Universidade do Minho
Escola de Direito

Joana Pimentel Furtado

A privacidade e proteção de dados pessoais nos dispositivos da Internet das Coisas: o caso dos dispositivos de consumo

outubro de 2024

UMinho | 2024 Joana Pimentel Furtado **A privacidade e proteção de dados pessoais nos dispositivos da Internet das Coisas: o caso dos dispositivos de consumo**

Universidade do Minho
Escola de Direito

Joana Pimentel Furtado

A privacidade e proteção de dados pessoais nos dispositivos da Internet das Coisas: o caso dos dispositivos de consumo

Dissertação de Mestrado
Mestrado em Direito e Informática

Trabalho efetuado sob a orientação da
Profª. Doutora Teresa Alexandra Coelho Moreira
e do
Prof. Doutor José Carlos Bacelar Ferreira Junqueira Almeida

outubro de 2024

Agradecimentos

Aos meus pais e irmã pelo apoio incondicional, não só durante a realização desta dissertação, mas ao longo de todos estes anos. Mesmo quando distantes, continuam a ser o meu maior pilar.

Ao Guilherme, pelo apoio diário e por acreditares sempre em mim. Sem ti este percurso teria sido muito mais difícil.

À Universidade do Minho pela oportunidade de realizar o meu mestrado num ambiente enriquecedor e por proporcionar os recursos necessários para o desenvolvimento desta dissertação.

Um agradecimento especial aos meus orientadores, a prof.ª Doutora Teresa Alexandra Coelho Moreira e o prof. Doutor José Carlos Bacelar Ferreira Junqueira Almeida pela disponibilidade e valiosas contribuições ao longo deste processo.

Declaração de Integridade

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração. Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

A privacidade e proteção de dados pessoais nos dispositivos da Internet das Coisas: o caso dos dispositivos de consumo

Resumo

A Internet das Coisas é uma tecnologia cada vez mais presente no nosso dia-a-dia. Este tipo de tecnologia pode ser implementado em diversos setores, em especial nos vários objetos de consumo que utilizamos diariamente, desde relógios, óculos, televisões, eletrodomésticos, câmaras de segurança domésticas, entre outros. A oferta deste tipo de dispositivos "ligados" à internet está a aumentar e a transformar o modo como vivemos.

A UE tem desenvolvido diversos regulamentos com o propósito de proteger a privacidade e os dados pessoais dos indivíduos, sendo importantes no contexto da Internet das Coisas, uma vez que os seus dispositivos trazem diversos problemas em termos de privacidade e proteção de dados, mas também a níveis de segurança e legalidade. Coloca-se destaque ao Regulamento Geral sobre a Proteção de Dados que desempenha um papel fundamental no domínio da proteção dos dados pessoais através da implementação de diversos princípios fundamentais e de direitos e liberdades dos titulares dos dados.

Com a presente dissertação pretendemos compreender o que se entende por Internet das Coisas, quais os problemas que decorrem da sua utilização e quais as soluções para esses problemas. Começamos por analisar o conceito de privacidade e a sua evolução ao longo do tempo e algumas das leis e regulamentos implementados para proteção dos dados pessoais, a nível nacional, europeu e internacional. De seguida, tentamos entender em que consiste a Internet das coisas, qual a sua história, como funciona e os dispositivos de consumo existentes. Posteriormente, são analisados os diversos problemas decorrentes dos dispositivos de consumo da Internet das Coisas e por último, os meios de resolução dos problemas mencionados, que inclui algumas medidas jurídicas implementadas pelos regulamentos da União Europeia, em especial o RGPD, e alguns métodos e boas práticas tecnológicas.

Palavras-chave: Internet das Coisas; privacidade; proteção de dados; Regulamento Geral sobre a Proteção de Dados

Privacy and personal data protection in Internet of Things devices: the case of consumer devices

Abstract

The Internet of Things is a technology that is increasingly present in our daily lives. This type of technology can be implemented in various sectors, especially in the various consumer objects we use daily, from watches, glasses, televisions, household appliances and home security cameras, among others. The supply of this type of "connected" devices to the internet is increasing and transforming the way we live.

The EU has developed several regulations to protect individuals' privacy and personal data, which are important in the context of the Internet of Things, since these devices pose several problems in terms of privacy and data protection, but also in terms of security and legality. Emphasis is placed on the General Data Protection Regulation, which plays a fundamental role in the field of personal data protection by implementing various fundamental principles and the rights and freedoms of data subjects.

This dissertation aims to understand what the Internet of Things consists of, what problems arise from its use and what solutions to these problems exist. We begin by analyzing the concept of privacy and its evolution over time and some of the laws and regulations implemented to protect personal data at national, European and international level. Next, we try to understand what the Internet of Things is, what its history is, how it works and the existing consumer devices. Afterwards, we analyze the various problems arising from Internet of Things consumer devices and, finally, the ways of resolving the problems mentioned, which includes some legal measures implemented by European Union regulations, especially the GDPR, and some technological methods and best practices.

Keywords: Internet of Things; privacy; data protection; General Data Protection Regulation

Índice

Abreviaturas

AA – Aprendizagem Automática

AIPD - Avaliação de Impacto sobre a Proteção de Dados

API – Application Programming Interface

ARPA - Advanced Research Project Agency

ARPANET – Advanced Research Projects Agency Network

CCR – Command and Control Research

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CEDH – Convenção Europeia dos Direitos Humanos

CMS – Computação Multipartidária Segura

CNPD – Comissão Nacional de Proteção de Dados

CRP – Constituição da República Portuguesa

DUDH - Declaração Universal dos Direitos do Homem

EEE – Espaço Económico Europeu

IA – Inteligência Artificial

IP – Internet Protocol

IPTO – Information Processing Techniques Office

IoT – Internet of Things, Internet das Coisas

LAN – Local Area Network

NFC – Near Field Communication

PDdCD – Proteção de Dados desde a Conceção e por Defeito

PET – Privacy-Enhancing Technologies

RA – Realidade Aumentada

RFID – Radio Frequency Identification

RGPD – Regulamento Geral de Proteção de Dados

RV - Realidade Virtual

SPA – Smart Home Personal Assistants

TCP – Transmission Control Protocol

TEDH – Tribunal Europeu dos Direitos do Homem

TEE– Trusted Execution Environment

TIC – Tecnologias da Informação e Comunicação

UE – União Europeia

WWW – World Wide Web

XAI – Explainable Artificial Intelligence

Introdução

Com o surgimento da internet e com o seu contínuo desenvolvimento foram criadas diversas tecnologias que foram colocando progressivamente em risco a privacidade e proteção de dados pessoais. Um exemplo dessas tecnologias desenvolvidas é a Internet das Coisas que abarca diversos dispositivos de consumo e que se encontram cada vez mais presentes à nossa volta e colocam diversos problemas aos seus utilizadores, apesar dos seus inúmeros benefícios. É, por isso, relevante conhecer esses problemas e saber como os resolver de forma a podermos simultaneamente aproveitar os seus benefícios e mitigar os seus problemas.

Posto isto, no primeiro capítulo, começamos por fazer uma breve referência da história do surgimento da internet. Após isso, é analisado o conceito de privacidade, que foi alterando ao longo do tempo para acompanhar os diversos progressos tecnológicos realizados. De modo a garantir a privacidade e proteger os dados pessoais, foram criadas diversas leis e regulamentos, recebendo mais destaque o Regulamento Geral sobre a Proteção de Dados. Este Regulamento tem um papel importante, pois estabelece os diversos princípios fundamentais e direitos dos titulares dos dados, protegendo o tratamento dos dados pessoais no âmbito da União Europeia. Este possibilita que os cidadãos tenham acesso e controlem os seus dados e apresenta diversas regras que as organizações devem seguir de forma a garantir a privacidade e segurança dos indivíduos e simultaneamente beneficiar de um maior grau de confiança por parte dos consumidores.

De seguida, no segundo capítulo, pretende-se perceber em que consiste a Internet das Coisas, a sua história e como funciona. Depois, são mencionados os dispositivos de consumo da IoT existentes mais importantes, uma vez que dispositivos inteligentes como eletrodomésticos, câmaras de segurança, dispositivos vestíveis, televisões e outros objetos estão a ser cada vez mais utilizados no dia-a-dia dos consumidores e trazem diversos benefícios.

Contudo, apesar desses inúmeros benefícios, os dispositivos de consumo apresentam problemas significativos em termos de privacidade e proteção de dados. Neste sentido, no terceiro capítulo, são mencionados alguns desses problemas, pois, esses dispositivos recolhem uma grande variedade de informações pessoais que podem causar potenciais violações de privacidade através, por exemplo, da troca de dados pessoais entre os diversos dispositivos ou para terceiros, isto sem o conhecimento ou consentimento do utilizador. Deste modo, a privacidade e a proteção de dados pessoais torna-se, assim, uma preocupação central no âmbito da Internet das Coisas. A utilização dos

dispositivos cria diversos problemas legais e de privacidade e segurança, uma vez que a informação recolhida pode ser combinada e analisada sem a adequada transparência, segurança, responsabilidade ou consentimento.

