplicar.

No meu entender, a responsabilidade por danos provocados por este chat nem sequer deveria de ser subsumida na mesma legislação dos outros sistemas de IA.

Estes chats são sistemas extremamente complexos e muito mais avançados que a maioria das tecnologias. Por isso, necessitaria de uma legislação própria, de forma a assegurar o controlo e proteção dos utilizadores.

Por outro lado, o facto da utilização em massa destes chats pode levar à lavagem cerebral dos seus utilizadores através de, por exemplo, dados maliciosos que podem causar em resultados maliciosos. Basta o chat aprender a partir de dados históricos ou até existir o *hakeamento de um chatboot* e, a consequente inserção de uma informação falsa ou caluniosa para criar ou perpetuar uma ideia discriminatória ou desigual.

Estes chats podem, por isso, provocar discriminação e ser influenciados pelo preconceito na medida em que é treinado com bases de dados retiradas da internet e histórico de interações, o que pode levar a respostas e aconselhamentos que não são justos ou precisos para todas as partes.

Se, por exemplo, utilizarmos o *ChatGpt* para pedir uma *odd* de um presidente se ele for de uma determinada religião o chat pode fazê-lo, todavia se ele for de outra religião o chat pode recusar-se a fazê-lo.¹³⁸

Com o lançamento do *ChatGpt*,(LLMs) alterou-se a maneira como pensamos e vivemos.

É verdade que a UE foi das primeiras a legislar sobre modelos de IA, no entanto, esta legislação não está nem de perto preparada para regular os LLMs.

Outro dos problemas deste chat é que a informação que é enunciada por ele não é verificada podendo levar a erros. Como exemplo disso, temos o problema chamado “hallucination” ou “stochastic parrots”, ocorrendo quando o chat cria texto baseado em

¹³⁸ Colóquio Tribunais e inteligência artificial – uma odisseia no século XXI, 12 de maio de 2023, 01:29:15 até 03:30:05, consultável em <https://www.stj.pt/?p=17432>.

padrões internos na vez do verdadeiro contexto da conversa, no caso do primeiro e quando, há a repetição dos dados de treino na vez da necessária compreensão do contexto.¹³⁹

Um outro problema, que surge com a utilização destes chats é a questão do plágio. O problema da interação com estes chats é que a informação entregue por estes modelos tecnológicos é retirada livremente da internet e sem qualquer referência bibliográfica. Ora, se o utilizador utilizar essa informação, cuja autoria é assegurada pelo chat, também ele estará a atribuir a autoria a algo que na realidade não criou essa informação.

Neste contexto, surge ainda a questão de quem é o autor do trabalho final do chat.

A obra poderá ser do criador do software com IA? Esta posição é a melhor pelo facto de que a inserção da informação no modelo não significa que o mesmo contenha a autoria dessa informação.

Será do criador da infraestrutura do software? Desta vez, no contexto da propriedade intelectual e não como direitos de autor? Neste sentido, a própria criação intelectual poderia pertencer ao utilizador do recurso criativo artificial.

Ou a obra criada será um bem de domínio público uma vez que as máquinas não podem criar obras intelectuais?

Nenhuma das soluções se afigura a mais adequada uma vez que tudo dependerá do contexto da obra criada.¹⁴⁰ (Panagopoulou, Parpoula, & Karpouzis, 2023)

A criação pelo modelo é livre, no entanto, questiona-se se a criação do software está abrangida pela liberdade de escolha. Ou seja, se eventualmente quando submetemos uma pergunta ao software e ele decidir qual a resposta a ser enviada e essas repostas forem de conteúdo ofensivo ou calunioso, no caso de serem consideradas como uma expressão do software, então qualquer governo que tentar regular essa resposta poderá ser considerada censura?¹⁴¹

Ora, é certo que estes avanços tecnológicos são uma mais valia para o quotidiano da sociedade, no entanto, é necessário termos consciência dos riscos que os mesmos criam na nossa privacidade.

¹³⁹ LI, Zihao, 2023, The Dark Side of ChatGpt: Legal and Ethical Challenges from Stochastic, pág. 2.

¹⁴⁰ PANAGOPOULOU, Fereniki; PARPOULA, Christina; KARPOUZIS, Kostas, 2023, Legal and ethical considerations regarding the use of ChatGpt in education pág. 6.

¹⁴¹ PANAGOPOULOU, Fereniki; PARPOULA, Christina; KARPOUZIS, Kostas, 2023, Legal and ethical considerations regarding the use of ChatGpt in education pág. 6.

A legislação aplicável deve ser flexível e adaptável para ir acompanhando estas alterações tecnológicas, mas mantendo alguma rigidez na maneira como estes princípios tecnológicos agem e utilizam os nossos dados.

9.1. O ChatGpt e a proteção de dados

O *ChatGpt*, tal como já enunciado anteriormente, utiliza técnicas avançadas de IA para gerar conversação e aprender com a informação recebida.

O mesmo iniciou a sua atividade em 2021 e, nessa altura, recolhia todo e qualquer dado pessoal sem sequer pedir autorização aos seus utilizadores. O certo é que, tal ato foi descoberto na Itália e o governo italiano decidiu investigar a situação, tendo até equacionado a não permissão deste chat naquele país. Todavia, a aderência ao mesmo não abrandou nem um pouco começando o mesmo a ser utilizado por utilizadores e empresas.

Aliás, a Autoridade Italiana de Proteção de Dados ordenou a restrição temporária do tratamento de dados de utilizadores italianos contra a *OpenAI* e, paralelamente, iniciou uma investigação para verificar o cumprimento das medidas de proteção de dados.

Ora, a partir daí a *OpenAI* criou processos de identificação e pedidos de consentimento da utilização de dados. No entanto, não se sabe a quantidade de dados pessoais recolhidos ou quais foram os utilizadores que sem o seu conhecimento entregaram dados pessoais.

Neste seguimento, urge a necessidade de avaliar a situação do *ChatGpt* e da proteção de dados.

Nada melhor, no âmbito do estudo do *ChatGpt*, do que perguntar ao próprio chat quais são as medidas que o mesmo adota na proteção de dados.

Perguntei, por isso, ao *ChatGpt* como ele procedia ao armazenamento dos meus dados pessoais. O mesmo respondeu que, não armazena qualquer dado pessoal, a não ser que os mesmos sejam inseridos aquando da conversa. Uma vez terminada a sessão, o mesmo afirma que não retém qualquer dado. Afirma ainda que, a *OpenAI* leva o tema da proteção de dados de forma muito séria e que, o chat é concebido à volta do não armazenamento de informação pessoal a não ser que seja absolutamente necessário para a conversa.

Perguntei ainda, como o mesmo procedia à proteção dos meus dados ao que o mesmo respondeu que o tema da proteção de dados era uma preocupação importante na era digital.

Neste sentido, o chat enumerou várias medidas e práticas que as empresas e as organizações implementam para proteger os dados pessoais como a criptografia, o acesso

restrito, a proteção de rede, as atualizações regulares de segurança, políticas de privacidade transparentes, consentimento informado, anonimização de dados, monitoramento e detecção de ameaças, treinamento de funcionários e até leis de proteção de dados. O certo é que, apenas enumerou o que as outras empresas faziam não tendo de forma alguma afirmado que esses atos eram os que o mesmo também praticava. Este acontecimento pode ter ocorrido devido a lapso de escrita por parte do chat, no entanto, tal facto não me permite indicar quais as medidas aplicadas pelo mesmo.

O chat afirmou que a proteção de dados pessoais é uma responsabilidade partilhada entre as empresas e os utilizadores, pelo que era necessário que os utilizadores estivessem cientes de como os dados eram recolhidos e usados, tomando medidas para proteger a própria privacidade.

Perguntei ainda se, durante a conversa em causa poderia existir a possibilidade de hackeamento da mesma, ao que o mesmo respondeu que implementava medidas de segurança para proteger conversas e dados dentro das suas plataformas (quais medidas? não respondeu) mas, que não podia assegurar com absoluta certeza que era 100% vulnerável a ataques.

Afirma ainda que, depois de regenerar a questão, que a *OpenAI* utiliza como práticas de segurança cibernética a criptografia de dados em trânsito e em repouso, proteção de acesso, monitoramento de ameaças e atualizações regulares de segurança.

No dia 25 de abril deste ano, a *OpenAI* divulgou um anúncio no *ChatGpt* do qual introduziu a possibilidade de os utilizadores desativarem o histórico desse chat.

Afirmou ainda que, devido a isso, as conversas deixariam de ser utilizadas para o treino dos seus modelos. Desta forma a *OpenAI* espera que esta medida seja mais adequada à proteção de dados do que as anteriormente elaboradas.

Quando o chat estiver desligado as conversas serão armazenadas por 30 dias para efeitos de monitorizar abusos e, depois eliminadas permanentemente.¹⁴²

Após a análise desta publicação surgiu uma dúvida. Se o chat, tal como supramencionado, em conversa, assegurou o não armazenamento ou aprendizagem através

¹⁴² “We've introduced the ability to turn off chat history in ChatGpt. Conversations that are started when chat history is disabled won't be used to train and improve our models, and won't appear in the history sidebar. These controls, which are rolling out to all users starting today, can be found in ChatGpt's settings and can be changed at any time. We hope this provides an easier way to manage your data than our existing opt-out process. When chat history is disabled, we will retain new conversations for 30 days and review them only when needed to monitor for abuse, before permanently deleting”, New ways to manage your data in chat GPT, disponível em <https://openai.com/blog/new-ways-to-manage-your-data-in-ChatGpt>.

das conversas realizadas, então porque é que a *OpenAI*, criadora do chat, publica uma notícia afirmando que a partir do mês de maio, e após a desativação do histórico do chat pelo utilizador, o mesmo vai deixar de aprender a partir das conversas efetuadas?

Isto significa que, o histórico de conversas, que alegadamente era armazenado apenas durante a utilização, estava a ser guardado e utilizado para treinar e melhorar os modelos de chat. E ainda que, não seja suposto inserir dados pessoais na conversa o certo é que, quando isso ocorre, o chat vai armazenar como dados de aprendizagem.

A *OpenAI* anuncia ainda que, os mesmos encontravam-se a tentar melhorar a subscrição do *ChatGpt business* para profissionais que necessitam de maior controlo sobre os seus dados.¹⁴³

Estes anúncios demonstram que, ao contrário daquilo que o chat assegura, não há ainda segurança suficiente, em matéria de proteção de dados, que permita a utilização diária ou até profissional dos mesmos.

A utilização dos LLMs, principalmente por crianças, levanta preocupações no que concerne proteção da privacidade e à segurança de dados principalmente considerados sensíveis.

Tal como já mencionado, o funcionamento destas tecnologias necessita de recolha e processamento em massa de dados, o que torna difícil o seu controlo. Além disso, estes chats, dotados de IA, muitas vezes superam as expectativas dos seus criadores e isso torna-os difíceis de controlar.

Para além disso, o facto destas tecnologias serem muito recentes não existe ainda grandes investigações sobre as mesmas o que torna a informação sobre elas muito escassa e imprecisa.

E, as imprecisões das respostas dadas por entidades como a *OpenAI* e a possibilidade de acesso a dados pessoais, no que respeita à proteção de dados, retira a confiança que já foi atribuída a outras tecnologias IA pré-existentes.

¹⁴³ “We are also working on a new ChatGpt Business subscription for professionals who need more control over their data as well as enterprises seeking to manage their end users. ChatGpt Business will follow our API’s data usage policies, which means that end users’ data won’t be used to train our models by default. We plan to make ChatGpt Business available in the coming months.

Finally, a new Export option in settings makes it much easier to export your ChatGpt data and understand what information ChatGpt stores. You’ll receive a file with your conversations and all other relevant data in email.” OpenIA, New ways to manage your data in ChatGpt, disponível em <https://openai.com/blog/new-ways-to-manage-your-data-in-ChatGpt>.

No que concerne ao RGPD, o mesmo quando foi desenvolvido não foi intimamente criado para prever situações de mutações da IA, por isso, há quem acredite que o mesmo é flexível o suficiente para ser aplicado a essas situações e quem considere que é necessário a criação de legislação própria para evitar lacunas e assegurar a proteção dos dados.