Por fim, no quarto e último capítulo, são reveladas formas de resolver esses problemas decorrentes da utilização da IoT, em que, de forma a os combater, é essencial a colaboração entre as diversas partes interessadas, de modo a desenvolverem diversas estratégias tanto jurídicas como técnicas que respeitem a privacidade e garantem a segurança dos utilizadores, ao mesmo tempo que se promove a inovação da Internet das Coisas.

Capítulo I – A Privacidade e Proteção de Dados Pessoais

1. A Evolução da Internet e a Privacidade

A expansão da internet, embora tenha contribuído para um fácil acesso a um mundo de informações e comunicações, colocou-nos diante o desafio da proteção da nossa privacidade e dos nossos dados pessoais que se tornaram vulneráveis a invasões e explorações constantes. E a sua permanente evolução, com a introdução da Inteligência Artificial (IA), da Internet das Coisas (IoT), do *Big Data*, entre outras, traz cada vez mais novos desafios.

1.1. A Internet

A história da internet começou quando o presidente dos EUA, Eisenhower, criou em 1957 a ARPA *(Advanced Research Project Agency*) como reação aos avanços tecnológicos russos e cujo objetivo era o desenvolvimento de programas relacionados com satélites e com o espaço. Após a entrega em 1961 de um computador IBM pela Força Aérea à Universidade da Califórnia foi possível à ARPA desenvolver a sua investigação na área da informática. Foi criado o *Information Processing Techniques Office* (IPTO) por Joseph Licklider, coordenador do *Command and Control Research* (CCR), para a transmissão de dados e comunicação interativa. Para que houvesse uma comunicação rápida entre as equipas de investigadores foi necessária a construção de uma rede, tendo a investigação sido dirigida para a construção de redes de comunicação de dados[1].

A primeira rede de computadores foi construída entre quatro universidades[2], tendo nascido a 1 de Dezembro de 1969 a ARPANET (*Advanced Research Projects Agency Network*). Na década de 70, foi desenvolvido o TCP/IP (*Transmission Control Protocol e Internet Protocol*), um conjunto de protocolos que permitia que diferentes redes comunicassem entre si, tornando-se a base da comunicação na internet[3].

Na década de 90, o Departamento de Defesa dos EUA desmantelou a ARPANET e com a criação da *World Wide Web* (WWW), a internet expandiu-se rapidamente. A *World Wide Web* tornou-se a componente mais importante da internet, como instrumento de comunicação e de interação entre as pessoas e de transmissão de informação[4]. "A internet transformou-se num sistema mundial público, de redes de computadores – numa rede de redes – ao qual qualquer pessoa ou computador pode

1 ALMEIRA, José Maria Fernandes, Breve história da INTERNET, disponível em https://repositorium.sdum.uminho.pt/bitstream/1822/3396/1/INTERNET.pdf, p.1-2.

[2] Na Universidade da Califórnia, em Los Angeles, no SRI (*Stanford Research Institute*), na Universidade de Utah e na Universidade da Califórnia, em Santa Bárbara.

3 ALMEIRA, José Maria Fernandes *Op. Cit*., p.3-4.

[4] GARCIA, Marques; MARTINS, Lourenço, Direito da Informática, Edições Almedina, 2000, p.52.

conectar-se" e quando "obtida a conexão o sistema permite a transferência de informação entre computadores" [5].

A internet passou, portanto, por várias fases de desenvolvimento, evoluindo de uma rede de pesquisa académica e militar para uma plataforma global que afeta quase todos os aspetos da vida moderna. Atualmente, é utilizada em todos os setores de atividade tendo revolucionado profundamente a forma como vivemos, comunicamos, nos entretemos e trabalhamos. Com esta evolução da internet e com o aumento da sua utilização pelo público em geral, a questão da privacidade começou a ganhar gradualmente mais importância. À medida que as pessoas navegam na Internet, vão produzindo um enorme conjunto de dados e deixam, de forma ativa ou passiva, um rasto de informações[6]. As novas inovações tecnológicas tem vindo a dar cada vez mais diversos meios de invasão da privacidade das pessoas, dando origem ao processo de perda de anonimato das mesmas[7]. E contribuindo, também, para uma sociedade de controlo ou vigilância ao serem os dados pessoais alvo de uma contínua recolha, tratamento e processamento, utilizados para diversas finalidades[8].

1.2. A Privacidade

O conceito de privacidade surge desde a Antiguidade Clássica, em que na altura Aristóteles distinguia a esfera privada (*oikos*), da esfera pública (*polis*). Enquanto a esfera privada fazia referência ao respeito pela família e a questões biológicas e económicas, a esfera pública correspondia ao respeito pela liberdade política dos cidadãos. Tendo mais tarde, este conceito de privacidade passado a abranger tudo o que fosse pessoal, desde a família como as relações mais próximas de cada indivíduo até chegar ao "indivíduo singularmente entendido" e passando, seguidamente, a abranger também a "dimensão de ação e a esfera protegida" em que cada pessoa pode atuar num caminho que é independente de influências e decisões do Estado, da sociedade e das instituições[9].

A existência de um conceito universal de privacidade é um desafio devido à sua natureza complexa, que reflete variações culturais, sociais e legais. Diferentes pessoas, comunidades e sociedades atribuem significados distintos à privacidade, tornando difícil estabelecer um conceito único e abrangente. A privacidade ou "vida privada" é considerada pela doutrina como "obscura e sem um

5 ALMEIRA, José Maria Fernandes *Op. Cit.*, p.4.
[6] CORREIA, Victor, Da Privacidade, Significado e Valor, Edições Almedina, 2018, p.78
[7] MOREIRA, Teresa Coelho, A privacidade dos trabalhadores e as novas tecnologias de informação e comunicação : contributo para um estudo dos limites do poder de controlo eletrónico do empregador, Tese de Doutoramento, Universidade do Minho, 2010, disponível https://repositorium.sdum.uminho.pt/handle/1822/10470, p.29.
[8] MOREIRA, Teresa Coelho, *Op. Cit.*, p.34.
[9] CORREIA, Victor, Da Privacidade, Significado e Valor, *Op. Cit.*, p.45-46.

verdadeiro conteúdo preciso"[10] e em que muitas vezes tem um significado que difere conforme as pessoas e a situação em concreto[11] sendo, portanto, difícil delimitar o seu âmbito.

Para VICTOR CORREIA, privacidade significa "a possibilidade de ser deixado em paz, e a possibilidade de conservar o anonimato" e, o conceito de direito à privacidade "implica uma liberdade reconhecida à luz dos Direitos do Homem, direito esse que em muitos países é reconhecido e protegido juridicamente a cada indivíduo"[12]. O direito à privacidade é um dos direitos mais importantes da idade contemporânea[13]. Por privacidade entendemos como o poder de manter certas coisas íntimas reservadas, como os nossos pensamentos, as nossas experiências, os nossos planos, as nossas conversas[14]. De um modo geral, a privacidade é o conjunto das informações acerca do indivíduo, no qual ele pode decidir em manter sobre o seu exclusivo controlo ou comunicar, decidindo a quem comunicar, quando, onde e como[15]. Contudo, atualmente fornecemos dados pessoais tanto de forma consciente como inconscientemente. Partilhamos todos os dias informação sobre nós próprios: o que compramos, o que gostamos, os nossos dados biométricos, onde estamos e onde nos dirigimos, entre muito mais[16].

A ideia de direito à privacidade tem a sua origem com o artigo "*The right to privacy"*, publicado na *Harvard Law Review* de Samuel D. Warren e Louis D. Brandeis, em 1890. No qual defenderam a existência do "direito a ser deixado só" (*right to be left alone*). Direito este que "permitiria aos seus sujeitos (...) exigir a não perturbação da sua privacidade, impedindo a recolha de informações sobre a sua vida íntima ou a revelação de informações, mesmo que estas fossem verdadeiras"[17]. Surgindo assim, uma "primeira formulação jurídico-doutrinal do direito à privacidade", com natureza constitucional e "ligado à personalidade" [18].

O direito à privacidade trata-se de um direito fundamental. Este direito faz parte dos direitos de personalidade, uma vez que decorre da dignidade humana e interliga-se com outros direitos[19]. Segundo VITOR CORREIA, os direitos de personalidade "significam que todo o indivíduo tem o direito de controlar o uso do seu nome, da sua imagem, do seu corpo, da sua aparência ou de quaisquer outros elementos

[10] MOTA PINTO, Paulo, "A proteção da vida privada na jurisprudência do Tribunal Constitucional", disponível em https://www.tribunalconstitucional.pt/tc/conteudo/files/textos/textos0202035.pdf, p. 7
[11] MOREIRA, Teresa Coelho, *Op. Cit.*, p.68.
[12] CORREIA, Victor, *Op. Cit.*, p.51.
[13] MOREIRA, Teresa Coelho, *Op. Cit.*, p.68.
[14] VÉLIZ, Carissa, "Privacidade é poder, por que razão e como devemos recuperar o controlo dos nossos dados, Bertrand Editora,2022, p. 11
[15] CORREIA, Victor, Sobre o Direito à Privacidade, O Direito, ano 146, n.º 1, 2014, disponível em https://www.academia.edu/es/6106718/Sobre_o_direito_à_privacidade , p.5
[16] MAMEDE, Ricardo Paes, A vida sem privacidade, artigo, 2022, disponível em https://www.uc.pt/protecao-de-dados-e-informacao-administrativa/artigos-e-opinioes/a-vida-sem-privacidade/.
[17] FARINHO, Domingos Soares, Intimidade Da Vida Privada e Media no Ciberespaço, Edições Almedina, 2006, p.44.
[18] MOREIRA, Teresa Coelho, *Op. Cit.*, p.74.
[19] MOREIRA, Teresa Coelho, *Op. Cit.*, p.68.

constitutivos da sua identidade" [20]. O direito à privacidade é considerado um direito universal pois, é aplicável a todas a pessoas, não obstante a sua nacionalidade, etnia, religião, etc[21]. Estando aqui em causa o princípio da universalidade dos direitos do homem[22].

A evolução do direito à privacidade e do direito à proteção de dados tem sido modelados ao longo do tempo por diversas convenções e declarações importantes no âmbito do direito internacional e europeu. Foi apenas após a II Guerra Mundial que começou a existir um interesse em regular a proteção do direito à privacidade, podendo também ser qualificado como direito ao respeito da vida privada. A proteção do direito à privacidade surge, então, na *Declaração Universal dos Direitos do Homem* (DUDH), aprovada a 10 de dezembro de 1948[23]. Conforme o seu artigo 12.º, "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei". A DUDH tinha como propósito reconhecer vários direitos necessários para a vida e desenvolvimento do Homem em sociedade e apesar de esta Declaração não ter um carácter vinculativo, teve uma "grande força moral e política e muitas das suas disposições foram adotadas noutros diplomas normativos internacionais" [24].

Em 1949, foi criado o Conselho da Europa que tem o objetivo de "proteger os direitos humanos e as liberdades fundamentais e promover uma maior unidade entre os Estados Europeus". Após um ano da sua criação foi elaborada a *Convenção Europeia dos Direitos Humanos* que tem o propósito de proteger direitos e liberdades fundamentais, constituindo-se assim o primeiro texto europeu que consagrou a proteção da privacidade[25]. O seu artigo 8.º prevê o "direito ao respeito pela vida privada e familiar" e estipula que "qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência". Este direito insere-se na categoria dos direitos de personalidade "que estão ligados à própria existência da pessoa". Segundo TERESA COELHO MOREIRA procura-se assegurar a cada pessoa "um âmbito próprio e reservado face a ingerências de terceiros por forma a garantir um determinado nível de qualidade de vida e, também, assegurar o desenvolvimento da própria personalidade" [26]. Foi criado pela Convenção Europeia, o Tribunal Europeu dos Direitos do Homem (TEDH), com o "objetivo de proteger os cidadãos contra violações dos direitos humanos". Deste modo, qualquer pessoa cujos direitos tenham sido violados por um Estado-Membro nos termos

[20] CORREIA, Victor, Da Privacidade..., *Op. Cit.*, p.52.
[21] CORREIA, Victor, Da Privacidade..., *Op. Cit.*, p.52.
[22] MOREIRA, Teresa Coelho, *Op. Cit.*, p.138.
[23] MOREIRA, Teresa Coelho, *Op. Cit.*, p.83-84.
[24] MOREIRA, Teresa Coelho, *Op. Cit.*, p.84.
[25] MOREIRA, Teresa Coelho, *Op. Cit.*, p.116.
[26] MOREIRA, Teresa Coelho, *Op. Cit.*, p.124.

da Convenção pode levar o caso ao Tribunal e os acórdãos que determinem que houve violação dos direitos humanos são vinculativos para os países em causa[27].

A DUDH e a CEDH foram criadas muito antes do desenvolvimento da internet e dos computadores. O surgimento desses instrumentos trouxeram muitos benefícios às pessoas e à sociedade em geral, contudo, ao mesmo tempo, apresentam variadíssimos novos riscos para o direito à privacidade[28]. Ou seja, na altura em que foi desenvolvida a tutela do direito ao respeito pela vida privada, "o perigo que as pessoas enfrentavam não estava relacionado com a era da informática, mas sim perante as atividades desenvolvidas pela imprensa"[29]. Como resposta à carência de regras específicas que regulassem a recolha, tratamento e utilização de dados pessoais, surgiu um novo conceito de vida privada, com o propósito de abranger novas realidades relacionadas com as inovações tecnológicas[30], em que ficou conhecido em algumas jurisdições como "privacidade informacional" ou como "direito à autodeterminação informacional"[31].

A Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal – a Convenção 108 – de 28 de janeiro de 1981, adotada pelo Conselho da Europa, foi o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados visando "garantir (...) a todas as pessoas singulares (...) o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal"[32] e teve um papel importante tendo sido "decisivo na consolidação dos princípios gerais e dos termos base utilizados", pois a sua "linguagem, os conceitos e os princípios formadores da proteção de dados encontraram aí (...) as suas bases mais sólidas" [33].

A 24 de outubro de 1995 foi adotada a Diretiva 95/46/CE do Parlamento Europeu e do Conselho que estabeleceu um quadro regulamentar com o fim de criar um equilíbrio entre um nível elevado de proteção da vida privada das pessoas e a livre circulação de dados pessoais no interior da UE tendo fixado limites estritos à recolha e à utilização de dados pessoais e solicitado "a criação, em cada Estado-Membro, de um organismo nacional independente encarregado do controlo de todas as

[27] *In* https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=LEGISSUM:eu_human_rights_convention
[28] Manual da Legislação Europeia sobre Proteção de Dados, abril de 2018, disponível em https://fra.europa.eu/pt/publication/2022/manual-da-legislacao-europeia-sobre-protecao-de-dados-edicao-de-2018, p. 21.
[29] MOREIRA, Teresa Coelho, *Op. Cit.*, p.79.
[30] MOREIRA, Teresa Coelho, *Op. Cit.*, p.78.
[31] Manual da Legislação Europeia sobre Proteção de Dados, *Op. Cit.*, p. 21.
[32] *In* https://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais
[33] CORDEIRO, António Barreto Menezes, Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019, Edições Almedina, 2022, p. 67

atividades relacionadas com o tratamento de dados pessoais" [34]. Foi revogada posteriormente pelo Regime Geral de Proteção de Dados (RGPD).

A 7 de dezembro de 2000 foi aprovada a Carta dos Direitos Fundamentais da União Europeia (CDFUE) que enumera diversos direitos fundamentais. No artigo 7.º encontra-se o previsto o "respeito pela vida privada e familiar" que refere que "todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações". Em relação ao artigo 8.º está prevista a "proteção de dados pessoais", o qual menciona no seu número 1 que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito". Dados esses que "devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação", de acordo com o número 2 desse mesmo artigo[35]. De acordo com ANTÓNIO BARRETO MENEZES CORDEIRO, os fundamentos últimos do direito à proteção de dados e dos direitos dos titulares de dados pessoais encontram-se neste artigo 8.º da Carta, que reconhece a natureza fundamental e universal do direito à proteção de dados; elenca um conjunto variado de princípios concretizados no RGPD; consagra o consentimento como principal fundamento de licitude do tratamento de dados pessoais; identifica alguns direitos dos titulares e determina a constituição de uma autoridade independente para fiscalizar o seu cumprimento[36]. Segundo este mesmo autor, o direito à proteção de dados deve ser entendido como "o conjunto sistematizado de princípios, normas e institutos que regula os dados pessoais das pessoas singulares e o seu tratamento" [37].

O direito à proteção de dados e o direito à privacidade procuram proteger valores semelhantes, como a dignidade humana e a autonomia dos indivíduos, assegurando que estes "possam livremente desenvolver as suas personalidades, pensar e formar as suas opiniões". São também um requisito prévio para o exercício de outras liberdades fundamentais, como a liberdade de expressão. Contudo, estes direitos diferem na sua formulação e alcance. Enquanto o direito à privacidade consiste numa proibição geral da intromissão, sem prejuízo de alguns critérios do interesse público que justificam essa intromissão em certos casos, o direito à proteção de dados trata-se de um "sistema de verificações e de equilíbrios" com o objetivo de proteger os indivíduos sempre que os seus dados são tratados[38].

---

[34] *In* https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046
[35] MONIZ, Graça Canto, Manual de Introdução à Proteção de Dados Pessoais, Edições Almedina, 2023, p. 10.
[36] CORDEIRO, António Barreto Menezes, *Op. Cit.*, p. 69.
[37] CORDEIRO, António Barreto Menezes, *Op. Cit.*, p. 35.
[38] Manual da Legislação Europeia sobre Proteção de Dados, *Op. Cit.*, p. 22.