Independentemente da divergência doutrinal, a União Europeia prevê apresentar um projeto de lei para regulamentar a Inteligência Artificial (IA), de forma a incluir todas as mutações derivadas da mesma.

Até lá, o RGPD é a base que dita os requisitos mínimos para que os dados dos utilizadores sejam protegidos, havendo o risco de poder se revelar como insuficiente para a complexidade deste tema.¹⁴⁴

10. O regulamento geral de proteção de dados

10.1 A proteção de dados na europa

É indiscutível a importância do papel do Regulamento Geral de Proteção de Dados na proteção dos dados pessoais.¹⁴⁵

Com o aumento da recolha de dados pessoais, a dificuldade de proteção dos mesmos pelas entidades, a necessidade do reforço das competências das autoridades no controlo tornou-se imprescindível a criação de uma legislação que regulasse toda a situação.

Manuel Carlos Lopes Porto refere que, para além de outros, um dos compromissos que a União Europeia assumiu aquando da sua formação foi a criação de uma sociedade assente na informação.¹⁴⁶

Ora, para que isto fosse possível, era imperativo o estabelecimento de matérias de proteção de dados estabelecidas e que essas medidas fossem transversais a todos os Estados Membros.

A diretiva 95/46/CE foi criada considerando que “os sistemas de tratamento de dados estão ao serviço do homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares, independentemente da sua nacionalidade ou da sua residência, especialmente da vida privada” que “o recurso ao tratamento de dados pessoais nos diversos

¹⁴⁴ SILVA, Joana Vaz, 16 de abril de 2023. A batalha do séc. XXI? – Chat GPT vs Proteção de dados. Review for Direito Criativo. Disponível na Internet em: <https://direitocriativo.com/a-batalha-do-sec-xxi-chat-gpt-vs-protecao-de-dados/>.

¹⁴⁵ Regulamento (UE) 2016/679 do Parlamento e do Conselho de 27 de Abril de 2016. Segundo o art. 99º entrou em vigor “no vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia”, no dia 4 de Maio de 2016, tendo o n.º 2 acrescentado do mencionado artigo acrescentado que o mesmo apenas entraria em vigor que o mesmo só seria aplicável no dia 25 de Maio de 2018.

¹⁴⁶ PORTO, Manuel Carlos Lopes, Teoria da Integração e Políticas da União Europeia, 2016, pág. 455

domínios das atividades económicas e sociais é cada vez mais frequente na comunidade”, que “o progresso registado nas tecnologias da informação facilita consideravelmente o tratamento e a troca dos referidos dados.” e que “para eliminar obstáculos à circulação de dados pessoais, o nível de proteção de direitos e liberdades das pessoas no que diz respeito ao tratamento desses dados deve ser equivalente em todos os Estados-membros”¹⁴⁷.

Desta forma, e considerando que, para o funcionamento do mercado interno é necessário a livre circulação de mercadorias, pessoas, serviços e capitais, e para que isso possa ocorrer, a livre circulação de dados deve ser permitida, por um lado, mas por outro, devem ser protegidos os direitos fundamentais das pessoas.¹⁴⁸

A diretiva 95/46/CE abriu caminho para a criação e aprovação do Regulamento Geral de Proteção de Dados.

Aliás, foi neste sentido que o RGPD foi consagrado. No dia 13 de maio de 2014, no Proc. C-131/12, um Ac. contribuiu substancialmente para a criação da responsabilidade do motor de buscar na proteção de dados do utilizador ainda que, estes tenham sido recolhidos por sites de terceiros. Assim, de acordo com esse Ac., na sequência de uma pesquisa realizada a partir do nome de uma pessoa, e a lista de resultados exibir uma ligação para uma página que contiver dados sobre essa pessoa, esta pode dirigir-se diretamente ao motor de busca ou às autoridades competentes para a supressão dessa ligação da lista de resultados.

Desta forma, criou-se a possibilidade aos utilizadores de solicitarem aos motores de busca o apagamento de links ou informações que surjam através de pesquisa no seu nome.¹⁴⁹

10.2 O regulamento geral de proteção de dados

Tal como enuncia o n.º 2 do art. 288º do TFUE, o regulamento tem carácter geral, sendo obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados Membros.¹⁵⁰

O RGPD tem como “objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.”

¹⁴⁷ Considerandos n.º 2, 4 e 8 da Diretiva 95/46/CE.

¹⁴⁸ Considerando n.º 3 da Diretiva 95/46/CE.

¹⁴⁹ Ac. do Supremo Tribunal Europeu Proc. C-131/12 disponível em <https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT>.

¹⁵⁰ n.º 2 do artigo 288º do TFUE

Resumidamente, este regulamento pretende assegurar de proteção das pessoas singulares e, ao mesmo tempo, possibilitar o desenvolvimento e livre circulação de dados pessoais no mercado.

Pretende, desta forma, assegurar a segurança jurídica e a transparência aos operadores económicos, incluindo as micro, pequenas e médias empresas, possibilitando assim o mesmo nível de proteção judicial e impondo obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes, garantindo assim, um controlo coerente do tratamento de dados pessoais, sanções equivalentes em todos os Estados-Membros, bem como a cooperação efetiva entre as autoridades de controlo dos diferentes Estados-Membros.¹⁵¹

Foi criado como resposta à proteção de dados fruto da galopante evolução tecnológica e aos novos desafios criados pela partilha de dados pessoais e consequente necessidade de proteção de dados pessoais.

A utilização pelas empresas privadas e entidades públicas das novas tecnologias instigou a uma grande utilização de dados, levando as pessoas singulares a disponibilizarem constantemente as suas informações pessoais. Pelo que, ainda que as empresas beneficiem destes dados, é necessária uma proteção dos mesmos para evitar danos nos direitos à privacidade e integridade da pessoa humana.¹⁵²

Este regulamento atribui ainda, aos Estados-Membros, segundo o n.º 10 dos considerandos, possibilidade de criarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados. Desta forma, o presente regulamento não coloca de lado o direito dos Estados-Membros permitindo uma maior definição de possíveis situações de tratamento em que é ou não lícito o tratamento de dados pessoais. *o direito dos Estados.*¹⁵³

Surge assim, como uma resposta à atual necessidade de criação de um quadro normativo mais sólido e coerente.¹⁵⁴

Este regulamento veio desenvolver e expandir as normas, princípios e direitos estabelecidos na Diretiva 95/46/CE, principalmente no que concerne ao consentimento e à notificação da violação dos direitos dos titulares de dados pessoais.

¹⁵¹ Considerandos n.º 2 e 13 do RGPD.

¹⁵² Considerando n.º 6 do RGPD.

¹⁵³ Considerando n.º 10 do RGPD.

¹⁵⁴ Considerando n.º 7 do RGPD.

10.3 Os dados pessoais

A Diretiva e o Regulamento estabeleceram que os princípios da proteção de dados aplicam-se a todo e qualquer “tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinado”.¹⁵⁵

A Diretiva 95/46/CE entendia por dados pessoais: “qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um n.º de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social”.¹⁵⁶

Já no RGDP, a identificação do titular dos dados pessoais é alargada podendo abranger os identificadores por via eletrónica fornecidos por aplicações, ferramentas ou aparelhos.¹⁵⁷

A CE, definiu ainda, o conceito de dados pessoais como a “informação relativa a uma pessoa viva, identificada ou identificável”.¹⁵⁸

Acrescenta ainda que, dados como conjuntos de informações distintas, que podem levar à identificação de uma pessoa e ainda, dados que tenha sido descaracterizados, codificados ou pseudonimizados, mas que, no entanto, possam ser utilizados para identificar uma pessoa são ainda dados abrangidos pelo regulamento.

Apresenta ainda, exemplos do que integra o conceito de dados pessoais: tais como o nome, endereço, endereço de correio, número cartão de identificação, localização, um endereço IP, cookies, o indentificador de publicidade dos telemóveis, dados retidos num hospital e qualquer dado que possa identificar uma pessoa, entre outros.¹⁵⁹

¹⁵⁵ Art. 2º do RGPD.

¹⁵⁶ Al. a) do artigo n.º 2 da Diretiva 95/46/CE.

¹⁵⁷ “(...) tais como endereços IP (protocolo internet) ou testemunhos de conexão (cookie) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares.”, considerando n.º 30 do RGPD.

¹⁵⁸ CE, O que são dados pessoais?, consultável em https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_pt

¹⁵⁹ CE, O que são dados pessoais?, consultável em https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_pt

É importante salientar que, os dados pessoais que tenham sido pseudonomizados e encriptados, que ainda possam ser utilizados para identificar uma pessoa, encontram-se ainda dentro do âmbito do RGPD.¹⁶⁰

Por todo o exposto, é possível afirmar que, os dados pessoais que se encontram fora do âmbito de proteção do RGPD são que tenham sido anonimizados e que esse processo seja irreversível.¹⁶¹

O art. 9º do RGPD alargou as categorias de dados pessoais sensíveis expostos na Diretiva 95/46/CE, proibindo 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.¹⁶²

A proteção dos dados pessoais sensíveis mereceu pelo RGPD uma maior proteção na medida em que, estes, pela sua natureza, caso sejam afetados, possam implicar riscos significativos para os direitos e liberdades fundamentais.¹⁶³

10.4 Tratamento de dados pessoais

O n.º 2 do art. 4º do RGPD define o tratamento de dados pessoais como uma operação, ou operações, efetuada por qualquer meio tecnológico, automatizado ou não, sobre dados pessoais. Este tratamento inclui a “(...) recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.”¹⁶⁴

¹⁶⁰ Nos termos do n.º 5 do artigo 4º do RGPD entende-se por pseudonimização “o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;”

¹⁶¹ Anonimização consiste, segundo o considerando 26 da Diretiva 95/46/CE na eliminação de elementos suficientes de modo a que deixe de ser possível identificar o titular dos dados pessoais.

¹⁶² art. 9º do RGPD.

¹⁶³ Considerando n.º 50 do RGPD.

¹⁶⁴ n.º 2 do art. 4º do RGPD; Para a definição do conceito de tratamento de dados, importa também o Ac. do TJUE de 13 de maio de 2014 do caso do Google Spain, que afirmou que, “a atividade de um motor de busca, como fornecedor de conteúdos, que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, pô-las à disposição dos internautas por determinada ordem de preferência, deve ser qualificada de «tratamento de dados pessoais», na aceção daquela disposição, quando essas informações contenham dados pessoais.” disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62014CJ0131>.

Já a al. b) do art. 3º da Lei n.º 67/98, de 26 de outubro, definia tratamento de dados como qualquer operação sobre dados pessoais “efetuada com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;”¹⁶⁵

Ora, o tratamento automatizado de dados pessoais possibilita a criação de perfis dos titulares dos dados pessoais o que, a final, permite o direcionamento de bens e serviços específicos.

Importa ainda referir que, segundo o n.º 2 do art. 9º do RGPD existem situações em que a proibição não se aplica, existindo como exceções, o consentimento do titular, a necessidade de proteger os interesses vitais do titular dos dados, se for necessário para efeitos de 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, entre outros.¹⁶⁶

O tratamento de dados pessoais pode parecer, à primeira vista, insignificante na proteção de dados, no entanto, o tratamento de dados pessoais gera muitas informações aliciantes para as empresas, principalmente no que concerne às técnicas de BD que possibilitam o armazenamento e tratamento de uma grande quantidade de dados. Este tratamento pode afetar a privacidade dos cidadãos, pelo que o controlo do mesmo é um dos objetivos principais do RGPD.

O art. 15º do RGPD afirma que, o responsável pelo tratamento dos dados deve fornecer ao titular dos mesmos as informações inerentes aos seus dados pessoais. No entanto, o responsável pelos dados não está obrigado a comunicar todo e qualquer dado que o titular dos dados pretende.

Neste seguimento, temos como exemplo o Ac. do TJUE de 22 de Junho de 2023, no qual a questão prejudicial foi o facto de J.M, outrora empregado e cliente do banco Pannki S., ter tido conhecimento de que os seus próprios dados de cliente tinham sido consultados por membros do banco em causa.

Neste sentido, este requereu ao banco que lhe comunicasse a identidade das pessoas que tinham consultado tais dados, datas das consultas e as finalidades do tratamento dos

¹⁶⁵ al. b) do art. n.º 3 da Lei n.º 67/98, de 26 de outubro.

¹⁶⁶ n.º 2 do art. 9º do RGPD.

referidos dados, o que o banco recusou, alegando que a comunicação da identidade dessas pessoas constituía também dados pessoais das mesmas.

J.M submeteu o caso ao supervisor da proteção de dados que indeferiu o pedido com base na confirmação dos argumentos do banco.

Posto isto, o processo chegou ao tribunal que suspendeu o mesmo e o reenviou ao TJUE para avaliação.

Nesta questão, o TJUE entendeu que, o n.º 1 art. 15º deve ser entendido no sentido de que “se aplica a um pedido de acesso às informações referidas nesta disposição quando as operações de tratamento abrangidas por esse pedido tenham sido efetuadas antes da data em que o referido regulamento começou a ser aplicável, mas o pedido tenha sido apresentado após essa data.”¹⁶⁷

Já o n.º 3 do art.º 15 foi interpretado pelo TJUE no Ac. de 4 de maio de 2023, no sentido de que, o lesado tem o direito de obter, do responsável pelo tratamento, uma cópia dos dados pessoais em fase de tratamento, devendo a mesma ser uma reprodução fiel e inteligível de todos esses dados.¹⁶⁸

No que concerne ao tratamento transfronteiriço, o art. 44º deste regulamento refere que, para que exista uma transferência de dados pessoais para um país terceiro ou uma organização internacional, deve ser cumprido o RGPD e garantido o nível de proteção dos titulares que o regulamento assegura.

Desta fora, de acordo com o art. 45º, pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver

¹⁶⁷ Afirma ainda no Ac. TJUE (1ª secção), 22 de junho de 2023, que: “as informações relativas a operações de consulta dos dados pessoais de um titular, sobre as datas e as finalidades dessas operações, constituem informações que esse titular tem o direito de obter do responsável pelo tratamento ao abrigo desta disposição. Em contrapartida, a referida disposição não consagra esse direito no que respeita às informações relativas à identidade dos empregados do referido responsável que procederam a essas operações sob a sua autoridade e em conformidade com as suas instruções, a menos que essas informações sejam indispensáveis para permitir ao titular dos dados exercer efetivamente os direitos que lhe são conferidos por este regulamento e desde que sejam tidos em conta os direitos e as liberdades desses empregados.” consultável em <https://curia.europa.eu/juris/document/document.jsf?jsessionid=D10F722E24D570C333CBF545A4700AC6?text=&docid=274867&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=24645757>.

¹⁶⁸ Neste sentido, o TJUE (1ª secção) no Ac. de 4 de maio de 2023, entende ainda que, “este direito pressupõe o direito de obter a cópia de extratos de documentos ou de documentos completos ou ainda de extratos de bases de dados que contenham, nomeadamente, os referidos dados, se o fornecimento dessa cópia for indispensável para permitir ao titular dos dados exercer efetivamente os direitos que lhe são conferidos por este regulamento, sendo de sublinhar que devem ser tidos em conta, a este respeito, os direitos e liberdades de terceiros.”, e que “o conceito de «informação» nele previsto refere-se exclusivamente aos dados pessoais cuja cópia o responsável pelo tratamento deve fornecer por força do primeiro período desse n.º.”, consultável https://curia.europa.eu/juris/document/document_print.jsf?mode=lst&pageIndex=0&docid=273286&part=1&doclang=PT&text=&dir=&occ=first&cid=6472200.

considerado que esse país terceiro assegura um nível de proteção adequado. Todavia, esta transferência não exige autorização específica.

No que concerne a este tipo de decisões de adequação da Comissão, importa referir a decisão Safe Harbor, criada em 2000 pelo Departamento de Comércio dos EUA, conjuntamente com a Comissão Europeia, com o intuito de possibilitar a livre transferência de dados da EU para os EUA.

Resumidamente, as empresas americanas declaravam subscrever os princípios do Safe Harbor e desta forma tornavam-se certificadas a transferir os dados.

Todavia, o TJUE, no Ac. de 6 de outubro de 2015, veio declarar a invalidade do Safe Harbour.

O famoso caso Schrems ocorreu quando, no âmbito de uma pesquisa académica o mesmo descobriu que o Facebook armazenava e utilizava os dados pessoais dos seus utilizadores, inclusive os eliminados.

Após o incidente, Schrems apresentou variadas queixas ao Comissário Irlandês para a proteção de dados onde questionava a política de privacidade do Facebook. O Proc. chegou até ao High Court que suspendeu a instância por entender que as questões que deveriam ser analisadas à luz do direito europeu.

Neste sentido, o TJUE veio impedir que o Safe Harber servisse de base legal para as transferências de dados pessoais da EU para os EUA, ao declara-la invalida por considerar que o mesmo não oferecia garantias suficientes de proteção de dados pessoais, tanto na transferência como na resolução de conflitos dos mesmos.

Em suma, ainda que existisse uma decisão da Comissão que qualifique como adequado o nível de proteção de dados pessoais oferecido por um país terceiro, nada impede que as autoridades nacionais de proteção, no seguimento de uma queixa, averiguem o contexto dessa decisão.¹⁶⁹

10.4.1. Princípios relativos ao tratamento de dados pessoais

O RGPD garante a proteção dos dados pessoais dos cidadãos através de princípios orientadores que conduzem os normativos no que concerne à proteção de dados.

¹⁶⁹ SILVA, Heraclides Sequeira dos Santos, 2017, A proteção de dados pessoais na era global: o caso schrems, pág. 41 a 55, disponível em https://run.unl.pt/bitstream/10362/20567/1/Silva_2017.pdf.

Este regulamento, apresentou um reforço dos princípios consagrados na Diretiva 95/46/CE, consagrando ainda novos princípios orientadores do comportamento das entidades responsáveis pelo tratamento.

Estes princípios encontram-se plasmados no art. 5º sendo eles, a licitude, lealdade e transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade e, por fim responsabilidade.¹⁷⁰

Ora, o princípio da licitude encontra-se ligado aos princípios da transparência e da lealdade, o que significa que para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa ou noutra fundamento legítimo, previsto por lei, quer no presente regulamento, quer noutra ato de direito da União ou de um Estado-Membro.¹⁷¹

O art. 6º do regulamento, equivalente ao art. 7º da Diretiva 95/46/CE, enumera as situações em que o tratamento de dados é considerado lícito sendo elas quando o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas, quando o tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados, quando o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito, quando o tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular, quando o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento, e quando o tratamento for necessário para efeito dos interesses legítimos¹⁷² prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

¹⁷⁰ art. 5º do RGPD.

¹⁷¹ Considerando n.º 40 do RGPD.

¹⁷² Considerando n.º 47 do RGPD “...a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta.”

Já o princípio da lealdade, encontra-se interligado com o princípio da transparência na medida em que, o responsável pelo tratamento deve elucidar o titular dos dados de todos os direitos, regras e riscos inerentes ao tratamento de dados, criando um vínculo de confiança entre o titular e o responsável.

O princípio da transparência exige que, qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, e formuladas numa linguagem clara e simples.

“(…) Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados (…)”.¹⁷³

Estes direitos, correlacionam-se para que as pessoas singulares, a quem os dados dizem respeito, sejam alertadas dos riscos, regras e direitos associados, e em especial, das finalidades específicas do tratamento dos dados pessoais que deverão ser explícitas e legítimas.

Os titulares dos dados pessoais devem conhecer, antes de os fornecer, quais os objetivos traçados para os seus dados.

O princípio da limitação das finalidades permite que, o titular dos dados possua informações sobre as finalidades determinadas para o tratamento dos dados, estabelecendo a al) a) do n.º 1 do art. 5º do RGPD que os dados pessoais devem ser recolhidos para determinadas finalidades.¹⁷⁴

Essa finalidade deve ser legítima, tendo como base legal o RGPD e de acordo com a legislação aplicável.

Este princípio cria um limite aos responsáveis pelo tratamento, devendo os mesmos cingir-se às finalidades apresentadas, limitando o tratamento às mesmas.

Uma questão que este princípio suscita é, como se afere a compatibilidade de uma nova finalidade, com a finalidade pela qual os dados foram inicialmente recolhidos.

¹⁷³ Considerando n.º 39 do RGPD.

¹⁷⁴ al. a) do n.º 1 do artigo 5º do RGPD.

O considerando 50 do RGPD proíbe o tratamento de dados para outros fins que não aqueles previstos, apenas podendo ser feito mediante prévia autorização e apenas se os novos fins forem compatíveis com as finalidades pré-definidas.¹⁷⁵

Desta forma, o responsável pelo tratamento, deverá ter em atenção, a existência de uma ligação entre a finalidade pré-definida e aquela que pretende efetuar devendo o contexto e as expectativas ser parecidas ou quase iguais.

Além disso, a natureza, as consequências e as garantias após o tratamento dos dados devem ser as mesmas também.

O considerado n.º 50 ressalva, no entanto que, no caso de o tratamento ser necessário “para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, o direito da União ou dos Estados-Membros pode determinar e definir as tarefas e finalidades para as quais o tratamento posterior deverá ser considerado compatível e lícito.”¹⁷⁶

Ressalva ainda que, tudo o que são operações de tratamento para fins de arquivo de interesse público, fins científicos, históricos ou estatísticos são considerados tratamentos lícitos.

No entanto, o considerando 50 afirma ainda que, na hipótese de o titular dos dados ter dado o seu consentimento ou, no caso de o objetivo desse tratamento ser o interesse público, o responsável pelo tratamento é autorizado a proceder ao tratamento posterior dos dados pessoais, independentemente da compatibilidade das finalidades. Todavia, deverá ser garantida a aplicação dos princípios enunciados pelo presente regulamento e, em particular, a obrigação de informar o titular dos dados sobre essas outras finalidades e sobre os seus direitos, incluindo o direito de se opor.

O princípio da limitação das finalidades limita o desenvolvimento do BD porque, este último, alimenta-se de dados para se desenvolver, dados esses que no mundo ideal do BD deveriam de poder ser constantemente retirados de forma a permitir novos desenvolvimentos e inovações.

Este princípio, por outro lado, permite a adequação e limitação das finalidades para a utilização dos dados, permitindo uma maior confiança na abdicação de dados pessoais em prol do desenvolvimento e inovação.

¹⁷⁵ Considerando n.º 50 do RGPD.

¹⁷⁶ Considerando n.º 50 do RGPD.

O princípio da minimização dos dados significa, segundo a al) c) do n.º 1 do art. 5º do RGPD, que os dados pessoais utilizados devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades.

Este princípio, limita as entidades ao tratamento do mínimo necessário de dados para atingir o objetivo.¹⁷⁷

O princípio da exatidão, segundo a al) d) do n.º 1 do art. 5º do RGPD, determina que os dados devem ser exatos e atualizados sempre que necessário e devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora.

Já o princípio da limitação da conservação, segundo a al) f) do n.º 1 do art. 5º do RGPD, determina que os dados devem ser conservados de maneira a que haja a possibilidade de identificar os titulares dos dados, apenas durante o período necessário ao alcance das finalidades para os quais foram tratados. Os dados apenas poderão ser guardados, por períodos mais longos, se forem tratados para fins de arquivo de interesse público, de investigação, história ou fins estatísticos.¹⁷⁸

O considerando n.º 39 considera que, os dados pessoais devem ser conservados apenas pelo período considerado necessário, devendo o responsável pelo tratamento fixar prazos para o apagamento ou a revisão periódica, devendo ser adotadas todas as medidas razoáveis para que os dados pessoais inexatos sejam retificados ou apagados.

A al) f) do n.º 1 apresenta os princípios da integridade e confidencialidade, referindo que, os dados pessoais devem ser tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas.

Isto significa que, as entidades devem apresentar modelos de segurança que impossibilitem o acesso, utilização, destruição ou utilização dos dados por terceiros não autorizados, apostando em mecanismos de anonimização e pseudonimização.¹⁷⁹

¹⁷⁷ Considerando n.º 39 do RGPD.

¹⁷⁸ Considerando n.º 39 do RGPD.

¹⁷⁹ ««Pseudonimização», o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável» (n.º 5, artigo 4º RGPD).