2. Proteção Constitucional da Privacidade

A proteção da privacidade do nosso ordenamento jurídico é considerada inovadora[39]. É consagrada uma dicotomia protecional da privacidade, através dos artigos 26.º e 35.º da Constituição da República Portuguesa (CRP). A CRP consagra como princípio fundamental dos cidadãos o direito à privacidade ao declarar no artigo 26.º, número 1, que "a todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, à reserva da intimidade privada e familiar". O direito à privacidade é um direito absoluto, e impõe não apenas uma obrigação passiva universal, mas ainda um dever de respeito[40]. Neste artigo 26.º da CRP encontram-se consagrados diversos direitos de personalidade[41].

Em primeiro lugar, o direito ao desenvolvimento da personalidade, trata-se, conforme GOMES CANOTILHO e VITAL MOREIRA, de um "direito subjetivo fundamental ao indivíduo, garantindo-lhe um direito à formação livre da personalidade ou liberdade de ação como sujeito autónomo dotado de autodeterminação decisória" [42]. Portanto, este direito protege, a formação livre da personalidade, sem a imposição nem planificação estatal de modelos de personalidade; a proteção da liberdade de ação de acordo com o projeto de vida e das capacidades pessoais de cada pessoa e a proteção da integridade da pessoa[43]. Deste modo, como elementos principais verifica-se o direito à autoafirmação da pessoa em relação a si própria, contra quaisquer imposições de terceiros ou poderes públicos; o direito à autoexposição na interação com outros e, por último, o "direito à criação ou aperfeiçoamento de pressupostos indispensáveis ao desenvolvimento da personalidade"[44].

Outro direito que importa mencionar, presente neste artigo 26.º é o direito à reserva da vida privada e familiar, presente no número 1 e 2. O número 2 estipula que "a lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias". De acordo com GOMES CANOTILHO e VITAL MOREIRA, este direito resulta de dois direitos menores: "o direito de impedir o acesso de estranhos a informações 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" [45]. Segundo DOMINGOS SOARES, em Portugal, o direito à reserva da intimidade da vida privada "encontra os seus fundamentos na proteção da dignidade da pessoa

[39] MOREIRA, Teresa Coelho, *Op. Cit.*, p.195.
[40] CORREIA, Victor, Da Privacidade..., *Op. Cit.*, p. 61.
[41] CANOTILHO, Gomes; MOREIRA, Vital, Constituição da República Portuguesa Anotada, Volume I, Coimbra Editora, 2007, p. 461.
[42] CANOTILHO, Gomes; MOREIRA, Vital, *Op. Cit.*, p. 463.
[43] CANOTILHO, Gomes; MOREIRA, Vital, *Op. Cit.*, p. 463.
[44] CANOTILHO, Gomes; MOREIRA, Vital, *Op. Cit.*, p. 464.
[45] CANOTILHO, Gomes; MOREIRA, Vital, *Op. Cit.*, p. 467.

humana, na proteção do seu bem-estar físico e psíquico e na valoração própria da individualidade e autonomia de cada um"[46].

Passando ao artigo 35.º da CRP, com a epígrafe "Utilização da Informática", este tem como matriz essencial a temática da proteção de dados[47]. A CRP foi a primeira Lei Fundamental a reconhecer proteção constitucional aos titulares de dados pessoais[48] ao consagrar a proteção dos cidadãos face ao tratamento de dados pessoais informatizados. Este artigo 35.º foi fundamental para a posterior caracterização mundial do reconhecimento constitucional do acesso aos dados pessoais[49]. Conforme o número 1 do artigo 35.º "todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei".

Este artigo está relacionado com outros direitos, liberdades e garantias, como o desenvolvimento da personalidade, a dignidade da pessoa, da intimidade da vida privada, da integridade pessoal e da autodeterminação informativa. No número 2 do artigo 35.º, "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". Existe uma ligação entre os direitos mencionados e o respetivo tratamento informatizado. Quantos mais dados se relacionarem com a personalidade, dignidade e autodeterminação das pessoas, mais são as imposições quanto à sua recolha e utilização" [50]. Pretende-se garantir, então, um conjunto de direitos fundamentais relativos à proteção contra o tratamento informático abusivo de dados pessoais. Resulta também deste artigo o direito de acesso das pessoas aos registos informáticos que lhes digam respeito e o direito de atualização e retificação dos dados, de acordo com o número 1; o direito ao não tratamento informático de certas categorias de dados, segundo o número 3; e o direito ao sigilo, através da proibição do acesso aos dados por terceiros, de acordo o número 4.

O artigo 35º da CRP contempla um direito à autodeterminação informacional[51]. Todo este conjunto de direitos "tende a densificar o moderno direito à autodeterminação informacional", que dá a cada pessoa o direito de "controlar a informação disponível a seu respeito", de modo a impedir que a

[46] FARINHO, Domingos Soares, *Op. Cit.*, p. 44.
[47] GARCIA Marques; MARTINS Loureço, *Op. Cit.*, p. 168.
[48] CORDEIRO, António Barreto Menezes, *Op. Cit.*, p. 73.
[49] FUSTER, Gloria González, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer, 2014, p.67.
[50] CANOTILHO, Gomes; MOREIRA, Vital, *Op. Cit.*, p. 551.
[51] FARINHO, Domingos Soares, *Op. Cit.*, p. 44.

pessoa se transforme num "simples objeto de informações" [52]. Segundo TERESA COELHO MOREIRA, com este direito à autodeterminação informacional, cada pessoa "tem o direito de preservar a sua identidade, controlando a revelação e o uso dos dados que lhe dizem respeito e protegendo-se perante a capacidade ilimitada de arquivá-los, relacioná-los e transmiti-los"[53].

3. O Regulamento Geral de Proteção de Dados

A origem do Regulamento Geral de Proteção de Dados (RGPD) resulta, segundo GRAÇA MONIZ, da "necessidade de prevenir os riscos para os direitos fundamentais provocados pelos tratamentos de dados pessoais resultantes dos avanços tecnológicos"[54]. O RGPD sucedeu a Diretiva 95/46/CE. A adoção dessa Diretiva deveu-se ao surgimento das primeiras legislações nacionais no âmbito de proteção de dados, na década de 70, o que preocupou a Comissão Europeia pois os Estados-Membros acabariam por tomar soluções legislativas diferentes o que restringiria o fluxo de dados pessoais entre os Estados-Membros. Seria então necessário um ato legislativo da UE com o objetivo de "harmonizar legislações" e "remover obstáculos à livre circulação de dados pessoais[55].

Após o fim de vários anos de vigência da Diretiva 95/46/CE, foi adotado o RGPD que tem como finalidade "harmonizar e homogeneizar a matéria de proteção de dados nos vários países da UE" e consagra duas ambições importantes do processo de integração europeia que são a "realização do mercado interno, em especial a livre circulação de dados pessoais e a proteção dos direitos fundamentais"[56]. Portanto, com o RGPD pretende-se melhorar a confiança do titular dos dados pessoais enquanto consumidor da economia digital e, por um lado, "incentivar o desenvolvimento económico e a digitalização económica europeia" e, por outro, prevenir os riscos que esse processo traz para os titulares dos dados pessoais[57].

O tratamento de dados pessoais é perspetivado pelo legislador como uma atividade causadora de risco a um direito fundamental, sendo a sua proteção realizada através da regulação preventiva dos riscos criados pelo tratamento de dados pessoais[58]. Conforme o considerando 75 do RGPD, "o risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos

[52] CANOTILHO, Gomes; MOREIRA, Vital, *Op. Cit.*, p. 551.
[53] MOREIRA, Teresa Coelho, *Op. Cit.*, p. 221.
[54] MONIZ, Graça Canto, *Op. Cit.*, p. 8.
[55] MONIZ, Graça Canto, *Op. Cit.*, p. 9-10.
[56] MONIZ, Graça Canto, *Op. Cit.*, p. 13.
[57] MONIZ, Graça Canto, *Op. Cit.*, p. 22.
[58] MONIZ, Graça Canto, *Op. Cit.*, p. 28-29.

físicos, materiais ou imateriais, em especial, quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras", entre muitos outros riscos.

O RGPD consagra uma definição de "dados pessoais" e uma definição de "tratamento". De acordo com o n.º 1 do artigo 4.º, "dados pessoais" são a "informação relativa a uma pessoa singular identificada ou identificável; é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular". Nos termos do n.º 2 do mesmo artigo, entende-se por "tratamento", "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como 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".

O RGPD distingue também "dados sensíveis" ou "dados especiais", em relação aos demais dados[59]. De acordo com o Considerando 51, "merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais". Neste sentido, o artigo 9.º, nº 1, consagra que "é proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa". Diz respeito a uma categoria de dados profundamente pessoais, devido à situação de vulnerabilidade em que se coloca o titular dos dados e aos potenciais efeitos prejudiciais que resultam do seu tratamento[60]. As exceções encontram-se previstas no número 2 do mesmo artigo.

Segundo ANTÓNIO BARRETO MENEZES CORDEIRO, o direito da proteção de dados abrange duas áreas que podem ser analisadas de forma distinta e autónoma: "(i) a proteção de dados pessoais; e (ii) a segurança dos dados pessoais. A primeira foca-se no tratamento dos dados pessoais e na

[59] CORDEIRO, António Barreto Menezes, *Op. Cit.*, p. 132.
[60] CORDEIRO, António Barreto Menezes, *Op. Cit.*, p. 133.

proteção dos direitos dos titulares e a segunda concentra-se em garantir a integridade e a regular o acesso aos dados pessoais"[61].

3.1. Princípios fundamentais

O RGPD estabelece uma série de princípios fundamentais relativos ao tratamento de dados pessoais que as organizações devem seguir ao lidar com as informações pessoais e que se encontram previstos no artigo 5.º do RGPD.

a) Princípio da Licitude, Lealdade e Transparência

Encontra-se na alínea a) do número 1 do artigo 5.º e prevê que "os dados pessoais são objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados". Verifica-se que este princípio comporta três dimensões: a licitude, a lealdade e a transparência[62].

Conforme o Considerando 39 do RGPD, "o tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa". Por licitude, entende-se como o "cumprimento generalizado do Direito" num sentido amplo. Num sentido estrito, considera-se que significa que "todo e qualquer tratamento de dados pessoais, para ser lícito, carece de suporte, pelo menos, num dos seis fundamentos de licitude previstos no elenco taxativo do artigo 6.º do RGPD". Contudo, não basta ao responsável do tratamento de dados selecionar uma condição presente no artigo 6.º, é necessário também um fundamento que deve ser adequado, ou seja, que corresponda ao "objetivo, à essência e ao contexto do tratamento". Segundo GRAÇA MONIZ, os fundamentos de licitude, exceto o consentimento, "pressupõem todos a demonstração da necessidade do tratamento", e, "existindo alternativas realistas e menos intrusivas o requisito não se encontra preenchido"[63]. De acordo com o mesmo Considerando, "os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados" e "apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios".

O consentimento trata-se, portanto, de um fundamento de licitude[64] e encontra-se previsto no número 2 do artigo 8.º da CDFUE e na alínea a) do número 1 do artigo 6.º do RGPD, que dispõe que o tratamento só é lícito se "o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas". No RGPD, a definição de

[61] CORDEIRO, António Barreto Menezes, *Op. Cit.*, p. 35.
[62] MONIZ, Graça Canto, *Op. Cit.*, p. 66.
[63] MONIZ, Graça Canto, *Op. Cit.*, p. 66-68.
[64] Os restantes fundamentos de licitude estão previstos nas restantes alíneas do número 1 do artigo 6.º do RGPD, sendo eles: uma situação de contrato, o "cumprimento de uma obrigação jurídica", "interesses vitais do titular de dados", "interesse público" ou "exercício de autoridade pública" e, por último, "interesses legítimos prosseguidos pelo responsável pelo tratamento ou terceiro".

consentimento encontra-se no número 11 do artigo 4.º, que indica que o consentimento do titular dos dados trata-se de "uma manifestação de vontade, livre, específica, informada e explícita, pelo qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito seja objeto de tratamento". O regime geral aplicado ao consentimento encontra-se previsto no artigo 7.º do RGPD, com a epígrafe "Condições aplicáveis ao consentimento".

Em relação à lealdade, o artigo 8.º, n.º 2 da CDFUE prevê que os dados pessoais "devem ser objeto de um tratamento leal". A lealdade obriga que os dados pessoais não sejam tratados de um modo prejudicial, discriminador, enganador ou inesperado para o titular dos dados. Entende-se que se trata de um elemento autónomo em relação à licitude ou transparência pois, a lealdade, pode ser utilizada para contestar tratamentos que são formalmente válidos[65]. Segundo ANTÓNIO BARRETO MENEZES CORDEIRO, a "lealdade permite contestar determinados comportamentos que dificilmente poderiam ser descritos como violadores do artigo 6.º", tratando-se, a lealdade, de um conceito aberto, "passível de ser invocado em situações que contradigam o espírito do RGPD"[66].

Por seu turno, a transparência, tem como objetivo "capacitar o titular dos dados para responsabilizar as entidades que utilizam os seus dados pessoais e, assim, reforçar o controlo sobre os seus dados pessoais e a possibilidade de exercer os seus direitos"[67]. Conforme o Considerando 39 do RGPD, "deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados" e que o "princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples".

b) Princípio da Limitação da Finalidade

Previsto na alínea b) do número 1 do artigo 5.º, dispõe que os dados pessoais possam ser "recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades (...)". Este princípio determina limites ao tratamento dos dados de uma "forma flexível" ao desdobrar-se em dois elementos. Um elemento qualificativo, pois o "responsável só pode recolher dados para finalidades determinadas, explícitas e legítimas" e, um elemento restritivo, o qual os dados, uma vez recolhidos, "não podem ser posteriormente utilizados de forma incompatível com aquelas finalidades". Ambos elementos tem o

[65] MONIZ, Graça Canto, *Op. Cit.*, p. 99.
[66] CORDEIRO, António Barreto Menezes, *Op. Cit.*, p. 153.
[67] MONIZ, Graça Canto, *Op. Cit.*, p. 103.

objetivo de limitar o tratamento dos dados pelo responsável pelo tratamento evitando, assim, que o titular seja surpreendido com tratamentos inesperados[68] e garantindo o controlo dos respetivos direitos à autodeterminação informacional[69].

c) Princípio da Minimização dos Dados

Está previsto na alínea c) do número 1 do artigo 5.º, e diz que apenas devem ser tratados os dados pessoais "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados". Com este princípio pretende-se que "os dados desnecessários para os fins do tratamento não sejam conservados para qualquer eventualidade ou porque podem vir a ser úteis". É dado como entendido que este princípio se encontra materializado numa "obrigação de minimização de dados" no número 2 do artigo 25.º do RGPD[70]. De um modo geral, antes de ser iniciado um tratamento de dados pessoais, o responsável pelo tratamento tem de verificar se não existe outra alternativa que seja "menos intrusiva aos direitos e liberdades fundamentais do titular" dos dados[71].

d) Princípio da Exatidão

Presente na alínea d) do número 1 do artigo 5.º, dispõe que os dados pessoais que sejam alvo de tratamento sejam sempre "exatos e atualizados sempre que necessário" e que "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". Este princípio exterioriza que "o responsável pelo tratamento de dados deve adotar medidas técnicas e organizativas" de modo a "garantir que a fonte dos dados e o método de recolha são fiáveis"[72].

e) Princípio da Limitação da Conservação

Previsto na alínea e) do número 1 do artigo 5.º, determina que os dados pessoais sejam "conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados (...)". A finalidade do tratamento é o critério principal para determinar qual o prazo de conservação dos dados, contudo, existem outros fatores que também devem ser levados em conta na determinação do prazo (por exemplo, o tipo de dados tratados, o fundamento do tratamento)[73]. Portanto, o responsável pelo tratamento deve fixar os

[68] MONIZ, Graça Canto, *Op. Cit.*, p. 107-108.
[69] CORDEIRO, António Barreto Menezes, *Op. Cit.*, p. 155.
[70] MONIZ, Graça Canto, *Op. Cit.*, p. 107-114.
[71] MONIZ, Graça Canto, *Op. Cit.*, p. 106.
[72] MONIZ, Graça Canto, *Op. Cit.*, p. 106.
[73] MONIZ, Graça Canto, *Op. Cit.*, p. 118-120.

prazos para o apagamento ou revisão periódica, de modo a garantir que os dados pessoais sejam mantidos apenas durante o período de tempo necessário[74].

f) Princípio da Integridade e Confidencialidade

Está estipulado na alínea f) do número 1 do artigo 5.º, e indica 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". Conforme o Considerando 39, "os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas". Este princípio está ligado ao artigo 4.º, n.º 12 do RGPD que dispõe que a violação de dados pessoais significa "uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento"[75].

g) Princípio da Responsabilidade

Presente no número 2 do artigo 5.º do RGPD estabelece que "o responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo". Com este princípio, verifica-se uma "espécie de descentralização da proteção dos direitos fundamentais" realizada através da "atribuição de uma quota de responsabilidade às organizações", ou seja, aos responsáveis pelo tratamento, que devem "avaliar os riscos e decidir as medidas mais adequadas para os mitigar" [76].

A concretização principal deste princípio encontra-se no número 1 do artigo 24.º do RGPD, sobre a "responsabilidade do responsável pelo tratamento". De acordo com número 1, "tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares", "o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento", medidas essas que poderão ser revistas e atualizadas se necessário[77].

[74] CORDEIRO, António Barreto Menezes, *Op. Cit.*, p. 160.
[75] MONIZ, Graça Canto, *Op. Cit.*, p. 123.
[76] MONIZ, Graça Canto, *Op. Cit.*, p. 126.
[77] MONIZ, Graça Canto, *Op. Cit.*, p. 128.