Por fim, o princípio da responsabilidade atribui a responsabilidade ao responsável pelo tratamento de assegurar o cumprimento dos princípios enunciados no n.º 1 do art. 5º do RGPD, tendo ainda o dever de comprovar o cumprimento.

10.4.2 O Consentimento e o direito à indemnização

O n.º 4 do art. 11º do RGPD define consentimento do titular dos dados como sendo “uma manifestação de vontade, livre,¹⁸⁰ específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento”, o que significa que o titular dos dados deverá ter plena consciência das finalidades a que se destinam o tratamento dos dados e dar o seu consentimento explícito a cada uma delas.¹⁸¹

O considerando n.º 32 refere que, “o consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento.”

Este consentimento tem de abranger todas as atividades de tratamento realizadas com a mesma finalidade. E, quando o tratamento tiver fins múltiplos o consentimento deve ser realizado para cada uma das finalidades.

¹⁸⁰ Um exemplo do consentimento que não é livre: “Uma aplicação para telemóvel de edição de fotografias solicita aos utilizadores que ativem a localização por GPS para fins de prestação dos serviços. A aplicação também os informa de que utilizará os dados recolhidos para efeitos de publicidade comportamental. Nem a geolocalização nem a publicidade comportamental em linha são necessárias para a prestação do serviço de edição de fotografias, indo além da concretização do serviço principal prestado. Uma vez que os utilizadores não podem utilizar a aplicação sem darem o seu consentimento para estes efeitos, o consentimento não pode ser considerado livre.”, Grupo de Trabalho do Artigo. 29.º Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, pág. 12, consultável em https://www.uc.pt/protecao-dados/suporte/20180410_orientacoes_relativas_ao_consentimento_wp259_rev01.

¹⁸¹ Um ato positivo inequívoco significa que o titular dos dados deve agir com intenção de consentir o tratamento em causa, Grupo de Trabalho do Artigo 29.º Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, pág. 18, consultável em https://www.uc.pt/protecao-dados/suporte/20180410_orientacoes_relativas_ao_consentimento_wp259_rev01 e n.º 4 do art. 11º do RGPD.

Na possibilidade de o pedido de consentimento ter sido realizado por via eletrónica o mesmo tem de ser claro o que, maioritariamente das vezes, não o é.¹⁸²

Aliás, neste caso, o consentimento nem sequer pode impedir o acesso ao endereço eletrónico, o que também ocorre variadas vezes como veremos mais à frente.¹⁸³

O considerando 42 determina que, o responsável pelo tratamento deve demonstrar a possibilidade de recusa ou de retirar o consentimento sem que o titular dos dados seja prejudicado. Ou seja, essa retirada do consentimento não pode resultar num custo para o titular ou numa impossibilidade de acesso ou de utilização do site, aplicação, entre outros. Estas consequências são chamadas de prejuízos. Outros exemplos de prejuízos são a fraude, coação, entre outros.¹⁸⁴

Neste seguimento, os responsáveis pelo tratamento dos dados devem utilizar procedimentos de consentimento claros para os titulares. Devem ainda evitar ambiguidades e assegurar que o ato de prestação do consentimento é distinguível dos outros atos.

No caso de um site da internet, a simples utilização normal do site não pode ser entendida como manifestação de vontade do titular dos dados em consentir o tratamento de dados.¹⁸⁵

¹⁸² Considerando n.º 32 do RGPD.

¹⁸³ Um exemplo dessa situação: “Ao descarregar uma aplicação para telemóvel relativa a hábitos de vida, a aplicação solicita consentimento para aceder ao acelerómetro do telefone. Não se trata de algo necessário para a aplicação funcionar, mas é útil para os responsáveis pelo tratamento que pretendem saber mais acerca dos movimentos e dos níveis de atividade dos utilizadores. Posteriormente, se a utilizadora revogar esse consentimento, descobre que a aplicação só funciona parcialmente. Estamos perante um exemplo de prejuízo na aceção do considerando 42, o que significa que o consentimento nunca foi obtido validamente (e logo, o responsável pelo tratamento tem de apagar todos os dados pessoais acerca dos movimentos dos utilizadores recolhidos desta forma),” Grupo de Trabalho do Artigo 29.º Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, pág. 12.

¹⁸⁴ A título exemplificativo, “Uma revista de moda oferece aos leitores acesso para comprarem novos produtos de maquilhagem antes do lançamento oficial. Os produtos estarão disponíveis para venda brevemente, mas oferece-se aos leitores da revista uma antevisão exclusiva dos referidos produtos. Para beneficiarem da oferta, as pessoas devem dar a morada e concordar em subscrever a lista de endereços da revista. A morada é necessária para o envio dos produtos e a lista de endereços é utilizada para enviar ofertas comerciais de produtos, tais como cosméticos ou t-shirts, durante todo o ano.

A empresa explica que os dados que constam da lista de endereços apenas serão utilizados para o envio de artigos e publicidade em papel pela própria revista e que não são partilhados com outras organizações.

Caso o leitor não queira divulgar o seu endereço por esta razão, não existe prejuízo, uma vez que os produtos estarão disponíveis de qualquer forma.” Grupo de Trabalho do Artigo 29.º Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, pág. 12, consultável no link indicado acima.

¹⁸⁵ Um exemplo disso ocorre quando, por exemplo o “deslizar o dedo por uma barra no ecrã, assentir com a cabeça em frente a uma câmara inteligente, rodar o telemóvel no sentido dos ponteiros do relógio ou movimentá-lo de forma a desenhar no ar o número oito podem ser opções para indicar concordância, desde que sejam fornecidas informações claras e desde que seja evidente que o movimento em causa significa concordância com um pedido específico (p. ex. se deslizar o dedo para a esquerda por cima desta barra, concorda em utilizar as informações X para a finalidade Y. Repetir a ação para confirmar). O responsável pelo tratamento deve conseguir demonstrar que o consentimento foi obtido desta forma e os titulares dos dados

No contexto digital, muitos serviços necessitam de dados pessoais para operar, por isso, os titulares de dados recebem, diariamente, pedidos de consentimento que cobrem os seus ecrãs e exigem respostas através de cliques. Esta situação, para quem tem consciência do que ela representa, pode gerar fadiga. Para quem não tem consciência do que representa e apenas quer ter acesso àquele serviço ou informação, significa apenas uma operação rotineira. Isto leva a que, as questões ligadas ao consentimento deixem de ser lidas o que constitui um risco acrescido aos titulares dos dados, o que irá ser analisado mais adiante.

O art. 7º do RGPD apresenta as diversas situações aplicáveis ao consentimento.

Em primeiro lugar, no n.º 1 o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.¹⁸⁶

Em segundo lugar, o n.º 2 afirma que, “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.”¹⁸⁷

Nestes dois pontos encontra-se presente o princípio da informação na medida em que, para que o titular dos dados consiga dar um consentimento voluntário, ele deve estar plenamente informado sobre a utilização dada aos dados que este irá fornecer.

Essa informação não passa apenas pela finalidade atribuída ao mesmo, mas também pela possibilidade de o mesmo, a qualquer altura, poder por fim ao consentimento.

Em terceiro lugar, segundo o n.º 3 do supramencionado art., o titular dos dados tem a possibilidade de retirar, a qualquer momento, o consentimento. Esta retirada não compromete a licitude do tratamento efetuado baseado no anterior consentimento.

O n.º 3 do art. 7º refere ainda que o consentimento deve ser tão fácil de retirar quanto de dar, o que, no meu entendimento, ainda necessita de alguns ajustes.¹⁸⁸

Por exemplo, na pesquisa de qualquer site, após o consentimento do titular dos dados para a permissão de utilização dos dados, caso o mesmo pretenda eliminar esse consentimento posteriormente não o consegue realizar no próprio site onde o mesmo foi

devem conseguir retirar o consentimento tão facilmente como quando o deram.”, Grupo de Trabalho do Artigo 29.º Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, pág. 19.

¹⁸⁶ N.º 1 do Art. 7º do RGPD.

¹⁸⁷ N.º 2 do Art. 7º do RGPD.

¹⁸⁸ N.º 3 do Art. 7º do RGPD.

permitido apenas o conseguido fazer- lo através das definições no browser onde efetuou a pesquisa.

Ou seja, a possibilidade de eliminar o consentimento previamente dado não é facilmente alcançável.

Ora, a obrigação de consentimento não agradou aos utilizadores do BD uma vez que, por vezes a necessidade do consentimento impossibilita a recolha de dados podendo comprometer o desenvolvimento.

No entanto, o certo é que, se colocarmos numa balança os dois lados, ainda que o avanço tecnológico seja comprometido, não se pode permitir que a única arma atribuída aos consumidores, o consentimento, seja colocada em risco em prol do mesmo.

O considerando 42 do RGPD refere que “sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados (...)”.¹⁸⁹ Em conformidade com o considerando n.º1 Diretiva 93/13/CEE do Conselho, uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina.

Acrescenta ainda que “não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado.”¹⁹⁰

Ora, neste caso não existe uma presunção de aceitação que beneficie o responsável pelo tratamento, protegendo o titular dos dados de uma intromissão não autorizada na sua privacidade.

O n.º 4 do art. 7º do RGPD determina que para avaliar se o consentimento é dado de forma livre, é necessário verificar com 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.¹⁹¹

¹⁸⁹ Considerando n.º 42 do RGPD.

¹⁹⁰ Considerando n.º 1 da Diretiva 93/13/CEE do Conselho

¹⁹¹ n.º 4 do art. 7º do RGPD.

Ou seja, quando o titular dos dados não usufruir de uma opção verdadeiramente livre, fornecendo dados que não são necessários para a execução do contrato, não se poderá considerar que foi prestado de livre vontade.

A obrigatoriedade de ter de consentir a utilização de dados pessoais para além do que é estritamente necessário acaba por diminuir as escolhas do titular dos dados e constitui um obstáculo ao consentimento dado.

Uma vez que as normas de proteção de dados visam proteger os direitos fundamentais cria-se uma certa presunção de que o consentimento para o tratamento de dados pessoais não necessário e não deve ser encarado como troca para a prestação de um contrato ou da prestação de serviço.

De acordo com o Parecer 06/2014 do GT29, “a expressão «necessário para a execução de um contrato» deve ser interpretada de forma restritiva. O tratamento deve ser necessário para o cumprimento do contrato em relação a cada um dos titulares dos dados. Tal pode incluir, por exemplo, o tratamento dos dados relativos ao endereço da pessoa em causa para que os bens adquiridos em linha possam ser entregues ou o tratamento dos dados relativos ao cartão de crédito para que o pagamento seja efetuado. No contexto laboral, este fundamento pode permitir, por exemplo, o tratamento das informações relativas ao salário e dos dados relativos à conta bancária para que os salários possam ser pagos. Tem de existir uma relação direta e objetiva entre o tratamento dos dados e a finalidade da execução do contrato”.

Note-se que, o art. supramencionado apenas é aplicável se os dados pedidos não forem necessários para a execução do contrato (incluindo a prestação de um serviço) e a execução desse contrato ficar subordinada à obtenção desses dados com base no consentimento. Todavia, se o tratamento for necessário para a execução do contrato (incluindo a prestação de um serviço), então o art. 7.º n.º 4, não é aplicável.¹⁹²

Neste sentido, o considerando 43 do RGPD estabelece que, para o consentimento seja considerado de livre vontade, “este não deverá constituir fundamento jurídico válido

¹⁹² Um exemplo disso ocorre quando, por exemplo; “Um banco solicita aos clientes consentimento para que terceiros possam utilizar os seus dados de pagamento para fins de comercialização direta. Esta atividade de tratamento não é necessária para a execução do contrato nem para a prestação dos serviços bancários normais. Se a recusa do cliente em consentir o tratamento para estes fins implicar a não prestação dos serviços bancários, o encerramento da conta bancária ou, dependendo do caso, um aumento das comissões, o consentimento não pode ser dado livremente.” Grupo de Trabalho do Artigo 29.º Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, pág. 9 e 10, consultável em https://www.uc.pt/protecao-de-dados/suporte/20180410_orientacoes_relativas_ao_consentimento_wp259_rev01.

para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa.¹⁹³

Neste caso, é dada uma presunção de que o consentimento não foi dado de livre vontade.

Um exemplo desta situação é um apresentado GT29 quando refere que: “uma escola pública solicita aos estudantes consentimento para utilizar as suas fotografias numa revista estudantil impressa. O consentimento nestas situações seria uma verdadeira escolha desde que não fosse negado aos estudantes o ensino ou os serviços a que têm direito e estes pudessem recusar a utilização das referidas fotografias sem ficarem prejudicados.”¹⁹⁴

Outro exemplo do desequilíbrio de poder é, no âmbito laboral, uma vez que, existe uma relação de dependência entre empregador/trabalhador. Neste caso, o GT29 considera que é improvável que o titular dos dados possa recusar o tratamento de dados ao seu empregador sem que exista receio de sequelas. Nestes casos, é improvável que o consentimento seja dado de forma livre.

Acresce que, é ainda problemático o facto de serem os próprios empregados a procederem ao tratamento de dados pessoais dos atuais e futuros trabalhadores. Neste caso, também se considera pouco provável a liberdade do consentimento.

No que concerne ao direito de indemnização e responsabilidade descrito no art. 82º do RGPD o mesmo afirma em suma que, qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do mencionado regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos, tendo ainda o responsável pelo tratamento responsabilidade pelos danos causados.¹⁹⁵

Por isso, o responsável pelo contraente deve reparar qualquer dano provocado à vítima em virtude do tratamento dos dados, a não ser que prove que o facto que causou o dano não lhe é imputável.¹⁹⁶

¹⁹³ Considerando n.º 43 do RGPD.

¹⁹⁴ Grupo de Trabalho do Artigo 29.º Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, pág. 12.

¹⁹⁵ N.º 1 e 2 do art. 82º do RGPD.

¹⁹⁶ Considerando n.º 146 do RGPD.

Os tratamentos que violem o mencionado regulamento abrangem, não só os abrangidos por este, mas também o direito dos Estados-Membros que executa ao mesmo.

Quando estiver em causa mais que um responsável pelo mesmo tratamento cada um será responsabilizado pela totalidade dos danos causados, sem prejuízo de direito de regresso contra os outros responsáveis.¹⁹⁷

Nesta perspetiva, e como forma de compreender a presente disposição, temos a título exemplificativo o caso do Ac. do TJUE de 4 de maio de 2023, no qual este pedido foi apresentado no âmbito de um litígio que opõe UI à Österreichische Post AG, a respeito do recurso interposto por aquele destinado a obter uma indemnização pelo dano imaterial que afirma ter sofrido devido ao tratamento por esta sociedade de dados relativos às afinidades políticas de pessoas residentes na Áustria, em particular, ele próprio, apesar de não ter dado consentimento a esse tratamento.

Em suma, a sociedade de direito austríaco desde 2017 que recolhia informações sobre afinidades políticas da população austríaca utilizando um algoritmo.

Esse algoritmo que tinha em atenção diversos critérios sociais e demográficos e, através disso, definiu moradas de grupos que ele considerava os mais adequados. Desta feita, os dados foram vendidos a diferentes organizações para que estas pudessem direcionar a sua publicidade.

Por consequência, UI, não deu consentimento para o tratamento dos seus dados pessoais e sentiu-se ofendido por lhe ter sido atribuída afinidade aquele partido. Interpôs, por isso, ação contra Österreichische Post AG com vista à eliminação dos dados pessoais e à indemnização por danos imateriais.

O pedido foi parcialmente deferido pelos tribunais irlandeses, não lhe tendo sido concedido o direito à indemnização plasmado no art. 82º do RGPD.¹⁹⁸

¹⁹⁷ Considerando n.º 146 do RGPD.

¹⁹⁸ O artigo 82º do RGPD deve ser entendido, no sentido do Ac. do TJUE de 4 de maio de 2023, que, “(...) para efeitos da fixação do montante da indemnização devida a título do direito de indemnização consagrado neste artigo, os juízes nacionais devem aplicar as normas internas de cada Estado-Membro relativas ao alcance da indemnização pecuniária, desde que sejam respeitados os princípios da equivalência e da efetividade do direito da União.” Neste sentido deve a indemnização ser contabilizada tendo em conta a redação da disposição em causa e o contexto em que se insere “(...) [v., neste sentido, Acórdãos de 15 de abril de 2021, *The North of England P & I Association*, C-786/19, EU:C:2021:276, n.o 48, e de 10 de junho de 2021, *KRONE-Verlag*, C-65/20, EU:C:2021:471, n.o 25] (...)”

Reenviado o Proc. para o TJUE o mesmo entendeu que, em primeiro lugar, que o n.º 1 do art. 82º do RGPD deve ser interpretado no sentido de que a simples violação das disposições deste regulamento não é suficiente para conferir um direito de indemnização.

Segundo o douto Ac., sobre o n.º 1 do mencionado art. 82º, qualquer pessoa que tenha sofrido danos materiais ou imateriais derivados de uma violação do regulamento supramencionado, tem direito a ser indemnizado pelo responsável pelo tratamento.

No entanto, por outro lado, resulta ainda do artigo que a existência de um dano que foi sofrido constitui uma das condições para a aplicação do RGPD, tal como um nexo de causalidade entre esse dano e essa violação, sendo estas condições cumulativas.

Com efeito, o n.º 2 do art. 82º do RGPD enumera três condições necessárias para o surgimento do direito de indemnização, a saber, um tratamento de dados pessoais efetuado em violação das disposições do RGPD, um dano ou um prejuízo sofrido pelo titular dos dados, e um nexo de causalidade entre esse tratamento ilícito e esse dano.

Acresce que, o n.º 2 do art. 82º do RGPD enumera três condições necessárias para o surgimento do direito de indemnização, a saber, um tratamento de dados pessoais efetuado em violação das disposições do RGPD, um dano ou um prejuízo sofrido pelo titular dos dados, e um nexo de causalidade entre esse tratamento ilícito e esse dano.

Por isso, não se pode considerar que toda e qualquer violação das disposições do RGPD confere o direito de indemnização aqui em causa.

Para além disto, o tribunal entendeu que a interpretação do art. 82º n.º 1 é corroborada pelos considerandos 75, 85 e 146 do RGPD.¹⁹⁹

Destes retira-se, em primeiro lugar que, a criação de um dano no tratamento de dados é apenas potencial, em segundo lugar que, uma violação do RGPD não implica o surgimento de um dano e, em terceiro lugar, que tem de existir um nexo de causalidade entre o dano sofrido e a violação em causa.

A interpretação literal do art. 82.o, n.º 1, do RGPD é igualmente corroborada por uma comparação com outras disposições que figuram também no capítulo VIII deste

¹⁹⁹ “Por um lado, este considerando 146, que tem especificamente por objeto o direito de indemnização previsto no artigo 82.o, n.o 1, deste regulamento, refere-se, no seu primeiro período, aos «danos de que alguém possa ser vítima em virtude de um tratamento que viole o [referido] regulamento». Por outro lado, esses considerandos 75 e 85 mencionam, respetivamente, que «operações de tratamento de dados pessoais [são] suscetíveis de causar danos» e que «a violação de dados pessoais pode causar danos».”, Ac. do TJUE de 4 de maio de 2023 disponível em <https://curia.europa.eu/juris/document/document.jsf?jsessionid=89DF9C842926C52900ECB31AD7D2D116?text=&docid=273284&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=4910538>

regulamento, que regula, nomeadamente, as diferentes vias de recurso que permitem proteger os direitos do titular dos dados em caso de tratamento dos seus dados pessoais pretensamente contrário às disposições do referido regulamento.²⁰⁰

Do mesmo modo, os art. 83º e 84º do RGPD, que têm finalidade punitiva e não estão sujeitas existência de um dano individual.

Por isso, através da articulação destes artigos é possível retirar que existe diferenças entre as diferentes sanções, todavia, as mesmas complementam-se no sentido de que, por um lado uma incentiva o respeito pelo regulamento, possibilitando a qualquer pessoa pedir a indemnização por danos relativos ao tratamento dos seus dados e, por outro lado, desencoraja a reiteração de comportamentos ilícitos.

Considerou, por fim, o douto tribunal que, tendo em conta todos os fundamentos precedentes, a simples violação das disposições do regulamento não é suficiente para determinar um direito à indemnização.²⁰¹

Todavia, considerou ainda que, o facto de subordinar a indemnização de um dano imaterial a uma certa quantidade de gravidade colocaria em risco o regime instituído pelo regime do RGPD, uma vez que, esse ponto de referência, a gravidade ou não do dano poderia levar a diferentes decisões dependendo da apreciação de diferentes juízes.

Este entendimento não invalidaria, no entanto, que o lesado tivesse de apresentar as consequências negativas que levaram ao dano imaterial.

No que concerne ao montante da indemnização, o douto tribunal considerou que, a mesma deveria ser calculada de acordo com as normas internas de cada Estado-Membro desde que as mesmas respeitassem os princípios da equivalência e da efetividade do direito da União.²⁰²

O consentimento, tal como já mencionado tem de ser livre e informado. O certo é que, na altura do fornecimento de dados, o individuo é informado. No entanto, o que se levanta aqui é se o pedido de consentimento é desde logo transparente e, ainda que seja informado, se é compreendido.

²⁰⁰ Art. 77º e 78º do RGPD.

²⁰¹ Ac. do TJUE (3ª secção) de 4 de maio de 2023, consultável em <https://curia.europa.eu/juris/document/document.jsf?jsessionid=89DF9C842926C52900ECB31AD7D2D116?text=&docid=273284&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=4910538>.

²⁰² Ac. do TJUE (3ª secção) 4 de maio de 2023, consultável em <https://curia.europa.eu/juris/document/document.jsf?jsessionid=89DF9C842926C52900ECB31AD7D2D116?text=&docid=273284&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=4910538>.

Ora, basta uma pequena pesquisa na internet para se perceber que, sempre que se acede a um website o pedido de recolha de dados vem criado de forma não muito explicita. Ou seja, geralmente o pedido para consentimento geral é sempre mais aliciante do que a escola personalizada de fornecimento de dados. Aliás, geralmente o “gerir cookies” encontra-se de forma dissimulada.

Por isso, ainda que os sites sejam cumpridores da lei, o problema é que a falta de descrição de apresentação dos pedidos de consentimento põe em causa a decisão informada do utilizador.

Para além disso, não existiu qualquer explicação, quer em escolas, quer em empresas, quer nos meios de comunicação de como funciona a recolha, o tratamento e o armazenamento de dados quer pelos sites, quer pelas empresas.

A entrega de dados passou a ser mais um papel para assinar sem ler.

A criação de um programa elucidativo sobre partilha de dados informáticos e os seus perigos iminentes seria a solução para tentar diminuir esta lacuna informativa sobre a entrega e utilização de dados pessoais.

10.4.3 O consentimento de menores

O art. 8º do RGPD apresenta as condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade de informação.²⁰³

Determina que, o consentimento só é lícito se o menor tiver pelo menos 16 anos, e na medida em que, o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança.

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

Ora, países como Portugal, Reino Unido, Letónia, Finlândia, Estónia, Bélgica, Dinamarca, Malta e Suécia optaram por determinar a idade mínima de treze anos.²⁰⁴

²⁰³ Art. 8º do RGPD.

²⁰⁴ Segundo o art. 16º da Lei 58/2019 de 8 de Agosto “Nos termos do artigo 8.º do RGPD, os dados pessoais de crianças só podem ser objeto de tratamento com base no consentimento previsto na al) a) do n.º 1 do artigo 6.º do RGPD e relativo à oferta direta de serviços da sociedade de informação quando as mesmas já tenham completado 13 anos de idade.”; Refere ainda, no n.º 2 que: “Caso a criança tenha idade inferior a 13 anos, o tratamento só é lícito se o consentimento for dado pelos representantes legais desta, de preferência com recurso a meios de autenticação segura.”

Já a Áustria, Bulgária, Chipre, Itália, Lituânia e Espanha estabeleceram os catorze anos de idade e a República Checa e a França os quinze anos de idade.

Por fim, a Croácia, Alemanha, Grécia, Hungria, Irlanda, Luxemburgo, Países Baixos, Polónia, Roménia, Eslováquia e Eslovénia determinaram os dezasseis anos de idade como limite.

O considerando 38 estabelece a necessidade de existir uma maior proteção às crianças uma vez que, as mesmas têm menor tendência a conhecer os riscos, consequências, garantias e direitos relacionados com o tratamento de dados pessoais, devendo essa proteção específica “aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças”.²⁰⁵

Ressalva, no entanto, que o consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança.