3.2. Direitos dos titulares

A vontade do titular dos dados tem uma posição de relevo no RGPD. Neste aspeto, o princípio da participação do titular dos dados no tratamento, não enunciado no artigo 5.º do RGPD, garante a influência do titular dos dados nas operações de tratamento e reflete-se num conjunto de direitos que são assegurados ao titular dos dados[78]. Estes direitos estão previstos no capítulo III do RGPD.

a) Direito de Acesso

O artigo 8.º, n.º 2 da CDFUE dispõe que "todas as pessoas têm o direito a aceder aos dados coligidos que lhe digam respeito". O direito de acesso está consagrado no artigo 15.º do RGPD que determina que "o titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais" e às informações previstas nas alíneas a) a h) do artigo 15.º. O objetivo é que o titular dos dados fique numa posição que lhe permita verificar o tratamento dos seus dados e facilite o exercício de outros direitos[79]. Segundo o Considerando 63 do RGPD, "os titulares dos dados deverão ter o direito de aceder aos dados pessoais recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de tomar conhecimento do tratamento e verificar a sua licitude".

b) Direito à retificação

Relativamente ao direito à retificação, o artigo 8.º, número 2, da CDFUE estabelece que "todas as pessoas têm o direito a aceder aos dados coligidos que lhe digam respeito e de obter a respetiva retificação". Este direito está previsto no artigo 16.º do RGPD e dispõe que "o titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito" e "tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional"[80]. De acordo com o artigo 19.º, "o responsável pelo tratamento comunica a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação (...) dos dados pessoais (...), salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado".

[78] MONIZ, Graça Canto, *Op. Cit.*, p. 169.
[79] MONIZ, Graça Canto, *Op. Cit.*, p. 171.
[80] MONIZ, Graça Canto, *Op. Cit.*, p. 174-175.

c) Direito ao Apagamento (Direito ao Esquecimento)

O direito ao apagamento está consagrado no artigo 17.º do RGPD, com a epígrafe "Direito ao apagamento dos dados" («direito a ser esquecido»). Neste artigo parecem estar consagrados dois direitos diferentes: um direito ao apagamento, em sentido estrito, previsto no n.º 1; e um direito ao esquecimento, consagrado no n.º 2. Em conjunto, formam um direito ao apagamento em sentido amplo[81].

Portanto, o n.º 1 afirma que "o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada" quando se aplica um dos pressupostos previstos nas alíneas que fazem parte deste número 1. Relativamente ao número 2, "quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.º 1, toma as medidas que forem razoáveis (...) para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos". Aqui, o direito ao esquecimento surge do reconhecimento da insuficiência do apagamento dos dados pelo responsável pelo tratamento, em face das "especificidades de Internet" porque o simples facto de apagar determinada informação da internet de um sítio não significa que esta tenha sido apagada de toda a Internet[82].

d) Direito à limitação do tratamento

O direito à limitação do tratamento, previsto no artigo 18.º do RGPD, estabelece que "o titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma das seguintes situações": a) "contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão"; b) "o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização"; c) "o responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial"; e por último, d) "se tiver oposto ao tratamento nos termos do artigo 21.º, n.º 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados".

Consoante o n.º 2 do artigo 18.º, relativamente aos efeitos da limitação do tratamento, todas as operações de tratamento, com a exceção da conservação, apenas podem ocorrer em três situações:

[81] CORDEIRO, António Barreto Menezes, *Op. Cit.*, p. 274.
[82] CORDEIRO, António Barreto Menezes, *Op. Cit.*, p. 275.

"com o consentimento do titular"; "para efeitos de declaração, exercício ou defesa de um direito"; ou por motivos ponderosos de interesse público da União ou de um Estado-Membro". De acordo com o número 3, "o titular que tiver obtido a limitação do tratamento nos termos do n.º 1 é informado pelo responsável pelo tratamento antes de ser anulada a limitação ao referido tratamento".

e) Direito à Portabilidade

O direito à portabilidade dos dados está consagrado no artigo 20.º do RGPD. Nos termos deste artigo, "o titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se": "o tratamento se basear no consentimento dado" nos termos do artigo 6.º/ 1, a) ou 9.º/2, a), ou num contrato referido no artigo 6.º/1, b); e se "o tratamento for realizado por meios automatizados".

Na portabilidade cabem "os mecanismos de transmissão da informação entre diferentes sistemas informáticos e plataformas digitais". Como direito do titular, no âmbito da proteção de dados, a portabilidade tem uma dimensão individual e uma económica. No caso da dimensão individual, a portabilidade gere uma "ferramenta de autogestão do titular para controlar e determinar o destino dos seus dados pessoas", no caso da dimensão económica, tem a ver com a "intenção de facilitar a livre circulação de dados dentro da União Europeia e de estimular a concorrência entre prestadores de serviços"[83].

f) Direito de oposição

O direito de oposição encontra-se no artigo 21.º do RGPD que dispõe que "o titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular". Pode ser exercido em quatro situações: os tratamentos realizados com base no artigo 6.º, n.º 1, alínea e) ou f); a reutilização de dados pessoais de acordo com o artigo 6.º, n.º 4; em tratamentos para fins de comercialização direta; e por fim, nos tratamentos para fins de investigação científica, história ou para fins estatísticos[84]. Nos termos do número 1 do artigo 21.º, "o responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial".

[83] MONIZ, Graça Canto, *Op. Cit.*, p. 188.
[84] MONIZ, Graça Canto, *Op. Cit.*, p. 195.

g) Direito de não estar sujeito a decisões individuais automatizadas

O direito de não estar sujeito a decisões individuais automatizadas previsto no artigo 22.º do RGPD, com a epígrafe "Decisões individuais automatizadas, incluindo definição de perfis" estipula que "o titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar". De acordo com o número 4 do artigo 4.º do RGPD, entende-se a "Definição de perfis" como "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações".

Nas alíneas a), b) e c) do número 2 do artigo 22.º estão previstas as situações em que não se aplica o n.º 1 do artigo 22.º que são: quando a decisão é necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento; quando houver autorização da decisão pelo direito da União ou do Estado-Membro a que o responsável estiver sujeito; e quando a decisão é baseada no consentimento explícito do titular dos dados.

Existe um dever de prestar informação, conforme os artigos 13.º, n.º 2, alínea f) e 14.º, n.º2, alínea g). Sempre que haja decisões automatizadas na aceção do n.º 1 do artigo 22.º, "o responsável pelo tratamento tem de (i) comunicar ao titular que toma esse tipo de decisões; (ii) fornecer informações úteis relativas à lógica subjacente e (iii) explicar a importância e as consequências previstas do tratamento[85]. O que se pretende é que seja fornecido ao titular informação relevante, como "o tipo de dados usados no processo de definição de perfis ou de tomada de decisão", o "modo como é elaborado o perfil" e o "motivo pelo qual é relevante para a decisão automatizada, entre muitos outros aspetos" [86].

3.3. A Lei da Proteção de Dados Pessoais (Lei n.º 58/2019, de 08 de agosto)

A Lei 58/2019, de 8 de agosto assegura a execução, na ordem jurídica nacional, do Regulamento Geral de Proteção de Dados da União Europeia e estabelece as regras para o tratamento de dados pessoais. Nos termos do número 1 do artigo 2.º, esta lei "aplica-se aos tratamentos de dados pessoais realizados no território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante, mesmo que o tratamento de dados pessoais seja

[85] MONIZ, Graça Canto, *Op. Cit.*, p. 201.
[86] MONIZ, Graça Canto, *Op. Cit.*, p. 202.

efetuado em cumprimento de obrigações legais ou no âmbito da prossecução de missões de interesse público, aplicando-se todas as exclusões previstas no artigo 2.º do RGPD".

De acordo com o número 2, esta lei aplica-se também aos "tratamentos de dados pessoais realizados fora do território nacional quando: a) sejam efetuados no âmbito da atividade de um estabelecimento situado no território nacional; ou b) afetem titulares de dados que se encontrem no território nacional, quando as atividades de tratamento estejam subordinadas ao disposto no n.º 2 do artigo 3.º do RGPD; ou c) afetem dados que estejam inscritos nos postos consulares de que sejam titulares portugueses residentes no estrangeiro".

Nos termos do artigo 3.º, a "Comissão Nacional de Proteção de Dados (CNPD) é a autoridade de controlo nacional" e tem como propósito controlar e fiscalizar o cumprimento do RGPD e da presente lei, "bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos de dados pessoais" de acordo com o número 2 do artigo 4.º da Lei 58/2019.

Capítulo II – A Internet das Coisas

1. Introdução

A Internet das Coisas, em inglês, *Internet of things* (IoT), é o termo utilizado para designar os diversos tipos de dispositivos que estão ligados à internet. Trata-se de uma infraestrutura em que milhares de milhões de sensores integrados em dispositivos comuns são criados para registar, tratar, armazenar e transferir dados e, uma vez que estão associados a identificadores únicos, interagir com outros dispositivos ou sistemas que utilizam capacidade de ligação em rede. A IoT está estreitamente ligada às noções de computação "invasiva" e "omnipresente" porque se baseia no princípio do tratamento extensivo de dados através dos sensores que são criados para comunicar e trocar dados de forma contínua[87].