O que demonstra o artigo 8º é que, o mesmo apenas é aplicável se a razão para o tratamento for relacionada com a oferta de serviços a uma criança e que o tratamento baseia-se no consentimento.

O n.º 2 do art. 8º do RGPD refere que, o responsável pelo tratamento realiza 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.²⁰⁶

Basicamente, o que ocorre é que, quando prestam serviços a crianças com base no consentimento, considera-se que o responsável pelo tratamento deve verificar se o utilizador já ultrapassou a idade para o consentimento digital, ainda que os utilizadores afirmem que já ultrapassaram a idade para o consentimento. E, embora isto não esteja explícito no RGPD, o GT29 considera que é algo que se encontra implícito ao artigo.

Todavia, essa verificação não deve levar a um tratamento de dados excessivo,

²⁰⁵ Considerando n.º 38.

²⁰⁶ N.º 2 do art. 8º RGPD.

A verificação da idade não deve conduzir a um tratamento de dados excessivo, mas, em caso de dúvidas, o responsável pelo tratamento deve encetar esforços para avaliar a veracidade da situação.²⁰⁷

É importante afirmar que, em conformidade com o considerando 38, este consentimento dado pelo progenitor ou tutor não é necessário para serviços direcionados a crianças como, por exemplo, os de proteção de crianças.

A proteção dos menores, no âmbito da proteção de dados, encontra um obstáculo difícil de contornar, sendo ele o galopante avanço tecnológico, mais precisamente na utilização da internet.

Ora, um em cada três utilizadores de Internet é uma criança, que atualmente acede facilmente e sem supervisão, utilizam aplicações, jogam jogos online, e utilizam redes sociais.

Ainda que, se considere que a Internet ofereça muitas oportunidades de aprendizagem, comunicação, criatividade e entretenimento, ela acarreta sérios riscos para os utilizadores, principalmente os mais vulneráveis, como as crianças.

A Comissão pretende garantir a proteção dos jovens principalmente no que toca à proteção dos dados pessoais.

A estratégia europeia para uma Internet melhor para as crianças prevê um conjunto de medidas complementares, que vão desde o financiamento, coordenação e autorregulação para ajudar a criar um ambiente online mais seguro.

A plataforma Better Internet for Kids, fornece às crianças, pais e educadores uma grande quantidade de informações, orientações e recursos sobre questões que podem surgir na utilização da internet, apostando na consciencialização da segurança online.²⁰⁸

²⁰⁷ O GT29 apresenta um exemplo de uma empresa que enceta todos os esforços para a verificação da maioridade de consentimento: “Uma plataforma de jogos em linha quer garantir que os clientes menores só conseguem subscrever os seus serviços com o consentimento dos progenitores ou tutores. O responsável pelo tratamento segue os passos seguintes: Passo 1: pede ao utilizador que indique se tem menos ou mais de 16 anos (...) Se o utilizador indicar que a sua idade é inferior à idade para consentimento digital: Passo 2: o serviço informa a criança de que um dos progenitores ou tutores deve consentir ou autorizar o tratamento antes de o serviço ser prestado à criança. É pedido ao utilizador que revele o endereço eletrónico de um dos progenitores ou tutores. Passo 3: o serviço contacta o progenitor ou tutor e obtém o seu consentimento através de mensagem de correio eletrónico para o tratamento e toma medidas razoáveis para confirmar que o adulto tem responsabilidade parental. Passo 4: em caso de queixas, a plataforma toma medidas adicionais para verificar a idade do subscritor. Se a plataforma observar os outros requisitos do consentimento, a plataforma pode cumprir os critérios adicionais do artigo 8.º do RGPD seguindo estes passos.”, Grupo de Trabalho do Artigo 29.º Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, pág. 12.

²⁰⁸ European Commission, 24 de Março de 2022, consultável in <https://digital-strategy.ec.europa.eu/en/policies/digital-privacy>.

O consentimento de menores, no que concerne à proteção de dados, acarreta uma maior preocupação uma vez que, este consentimento é dado sem a supervisão dos responsáveis, e outras vezes é dado com o consentimento dos responsáveis porque nem estes compreendem os potenciais riscos.

Tal como enunciado anteriormente, encontramos-nos numa sociedade sedenta por informação, que inconscientemente entrega dados pessoais em troca de acesso a informação.

Ora, se um titular de dados, considerado maior para dar o seu consentimento, aceita imperativamente a entrega de dados pessoais sem conhecer os riscos, garantias e direitos que advêm desse ato, um menor, ainda que acompanhado, muito menos conhecerá.

O que significa que, ainda que exista uma idade mínima para permitir a utilização de dados pessoais, isso não é suficiente para que o consentimento seja dado de forma livre e consciente porque a sede de informação tolda a consciencialização do titular.

Acresce que, no caso da internet, na utilização de jogos e aplicações online, os avisos de permissão de utilização de dados são criados para que sejam apelativos e não preocupantes.

O interesse dos sites e aplicações é a permissão do acesso aos dados e por isso, omitem informações importantes sobre a utilização de dados para que a única apelabilidade esteja na permissão da utilização dos dados na sua totalidade.

Para além disso não é, na minha opinião, pelo facto de se reduzir a idade permitida para que o consentimento seja lícito, que irá diminuir a quantidade de assentimentos realizados sem conhecimento dos riscos, direitos e garantias.

O entendimento na redução da idade parte do facto de a população ter acesso, cada vez mais prematuramente, às novas tecnologias e à internet. E que, uma vez que o acesso aos mesmos é realizado cada vez mais cedo, mais cedo existirá conhecimento por parte dos menores, dos riscos inerentes na utilização desses.

Por isso, países como Portugal, Reino Unido, Bélgica, entre outros, definiram a idade mínima os treze anos.

Quanto a este tema existe uma divisão demarcada entre os aqueles que defendem que, a idade mínima são os treze anos e aqueles que entendem que são os 16 anos a idade mais adequada.

Os profissionais de sociologia, pedagogia, psiquiatria, entre outros, entendem que a idade mínima para o consentimento, nos termos do regulamento Geral de Proteção de Dados

é de treze anos, tendo como entendimento que, tal idade, é suficiente e que, uma vez atingindo esta os utilizadores já recorrem à internet naturalmente.

Quanto aos restantes, entendem que a idade mínima necessária ao consentimento será a de dezasseis anos, tendo como bases de entendimento, o desenvolvimento do intelecto necessário para um consentimento informado no âmbito do regulamento de dados.

10.4.3.1 Posição adotada

Esta quezília entre opiniões será sempre uma questão enquanto o crescimento e o desenvolvimento tecnológico se encontrarem em colisão com a preservação da dignidade e privacidade humana.

Numa sociedade com uma “fome” voraz por desenvolvimento e informação, a dedução da idade necessária para o consentimento na atribuição de dados torna-se um problema cuja solução nunca vai satisfazer os dois lados, o do desenvolvimento, o da defesa da dignidade.

Para que uma posição seja tomada é necessário diferenciar os tipos de consentimento suscitados no RGPD.

Encontra-se presente no considerando 32 que, “O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito (...)”²⁰⁹

Em primeiro lugar, o consentimento deve ser dado mediante um ato positivo, o que significa que não é possível supor que o titular, se conhecesse as circunstâncias em que os dados seriam utilizados, permitiria tal utilização.

Por isso deve o consentimento não pode ser presumido, apenas efetivo, o que se compreende tendo em atenção o elevado fluxo de utilização diária da internet.

Este ato é, antes de tudo, uma obrigação ética e, para além disso, uma exigência legal desenhada para proteger os dados pessoais dos utilizadores.

De seguida, em segundo lugar, o consentimento deve ser livre, pelo que é necessário que a sua atribuição tenha sido obtida sem qualquer coação ou manipulação. Não é permitido, portanto, quaisquer atos ardilosos que levem a um consentimento restrito.

²⁰⁹ Considerando n.º 32 do RGPD.

Para além disso, num ambiente de consumo complexo, o consentimento deve ser informado e esclarecido, no sentido que o utilizador tem de ter conhecimento das finalidades projetadas para a utilização dos seus dados.

A linguagem utilizada nos questionários não deve ser hermética e confusa, não podendo ainda ter questões de utilização omitidas, sendo obrigatório informações claras e em linguagem acessível sobre o tratamento dos dados pessoais

Esta claridade na linguagem encontra-se ligada à necessidade de o utilizador ser devidamente informado das finalidades de utilização dos seus dados, no entanto, num mundo de consumação de informação em massa questiona-se o facto de este conhecimento da informação ser consciente ou não.

Tal questão levanta-se especialmente na escolha da idade ideal para a atribuição dum consentimento na utilização de dados pessoais, uma vez que este consentimento não se pode resumir ao simples clique na opção “Aceito todos”.

Tal consentimento tem de ser, tal como já referido supra, um ato positivo claro, informado, inequívoco e livre e para que se possa determinar a idade ideal para a possibilidade do mesmo é requisito essencial a correlação entre o desenvolvimento cognitivo, a educação, a maturidade e o ambiente social.

Jean Piaget dividiu o desenvolvimento cognitivo da criança em quatro estágios mais ou menos delimitados. O primeiro, designado sensoriomotor, ocorre entre os 0 anos a 2 anos de vida em que o bebe compreende o mundo através dos seus sentidos e ações motoras; o segundo, o pré-operatório, desenvolve-se entre os 2 e os 6 anos de vida em que a criança começa “(...) *a símbolos, classificar objetos e utilizar lógica simples (...)*; o terceiro estágio, o operatório concreto, dos 7 aos 11 anos, caracterizado pela evolução na realização de operações mentais de maior complexidade, como a soma, subtração entre outras; e, por fim, o ultimo estágio, denominado o operatório formal, ocorre entre os 12 e seguintes anos, sendo característico neste estágio uma maior organização de ideias, eventos, e objetivos.²¹⁰

No final do último estágio o autor defende que, a criança já terá uma consciência espacial, conseguindo calcular distâncias, ter noção das consequências dos seus atos, um raciocínio intuitivo e indutivo e capacidade de resolução de simples problemas didáticos.

²¹⁰ RODRIGUES, Olga Maria Piazzentin Rolim & Melchiori, Lígia Ebner, Aspectos do desenvolvimento na idade escolar e na adolescência, pág. 4.

Estes estágios apenas atingem a sua plenitude com a implementação do ensino escolar na criança, dotado de matéria progressivamente mais complexas de forma a estimular o desenvolvimento cognitivo da mesma.

Ora, seguindo tal entendimento, uma criança com treze anos alegadamente poderia ter capacidade para dar um consentimento informado, livre e explícito para o tratamento de dados pessoais.

No entanto, não se pode olvidar que esse desenvolvimento depende de fatores endógenos, externos à criança, como a educação, o convívio com outros seres humanos, com a cultura e o meio ambiente.

Lev Vygotsky, na sua teoria sociocultural, defende que, só existe desenvolvimento se a pessoa for exposta a uma cultura e a um meio social. Neste sentido, “não é o desenvolvimento que antecede e possibilita a aprendizagem, mas, ao contrário, é aprendizagem que antecede, possibilita e impulsiona o desenvolvimento”.²¹¹

Ora, isso significa que, para que a criança consiga ter um desenvolvimento “tipicamente humano” ela precisa do convívio com o meio ambiente circundante e com adultos (andaimes) que ajudam a criança a desenvolver no meio social.²¹²

Transpondo esta informação para o tema em questão, à partida o problema estaria resolvido, uma vez que o meio social iria auxiliar a criança a desenvolver um entendimento informado sobre os riscos do fornecimento de dados.

No entanto, questiona-se ainda hoje se os humanos encontram-se suficientemente informados sobre os perigos da permissão no fornecimento de dados.

Mais, o aliciamento para o consentimento da partilha de dados é de tal modo bem pensado e cuidado que a incerteza na permissão torna-se certa quando se coloca em questão o acesso à informação.

O facto de as crianças terem cada vez mais um acesso precoce à internet não significa que esse acesso e principalmente o consentimento de partilha de dados seja informado.

Para além disso, hoje em dia, as crianças têm um acesso cada vez mais precoce à internet e, no meu entendimento, reduzir a idade de permissão na partilha de dados para treze

²¹¹ RODRIGUES, Olga Maria Piazzentin Rolim & Melchiori, Lúcia Ebner, Aspectos do desenvolvimento na idade escolar e na adolescência, pág. 4.

²¹² RODRIGUES, Olga Maria Piazzentin Rolim; MELCHIORI, Lúcia Ebner, Aspectos do desenvolvimento na idade escolar e na adolescência, pág. 5.

anos é nada mais que “tapar o sol com a peneira”, uma simples maneira de amenizar o problema.

Uma vez que, não se consegue controlar, diminui-se a idade para que esse controle seja reduzido.

Portanto, os treze anos apenas seriam uma idade ideal se existisse algum tipo de escolarização das crianças nesse sentido.

Piaget entendia que, os adolescentes aos dezasseis anos atingem o estágio mais elevado das operações mentais. Neste estágio, o adolescente tem um desenvolvimento cognitivo mais complexo adquirindo a capacidade hipotético-dedutiva, ou seja, tendo, em atenção determinados acontecimentos, decifrar possibilidades e consequências.

Neste sentido, o pensamento do adolescente permite-lhe a capacidade de análise e reflexão dos seus atos.²¹³

Desta forma, aos dezasseis anos o adolescente está, no meu entendimento, mais preparado para realizar uma análise dos perigos da permissão para o consentimento de utilização de dados pessoais por terceiros.

Assim, com esta alteração, Portugal passaria a fazer parte do grupo de países como a Croácia, Alemanha, Grécia, Hungria, Irlanda, Luxemburgo, Países Baixos, Polónia, Roménia, Eslováquia e Eslovénia determinaram os 16 anos de idade como limite.

Não obstante o dito, o mais importante seria ainda a criação de um programa de educação para os perigos das novas tecnologias. Desta forma, elucidar-se-ia os jovens para os perigos eminentes no consentimento para a utilização de dados.

²¹³ RODRIGUES, Olga Maria Piazentin Rolim. MELCHIORI, Lígia Ebner, Aspectos do desenvolvimento na idade escolar e na adolescência, pág. 11, consultável in https://acervodigital.unesp.br/bitstream/unesp/155338/3/unesp-nead_reei1_ee_d06_s01_texto01.pdf.

Conclusão

A preocupação inicial na realização deste trabalho de investigação foi a descrição e exemplificação do que era a inteligência artificial e a internet das coisas, as suas principais utilizações, vantagens e desvantagens.

Depois, o objetivo era verificar de que modo essas novas tecnologias afetavam o quotidiano da sociedade e, principalmente, em que medida estas poderão ter alterado a fronteira da vida privada, com prejuízos para o direito à privacidade.

Vive-se numa sociedade “sedenta” por informação, mas desinformada no que concerne aos riscos do acesso a essa informação através da internet. O acesso a dados pessoais é realizado em todo o lado e de toda e qualquer forma e a questão que imputa saber é se esse acesso foi autorizado pelo utilizador e de que forma esse acesso assegura a proteção dos dados pessoais.

O direito à privacidade passou a ser mais do que a garantia do isolamento físico e do segredo, evoluindo para o poder de controlar as informações sobre si e que os outros possam ter ou tenham acesso bem como a verificação das suas finalidades.

Visando a proteção do mesmo e a salvaguarda por outros direitos fundamentais, as Constituições e as leis têm velado pela sua garantia e proteção.

Este direito é tutelado por vários instrumentos jurídicos, tanto internacionais como nacionais. Ao nível nacional este direito é tutelado pela Constituição da República Portuguesa, direito civil, direito penal, direito administrativo, Lei de Proteção de Dados e, ao nível europeu, pelo Regulamento de Proteção de Dados e outras Diretivas.

Isso demonstra que as mencionadas legislações foram-se adaptando ao desenvolvimento tecnológico colocando um travão ao desenvolvimento desgovernado das novas tecnologias, assegurando a proteção dos seus utilizadores.

Acontece que, o avanço tecnológico é de tal forma rápido que a legislação criada se torna rapidamente obsoleta. O aparecimento de novas tecnologias, como por exemplo, o *ChatGpT*, redefinem a utilização dos dados pessoais como até agora eram conhecidos, o que leva a lacunas legais e novas lesões ao direito em causa.

Os dados são agora considerados como nova matéria-prima para empresas que procedem à recolha e venda dos mesmos com vista, por exemplo, à análise para o direcionamento de produtos e publicidade.

A utilização de dados pelas entidades tecnológicas levantou problemas não só ao nível da proteção de dados, mas também, ao nível da transparência, discriminação, responsabilidade, entre outros.

Porém, não será abusivo afirmar que, enquanto não existir uma sensibilização e tomada de consciência por parte dos utilizadores para a importância de se precaverem dos seus direitos e de se consciencializarem dos riscos da utilização destes equipamentos, não existirá nenhuma lei cem por cento eficaz.

Aliás, se utilizadores adultos não têm esse conhecimento ou consciência muito menos terão as crianças constantemente conectadas a estes equipamentos.

Esta questão é agravada quando, modelos de linguagem como o *ChatGpt*, asseguram a resposta a variadas questões e a elaboração de múltiplos documentos, dos quais não se responsabilizam pela inserção de dados pessoais ou pelas produções defeituosas ou erradas.

É claro que, a legislação criada neste sentido não deve impedir o acesso ou utilização destas novas tecnologias, pelo contrário, deve permitir que as mesmas proliferem contendo, no entanto, uma mão firme na proteção dos princípios éticos e jurídicos.

Portanto, parece possível afirmar que a presente dissertação, apesar das várias dificuldades encontradas no âmbito da investigação, conseguiu encontrar respostas para as perguntas inicialmente formuladas e que serviram de base para a elaboração deste trabalho.

Todavia, a mestrandia está consciente que este trabalho constitui apenas o ponto de partida para um estudo superior, certamente mais complexo e completo, para o estudo da proteção de dados na nova era digital.

Bibliografia

AC. Tribunal de Justiça UE 4 de maio de 2023. 1ª secção. Proc. C-487/21. Disponível na Internet em: <<https://curia.europa.eu/juris/document/document.jsf?jsessionid=89DF9C842926C52900ECB31AD7D2D116?text=&docid=273284&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=4910538>>.

AC. Tribunal de Justiça UE, 4 de maio de 2023. Proc. C-300/21. 3ª Secção. Disponível na Internet em: <<https://curia.europa.eu/juris/document/document.jsf?jsessionid=89DF9C842926C52900ECB31AD7D2D116?text=&docid=273284&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=4910538>>.

AC. Tribunal de Justiça UE, 13 de Maio de 2014. Proc. C-131/12. Grande Secção. Disponível na Internet em: <<https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT>>

AC. Tribunal Judicial UE, 22 de junho de 2023, Proc. C-579/21. 1ª secção. Disponível na Internet em: <<https://curia.europa.eu/juris/document/document.jsf?jsessionid=D10F722E24D570C333CBF545A4700AC6?text=&docid=274867&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=24645757>>.

AC. Tribunal Justiça UE, 6 de outubro de 2015, Proc. C-362/14. Grande secção. Disponível na Internet em: <<https://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=PT>>

ARAGÃO, Alexandra. 2020. Questões ético-jurídicas relativas ao uso de apps geradoras de dados de mobilidade para vigilância epidemiológica da Covid-19. Uma perspetiva Europeia. Coimbra: Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra. (Dissertação de Mestrado), pdf.

AROOSA, Ullah., et al. 2021. Securing NDN-based internet of health things through cost-effective signcryption scheme: Review of Hindawi, pág. 1 a 13. Disponível na Internet em: <<https://www.hindawi.com/journals/wcmc/2021/5569365/>>.

ASCENSÃO, José de Oliveira. 2003. *Direito Civil Teoria Geral*, 2º ed., revista e atualizada. Vol. II. Coimbra: Coimbra Editora.

ASHISH Ghosh, CHAKRABORTY Debasrita, LAW Anwesha. 2018. *Artificial intelligence in Internet of things*: Review of Wiley, pág. 1 a 12. Disponível na Internet em <https://www.researchgate.net/publication/328223360_Artificial_Intelligence_in_Internet_of_Things>.

ASTHON, Kevin. The Internet of Things will disrupt transportation. 2023 [referencia de 14 de Dezembro de 2017]. Disponível na Internet em https://youtu.be/PXncS2_63o4

ÀVILA , Ana Paula Oliveira, WOLOSYN, André Luís. 2017. A tutela jurídica da privacidade e do sigilo na era digital: Review of Revista de Investigações Constitucionais.

BHBOSALE, S., Pujari, V., & MULTANI, Z. 2020. National Seminar on “Trends in geography, commerce, IT and sustainable development”. Advantages And Disadvantages Of Artificial Intellegence: Review of Research Gate. pág. 1 a 3.

BORGES, Paulo. I. C. 2015. Internet-of-Things, An Arduino-based Domotic System for the Internet-of-Things. Lisboa: Instituto Superior Técnico, pág. 1 a 5.

BOSTROM, Nick. 2016. Superintelligence. Review for: Oxford University Press.

CANOTILHO, José Joaquim Gomes, MOREIRA, Vital 2007. Constituição da República Portuguesa Anotada, 4ª. ed. rev. ed., Vol. I. Coimbra: Coimbra Editora.

CARDOSO, Donato. 2019. O uso de aplicações IoT. Disponível na Internet em: <"<https://www.access.run/2019/07/4-aplicacoes-iot-nas-empresas-que-voce-precisa-conhecer/>">

CASTELLS, Manuel (2002). A sociedade em rede. 6ª ed., Vol. 1. São Paulo, Brasil : Paz e Terra S/A.

CASTRO, Catarina Sarmento. 2016. 40 anos de “Utilização da Informática” - o artigo 35.º da Constituição da República Portuguesa, Epública Revista de Direito.

CHIRIGATI, Fernando Seabra. 2009. Obtido de computação em nuvem: Universidade Federal do Rio de Janeiro. Disponível na Iternet em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2009_2/seabra/introducao.html>.

COLLAÇO, i. d. 2006. Comemorações dos 35 anos do código civil e dos 25 anos da reforma de 1977 (vol. ii). Coimbra: Coimbra Editora.

COMISSÃO EUROPEIA, O que são dados pessoais. (s.d.). Disponível na Internet em: <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_pt>

COMISSÃO EUROPEIA, 2019, Grupo Independente de peritos de alto nível sobre a inteligência artificial. Orientações éticas para uma IA de confiança. EU publicações. Disponível na Internet em: <<https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-pt/format-PDF>>.

CORDEIRO, A. Barreto Menezes. 2020. Direito da Proteção de dados. À luz do RGPD e da Lei n.º 58/2019. Coimbra: Coimbra Editora.

COUTO, M. L. 2016. O E-Commerce à luz do direito – Análise do Regulamento Geral da. 49. Porto: Universidade Católica Portuguesa (Dissertação de Mestrado), pdf.

CUNHA, Tiago Barros, FILHO, Adalberto Simão. 2017. A teoria dos círculos concêntricos e a preservação da privacidade humana no registo civil das pessoas naturais, V Congresso brasileiro de processo coletivo e cidadania Review for Universidade de Ribeirão Preto. pp. 265-282.

DIÁRIO DE NOTÍCIAS. 14 de Fevereiro de 2022. Ciberataques: Laboratórios Germano de Sousa mantêm-se encerrados. Disponível na Internet em : <<https://www.dn.pt/sociedade/ciberataques-laboratorios-germano-de-sousa-mantem-se-encerrados-14586892.html>>.

DIÁRIO DE NOTÍCIAS. 08 de Fevereiro de 2022. PJ investiga ataque informático à Vodafone. Diário de Notícias. Disponível na Internet em: <<https://www.dn.pt/sociedade/servicos-de-voz-movel-da-vodafone-registam-recuperacao-progressiva-14568590.html>>.

DIAS, Carlos André Ferreira. 2019. A privacidade na era da internet das coisas. Porto: Faculdade de Direito Universidade do Porto (Dissertação de mestrado) pdf.

DIENGUES, Pedro Miguel. 2020. *Vantagens e desafios: O incrível mundo novo da internet das coisas (IoT)*. Disponível na Internet em: <<https://www.sage.com/pt-pt/blog/vantagens-e-desafios-o-incr-vel-mundo-novo-da-internet-das-coisas-iot/>>.