Trata-se de uma tecnologia que está a revolucionar a forma como interagimos com o mundo à nossa volta. As grandes invenções, como a lâmpada, o telemóvel, as câmaras, entre outras, tornaram-se objetos que as pessoas utilizam no seu dia-a-dia e já não vivem sem elas e até ao surgimento das tecnologias digitais conectadas, estas coisas funcionavam independentes umas das outras. Uma lâmpada era apenas uma lâmpada e o telemóvel era simplesmente um telemóvel[88]. A Internet das Coisas veio revolucionar isto, passando a conectar à internet todo o tipo de objetos possíveis. Por exemplo, um telemóvel, uma lâmpada, uma fechadura de uma porta, um frigorífico, entre outros, funcionam como dispositivos IoT, têm componentes IoT ou são essenciais para que a IoT funcione e proporcione valor às pessoas[89]. Segundo LUÍS ANTUNES[90], a Internet das Coisas é a extensão da Internet a um nível subsequente, ou seja, aproximando o mundo digital do mundo físico das coisas e fazendo-os interagir.

A ideia central da IoT é criar uma rede inteligente onde diferentes objetos, desde eletrodomésticos até veículos, possam comunicar entre si, recolher informações em tempo real e, deste modo, proporcionar uma gestão mais automática e eficiente de diversas atividades. Essa interligação entre os objetos possibilita a criação de uma série de aplicações diversas em setores como a saúde, transporte, indústria, agricultura, casas e cidades inteligentes e muitos outros. A capacidade de recolher os dados em tempo real e de automatizar os processos torna-se um modo de facilitar a

[87] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Parecer 8/2014 sobre os recentes desenvolvimento na Internet das Coisas, adotado em 16 de setembro de 2014, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_pt.pdf, p. 4.
[88] GREENGARD, Samuel, The Internet of Things, The MIT Press Essencial Knowledge Series, 2021, p. ix-x.
[89] GREENGARD, Samuel, *Op. Cit.*, p. 14-15.
[90] ANTUNES, Luís Filipe, A Privacidade no Mundo Conectado da Internet das Coisas, *in* Forum de Dados, n.º 2, 2016, p. 54.

tomada de decisões mais informadas e eficientes e à medida que a IoT continua a evoluir, molda-se um futuro onde a conetividade não apenas simplifica as tarefas diárias, como também impulsiona a inovação, criando novas oportunidades e transformando a maneira como vivemos, trabalhamos e nos relacionamos com o mundo digital.

A ideia da IoT e dos dispositivos inteligentes surgiu nos inícios da década de 80 quando os computadores e as redes locais (*Local Area Network* - LAN) começaram a ganhar forma[91]. Foi a criação da internet e da *World Wide Web* que permitiram a partilha de informação entre redes de computador que possibilitaram o surgimento da ideia dos dispositivos inteligentes. Contudo, o termo *Internet of Things* surgiu apenas em 1999 por Kevin Ashton, um britânico pioneiro em tecnologia, considerado o pai da Internet das Coisas. Kevin Ashton utilizou tecnologia de identificação por radiofrequência (*Radio Frequency Identification* – RFID) para ligar diversos dispositivos e objetos[92].

À medida que a internet se tornou mais acessível e rápida, a possibilidade de conectar mais coisas além de computadores tornou-se real. Em 2008, o tema da Internet das Coisas foi formalmente reconhecido e discutido internacionalmente durante a realização da primeira conferência sobre o tema na Suíça, a "*First International Conference*, IOT 2008". Nessa conferência, foram discutidos temas como RFID, sensores, tecnologias de conexão e conversão de protocolos[93]. Nos últimos anos, a IoT explodiu em popularidade. Graças ao desenvolvimento de tecnologias de comunicação como o 5G e à análise de dados com recurso à IA e à aprendizagem automática, a IoT tem aplicações que vão desde os dispositivos de consumo, como relógios inteligentes, às infraestruturas urbanas (cidades inteligentes)[94].

No futuro, podemos esperar ainda mais integração, automatização e inovação, abrindo caminho para um futuro cada vez mais conectado e inteligente. De acordo com o *site Statistica,* prevê-se que o número de dispositivos da Internet das Coisas a nível mundial quase duplique, passando de 15,1 mil milhões em 2020 para mais de 29 mil milhões de dispositivos da IoT em 2030. Em 2030, o maior número de dispositivos da IoT encontrar-se-á na China, com cerca de 8 mil milhões de dispositivos de consumo. Os dispositivos de consumo representam cerca de 60% de todos os tipos de

[91] GREENGARD, Samuel, *Op. Cit.*, p. 9.
[92] GREENGARD, Samuel, *Op. Cit.*, p. 9.
[93] FILHO, Mauro Faccioni, Internet das Coisas, UnisulVirtual, 2016, disponível em https://www.researchgate.net/publication/319881659_Internet_das_Coisas_Internet_of_Things, p. 12.
[94] *In* https://www.statista.com/topics/2637/internet-of-things/#topicOverview

dispositivos ligados à IoT em 2020. Prevê-se que esta percentagem se mantenha a este nível nos próximos dez anos[95].

2. Como funciona a Internet das Coisas

À medida que os sensores, microchips e capacidades de análise de dados se tornam mais sofisticados, há uma capacidade crescente para observar ambientes e compreender as relações complexas entre os objetos e seres vivos. Os sistemas da IoT estão a redefinir radicalmente a forma como as máquinas interagem com o mundo à nossa volta e como os humanos interagem entre si. Existe muita coisa envolvida na ligação de todas estas "coisas" e na manutenção de ligações fiáveis e consistentes[96].

A conexão com a internet é o que está no centro da tecnologia da IoT ao permitir a transferência de dados de um dispositivo e sistema para outro, através de tecnologias como Wi-Fi, Bluetooth, redes móveis celulares como o 4G ou 5G, comunicação por campo de proximidade – (*Near Field Communication* – NFC), identificação por radiofrequência (*Radio Frequency Identification* – RFID), entre outros[97].

São os sensores que permitem que os dispositivos IoT capturem e processem dados do ambiente à sua volta. Esses sensores são os olhos, orelhas, nariz e dedos da IoT. Atualmente existem milhares de tipos de sensores diferentes que detetam luz, som, temperatura, campos magnéticos, humidade, movimento, químicos, entre muito mais.[98] E a contínua evolução destes sensores permitirá que os investigadores consigam criar dispositivos que consigam cheirar, provar ou realizar outras funções humanas[99]. À medida que a IoT evolui, o mesmo acontece com os conjuntos de *chips* utilizados nos sensores, dispositivos e máquinas. Os *microchips* estão cada vez mais otimizados para funções específicas da IoT, possibilitando maximizar a conetividade[100].

A computação em nuvem desenvolveu um conjunto de infraestruturas sofisticadas para armazenamento, envio de mensagens, segurança e conetividade. Tornou possível processar, encaminhar e sincronizar dados de forma muito mais eficiente. Seria virtualmente impossível para qualquer organização ou governo criar uma infraestrutura de armazenamento de dados capaz de suportar a IoT. As nuvens são, portanto, essenciais para a IoT porque, entre outras coisas,

[95] *In* https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
[96] GREENGARD, Samuel, *Op. Cit.*, p. 53.
[97] GREENGARD, Samuel, *Op. Cit.*, p. 61-63.
[98] GREENGARD, Samuel, *Op. Cit.*, p. 65.
[99] GREENGARD, Samuel, *Op. Cit.*, p. 68.
[100] GREENGARD, Samuel, *Op. Cit.*, p. 69.

proporcionam um ambiente altamente escalável para o armazenamento de dados pois, um grande número de dispositivos ligados gera enormes volumes de dados[101].

Na IoT, os transdutores[102] podem gerar dados, os microchips podem processá-los e as nuvens podem mover todos os dados, mas os atuadores[103] são essenciais para ler os dados dos sensores e fazer com que as coisas aconteçam. Exemplos de atuadores são os sistemas de segurança, as fechaduras de portas conectadas e os motores elétricos. Vários sensores presentes num dispositivo ou rede fornecem os dados que iniciam o evento físico desejado, seja o acompanhamento de movimento por câmara ou uma porta a se trancar[104].

A cooperação entre IoT e a aprendizagem automática (AA) aumenta ainda mais o potencial da tecnologia. A aprendizagem automática possibilita que os sistemas tenham a capacidade de aprender automaticamente e melhorarem a partir de experiências passadas sem a necessidade de serem previamente programadas[105]. A inteligência artificial assume, então, um papel importante para a IoT e tem sido cada vez mais utilizada na tomada de decisões diante de grandes volumes de dados. Como a IoT gera uma enorme quantidade de dados, o *Big Data* foi um dos seus grandes impulsionadores processando e analisando estes dados recolhidos pelos dispositivos IoT[106]. O *Big Data* trata-se da prática de combinar enormes volumes de informação proveniente de diferentes fontes e que podem ser analisados recorrendo à IA através da aprendizagem automática. Ou seja, utiliza técnicas de IA para extrair valores de grandes conjuntos de dados. Do *Big Data* resulta como benefícios a monitorização do comportamento humano, coletiva ou individualmente, e o seu potencial preditivo[107].