DINESH Kalla, NATHAN Smith. 2023 Study and analysis of Chat GPT and its impact on. Review for *International Journal of Innovative Science and Research Technology*.

ENCINAS, Eiranova Emilio. 2001. *Código civil Alemán comentado*. Madrid: Marcial Pons.

EUROPEAN COMMISSION. 2022. Digital privacy. Disponível na Internet em: <https://digital-strategy.ec.europa.eu/en/policies/digital-privacy>.

EXPRESSO, 30 de Janeiro de 2022. Hackers do Lapsu\$ Group anunciaram ter roubado informações do site do Parlamento. Site esteve em baixo durante cinco minutos, PJ está a investigar. Disponível na Internet em: <<https://expresso.pt/sociedade/hackers-do-lapsus-group-anunciaram-ter-roubado-informacoes-do-site-do-parlamento-site-esteve-em-baixo-durante-cinco-minutos-pj-esta-a-investigar/>>.

EXPRESSO, 9 de julho de 2016. Uma morte não vai parar os carros autónomos. Disponível na Internet em: <https://expresso.pt/sociedade/2016-07-09-Uma-morte-nao-vai-parar-os-carros-automonos>.

FERNANDES, Luís A. Carvalho. 2010. *Teoria Geral Do Direito Civil*, 5ª ed., Vol. II. Lisboa: Universidade Católica Editora. Disponível na Internet em: <<https://repositorio.ucp.pt/bitstream/10400.14/36594/1/97897254027>>.

FILHO, Nelson Bellicanta. 2019. Trumit - Gerenciador de confiança para IoT. Curitiba, Brasil: Universidade Federal do Paraná.

FROTA, Hidenberg Alves da. 2007. A proteção da vida privada, da intimidade e do segredo no Direito brasileiro e Comparado: Anuario de Derecho Constitucional Latinoamericano. Disponível na Internet em: <<http://historico.juridicas.unam.mx/publica/librev/rev/dconstla/cont/2007.2/pr/pr2.pdf>>

GARDNER, Howard. 2005. *Inteligências Múltiplas*, 1ª ed. Brasil: Artmed Editora.

GAYANTHA M. H., KITHULWATTAB, W.M.C.J.T., RATHNAYAKA. R.M.K.T. 2022. The Interconnection of Internet of Things and Artificial Intelligence: Disponível na Internet em: <[file:///C:/Users/Eduarda%20Guimar%C3%A3es/Downloads/srilankajournalofappliedsciences%20\(1\).pdf](file:///C:/Users/Eduarda%20Guimar%C3%A3es/Downloads/srilankajournalofappliedsciences%20(1).pdf)>.

GIOVANNI, B. 1936. *La stipulazione del contratto ad opera di una sola persona*, 1ª ed., Vol. XXII. Padova, Itália: CEDAM.

GONÇALVES, M. E. et al. 2003. *Direito da Informação. Novos direitos e formas de regulação na sociedade da informação*. Coimbra: Almedina.

GREENGARD, Samuel. 2015. *The Internet of Things*. Cambridge: The MIT Press.

GRUPO DE TRABALHO DO ART. 29º. 2014. Parecer 05/2014 sobre técnicas de anonimização. Grupo de Trabalho para a Proteção das Pessoas no que Diz Respeito ao Tratamento de Dados Pessoais. Disponível na Internet em:

<https://ec.europa.eu/justice/article-29/documentation/opinion_recommendation/files/2014/wp216_pt.pdf>.

HARARI, Yuval Noah. 2017. Homo Deus: A Breaf History of Tomorow. [S.I]: Harper.

HÖRSTER, Heinrich Ewald, SILVA Sónia Moreira da. 1992., A Parte Geral do Código Civil Portugues.2ª ed.[S.I]: Almedina.

JÚNIOR, Francisco Gomes, 2021. A proteção dos dados pessoais e os hackers, Migalhas. Disponível na Internet em: <https://www.migalhas.com.br/depeso/344504/a-protecao-dos-dados-pessoais-e-os-hackers>

JULIANA. 2021. Proteção de dados e Inteligência Artificial: desafio da LGPD. Neuralmind. Disponível na Internet: <<https://neuralmind.ai/2021/02/10/protecao-de-dados-e-inteligencia-artificial-o-desafio-da-lgpd/>>.

LEI DA PROTEÇÃO DE DADOS PESSSOAIS, Lei nº58/2019, de 08 de Agosto.

LI, Zihao. 2023. The Dark Side of ChatGPT: Legal and Ethical Challenges from Stochastic parrots and hallucination. Disponível na Internet em: <<https://arxiv.org/ftp/arxiv/papers/2304/2304.14347.pdf>>

LIMA, Pires de Lima, VARELA, João de Matos Antunes. 2010. Código Civil Anotado 4ª edição revista e atualizada. 4ª ed., Vol. I. Coimbra: Coimbra Editora.

MARTINS, José Eduardo Figueiredo de Andrade. 2020. Dilemas éticos e jurídicos do uso da inteligência artificial na prática jurídica. CIDP - Centro de Investigação de Direito Privado .

MATTEO, Larry A., Cannarsa, Michel, PONCIBÒ Cristina. 2019. The cambridge handbook of smart contracts, blockchain technology and digital platforms. Cambridge: Cambridge University Press.

MENDES, Pedro. 23 de Dezembro de 2022. StayAway Covid: como funciona a app. (I. Lourinho, C. Santos, Editores, & D. Proteste, Produtor) Obtido de Deco Proteste: <<https://www.deco.proteste.pt/tecnologia/telemoveis/noticias/stayaway-covid-como-funciona-a-app.>>

CORDEIRO, A. Menezes, Perestelo de Oliveira, A., & Pereira Duarte, D. 2019. Definição de Perfis e Decisões Individuais automatizadas no Regulamento Geral sobre a Proteção de Dados. Coimbra: Almedina.

MILLER, Michael. 2015. The internet of things - How Smart TVs, Smart Cars, Smart Homes and Smart Cities are Changing the World. Indianapolis: Pearson Education.

MIRANDA, Jorge., MEDEIROS, Rui. 2010. Constituição Anotada Portuguesa, 2ª ed. Coimbra: Coimbra Editora.

MÚTIPLoS. 2020. The Internet of things: Applications for business. Exploring the transformative potential of IoT. The economist Intelligence Unit. Disponível na Internet em: <https://euagenda.eu/upload/publications/18062020_cte-20report_final.pdf>

MÚTIPLoS. 2003. Estudos em homenagem ao professor doutor Inocêncio Galvão Telles, Vol. IV. [S.I.]: Almedina.

NEELAM, Sankeerthana. Internet of Things in Healthcare. Faculty of Computing, Blekinge Institute of Technology. (Dissertação de Mestrado) pdf.

NETO, Filipe Teixeira. 2017. A ilicitude enquanto pressuposto da responsabilidade civil delitual: um exame em perspectiva comparada (luso-brasileira). Review for CIDP revistas. Disponível na Internet em: <https://www.cidp.pt/revistas/rjlb/2017/6/2017_06_1163_1190.pdf>.

NESTOR, Caticha et al. Inteligência Artificial, Revista USP, ISSN 0103-9989. Disponível na Internet em: <<https://www.revistas.usp.br/revusp/issue/view/11447/1780>>.

NETO, Abilio. 2013. Código Civil Anotado. 18º ed. Lisboa: Ediforu Edições Jurídicas.

OTTONI, André Luís Carvalho. 2010. Introdução à Robótica. Universidade São João Del-Rei, Brasil Disponível na Internet em: <https://www.ufsj.edu.br/portal2-repositorio/File/orcv/materialdeestudo_introducaoarobotica.pdf>.

THE NORWEGIAN DATA PROTECTION AUTHORITY, 2018, Artificial intelligence and privacy. Disponível na Internet em: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>.

PANAGOPOULOU, Fereniki., PARPOULA, Christina., KARPOUZIS, Karpouzis. 2023. Legal and ethical considerations regarding the use of ChatGPT in education. Disponível na Internet em: < <https://arxiv.org/ftp/arxiv/papers/2306/2306.10037.pdf>>

PEPPET, Scoot R. 2015. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. Disponível na Internet em: <<https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf>>

PINTO, Carlos Alberto da Mota. 2005. *Teoria geral do direito civil*, 4ªed. Coimbra: Coimbra Editora.

PORTO, M. C. (2016). *Teoria da Integração e Políticas da União Europeia* (5ª Edição ed.). Almedina S.A.

PROPOSTA DE DIRETIVA 2022/0303 (COD) do Parlamento e do Conselho relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial, 28 de setembro de 2022, (Diretiva Responsabilidade IA),

RAMASAMY, Lakshmana Kumar, KADRY, Seifedine Kadry 2021. Blockchain in the Industrial Internet of Things.

RAMOS, Nuno André Novo, 2020. Responsabilidade civil em dano causado por mecanismo dotado de inteligência artificial, Universidade Lusíada Lisboa (Dissertação de mestrado), pdf.

RODRIGUES, Olga Maria Piazzentin Rolim., MELCHIORI, Lígia Ebner. Aspectos do desenvolvimento na idade escolar e na adolescência. Disponível na internet em: <https://acervodigital.unesp.br/bitstream/unesp/155338/3/unesp-nead_reei1_ee_d06_s01_texto01.pdf>.

RTP. 2022. Ciberataque. Laboratórios Germano de Sousa adiam reabertura. Disponível na Internet em: <https://www.rtp.pt/noticias/pais/ciberataque-laboratorios-germano-de-sousa-adiam-reabertura_n1384288>

REGULAMENTO (UE) 2016/679 de 27 de Abril de 2016,

SANTOS, Pedro Miguel 2016. Internet das Coisas: O desafio da privacidade. Setúbal: Instituto Politécnico Setúbal. (Dissertação de Mestrado) pdf.

SAS. Análises Preditivas: O que são e qual a sua importância. Disponível na Internet em: <https://www.sas.com/pt_br/insights/analytics/predictive-analytics.html>.

SILVA, Joana Vaz, 16 de abril de 2023. A batalha do séc. XXI? – Chat GPT vs Proteção de dados. Review for Direito Criativo. Disponível na Internet em: <https://direitocriativo.com/a-batalha-do-sec-xxi-chat-gpt-vs-protacao-de-dados/>.

SHINO, Kim., GANESH, Gandra Deka. 2020. Advanced Applications of Blockchain Technology. 1ª ed. Singapore: Springer.

SHULZE, Alberto De Franceschi Reiner. 2019. Digital Revolution - New Challenges for Law. [S.I]: C.H.Beck .

SILVA, Bárbara Jennifer Paz de Abreu da 2020. Inteligencia artificial e as suas implicações etico-juridicas. Faculdade de Direito da Universidade Nova de Lisboa. (Dissertação de Mestrado) pdf.

SILVA, Heraclides Sequeira dos Santos. 2017. A proteção de dados pessoais na era global: o caso schrmes. Faculdade de Direito da Universidade Nova de Lisboa Disponível na Internet em : <https://run.unl.pt/bitstream/10362/20567/1/Silva_2017.pdf>

SOFISICA. GPS - O que é, como funciona: Disponível na Internet em: <<https://www.sofisica.com.br/conteudos/curiosidades/gps.php>>.

STEPHENS-DAVIDOWITZ, Seth. (2018). Everybody lies, big data, new data, and what the internet can tell us about who we really are. [S.I]: HarperCollins.

SUPREMO TRIBUNAL DE JUSTIÇA, Colóquio Tribunais e inteligência artificial – uma odisseia no século XXI. (referência de 12 de maio de 2023). Disponível na Internet em: <<https://www.stj.pt/?p=17432>>.

TURNER, Jacob. 2019. Robot Rules. Regulating Artificial Intelligence. London, England: Palgrave Macmillan Cham.

VEIGA, Adélcia Solange Pereira Gonçalves da. 2020. Proteção de dados: O direito à privacidade na era digital. Universidade Autónoma de Lisboa. Disponível na Internet em: <https://repositorio.ual.pt/bitstream/11144/5046/1/Disserta%C3%A7%C3%A3o%20de%20Mestrado%20-%20Final%20-%20Revista%206.7.2020_%20AV.pdf>.