A recolha contínua de dados permite a obtenção de informações importantes sobre o desempenho e o comportamento dos dispositivos IoT. A análise desses dados possibilita a tomada de decisões mais informadas, o que pode resultar em melhorias na eficiência operacional e na otimização de processos. E a interação humana é fundamental para compreender as necessidades e expectativas dos utilizadores. A personalização de soluções IoT com base no *feedback* humano pode melhorar significativamente a experiência do utilizador, resultando em produtos e serviços mais adaptados às

[101] GREENGARD, Samuel, *Op. Cit.*, p. 73-74.
[102] Transdutor é um dispositivo utilizado em conversão de energia de uma natureza para outra.
[103] Atuador é um dispositivo que produz movimento.
[104] GREENGARD, Samuel, *Op. Cit.*, p. 79-80.
[105] KAUR, Jashanpreet, Safeguarding privacy in internet of things, Mohd Abdul Hafi, 2022, p. 34.
[106] KHARE, Shivanjali; TOTARO, Michael, Big Data in IoT, 2019, disponível em https://ieeexplore.ieee.org/abstract/document/8944495, p.1.
[107] BUTTARELLI, Giovanni, Inteligência Artificial, Robótica, Privacidade e Proteção de Dados, Forum de Dados, n.º 4, 2017, p. 28.

preferências individuais. As informações de origem humana são importantes para muitas aplicações da IoT[108].

3. Os dispositivos de consumo da Internet das Coisas

Por dispositivos de consumo compreende-se os diversos produtos eletrónicos criados para uso pessoal e doméstico. É fácil verificar nos dias de hoje o quão dependentes estamos destes produtos eletrónicos. Atualmente, nos EUA, uma casa típica contém cerca de 70 aparelhos eletrónicos, que vão desde fornos, máquinas de lavar roupa e loiça, computadores, impressoras, aspiradores, torradeiras, entre muitos outros[109]. A introdução de dispositivos eletrónicos – e, nos últimos anos, das poderosas capacidades computacionais incorporadas nesses dispositivos – alterou profundamente a forma como vemos televisão, comunicamos, compramos produtos, recolhemos informações e realizamos uma série de outras tarefas[110]. A Internet das Coisas trouxe uma revolução aos dispositivos de consumo, transformando objetos comuns em inteligentes e ligados à internet.

Os dispositivos de consumo da IoT podem ser separados em quatro grupos: os de tecnologia IoT estabelecida, as tendências atuais, as tendências emergentes e, por fim, os dispositivos IoT de nicho. O primeiro grupo refere-se aos dispositivos e sistemas que já estão totalmente conectados como *smartphones*; *wearables* e as *smart TVs.* O segundo grupo, das tendências atuais, representa os assistentes digitais, colunas inteligentes, robôs e sistemas de gestão de energia, como termóstatos inteligentes. O terceiro grupo, das tendências emergentes, integra dispositivos conectados que estão a ganhar força, como a iluminação inteligente, a segurança e os eletrodomésticos inteligentes. O último grupo inclui coisas como sistemas de carregamento de veículos elétricos e controladores e sistemas de jardinagem conectados, por exemplo[111].

Os assistentes virtuais são uma categoria proeminente na IoT, com dispositivos como *Amazon Echo* e *Google Home* tornando-se presença comum nas casas. São programas de inteligência artificial projetados para interagir com os utilizadores através, principalmente, de interfaces de voz, compreendendo linguagem natural e realizando tarefas variadas com base em comandos verbais[112]. Os assistentes virtuais tornam-se os facilitadores da interação humana com a vasta rede de dispositivos de consumo da IoT. Os *Smart Home Personal Assistants* (SPA) tem um ecossistema complexo que os

[108] TURUNEN, Markku, *et al*, Interaction and Humans in Internet of Things, 2015, disponível em https://www.researchgate.net/publication/281643568_Interaction_and_Humans_in_Internet_of_Things, p. 634.
[109] GREENGARD, Samuel, *Op. Cit.*, p. 97.
[110] GREENGARD, Samuel, *Op. Cit.*, p. 98.
[111] GREENGARD, Samuel, *Op. Cit.*, p. 100-101.
[112] SILVA, Diana; MALTA, Mariana; VASCONCELOS, Paulo, Desafios da Privacidade nos Assistentes Virtuais Pessoais, 2022, disponível em https://www.iscap.pt/ebusiness-rj/index.php/mne-rj/article/view/194, p.4.

permite realizar várias tarefas pedidas pelo utilizador apenas por comando de voz, tarefas como comprar bens e comida, fornecer informações, reproduzir música, mandar mensagens, controlar outros dispositivos inteligentes e muito mais[113].

Os dispositivos de consumo da IoT abrangem uma vasta gama de produtos, proporcionando praticidade, eficiência e uma experiência mais conectada para os utilizadores. Vamos explorar alguns dos dispositivos de consumo mais notáveis da IoT:

3.1. Casas Inteligentes

Um dos setores que tem sido mais afetado pela IoT é o da automação residencial ou domótica. Atualmente, os dispositivos IoT podem ser colocados em residências; dispositivos como lâmpadas, fechaduras, termóstatos, detetores de fumo, máquinas de lavar ou fornos "conectados" podem ser controlados à distância pela internet ou por meio de *smartphones* ou de assistentes virtuais. A atração por uma casa automatizada é a promessa de uma maior comodidade, de segurança melhorada e de sistemas energeticamente mais eficientes[114]. Por exemplo, os dispositivos que contêm sensores de movimento podem detetar quando um indivíduo está em casa e registar quais são os seus padrões de movimento e talvez desencadear ações específicas previamente identificadas (por exemplo, ligar uma luz ou alterar a temperatura da divisão)[115].

Numa casa inteligente incorporam-se diversos dispositivos de segurança como câmaras de segurança ligadas à internet que permitem que os utilizadores monitorizem de forma remota a sua casa. Os sistemas de segurança inteligentes e os dispositivos de monitorização, como a *Amazon Ring doorbell*, tornaram-se bastante populares[116]. As câmaras de segurança doméstica e os sistemas de segurança ligados à internet oferecem funcionalidades de monitorização à distância, de os ligar ou desligar de forma remota, e muitos destes sistemas podem enviar uma notificação ou um alerta de texto quando o sistema deteta algum movimento ou um evento que não corresponde a regras predefinidas. No futuro, estes sistemas de segurança poderão reconhecer os habitantes através de *tokens* de autorização permanentes ou temporários num smartphone ou num microchip incorporado no corpo, utilizando simultaneamente o reconhecimento facial e outros sensores para determinar quando alguém entrou sem autorização[117].

[113] ABDI, Noura, *et al*, Privacy Norms for Smart Home Personal Assistants, 2021, disponível em https://dl.acm.org/doi/abs/10.1145/3411764.3445122, p.1
[114] GREENGARD, Samuel, *Op. Cit.*, p. 112.
[115] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Parecer 8/2014, *Op. Cit.*, p. 7.
[116] GREENGARD, Samuel, *Op. Cit.*, p. 113.
[117] GREENGARD, Samuel, *Op. Cit.*, p. 115.

Outros dispositivos são os de gestão de energia como termóstatos inteligentes, - da *Nest Thermostat* ou *Ecobee*, por exemplo – que permitem o controlo remoto da temperatura e ajustam automaticamente a temperatura com base nos padrões de uso e preferências do utilizador de modo a otimizar a eficiência energética, permitindo reduzir as contas de eletricidade em cerca de 23%. Os sistemas de iluminação inteligente, como lâmpadas e interruptores inteligentes possibilitam o controlo remoto da iluminação, bem como a programação para poupar energia. No futuro, os sistemas de gestão de energia – com sensores integrados espalhados por toda a casa – aprenderão os padrões de movimento e de vida dos ocupantes, bem como as características únicas da casa. Utilizando a aprendizagem automática, ajustarão automaticamente os seus algoritmos e adaptar-se-ão às mudanças sazonais e a outras mudanças[118].

As lâmpadas inteligentes (da *Philips Hue*, por exemplo) oferecem a conveniência de ajustar a intensidade da luz com apenas o toque de um botão, entre muitas outras funcionalidades. Com a Alexa ou *HomeKit*, o proprietário pode definir horários para luzes e outros dispositivos, fazer com que as lâmpadas se acendam à entrada ou à saída e podem comandar todos os dispositivos à distância[119].

Uma das áreas mais importantes para a IoT e automatização da casa é a cozinha. Por exemplo, o micro-ondas da *AmazonBasics* responde a simples comandos de voz. O frigorífico da *Samsung Family Hub* contém um ecrã interativo que permite os utilizadores aceder a receitas, aplicações, notas, etc. O *Instant Pot Smart Wi-Fi* responde aos comandos via uma aplicação de *smartphone*. O *KitchenAid Smart Oven+* permite controlar o forno à distância, mas também inclui sensores ligados que interagem com um smartphone e respondem a comandos de voz através da Alexa ou do Assistente da Google. Nos próximos anos, a variedade de botões, teclados e controlos presentes nos aparelhos acabará por desaparecer e passará a ser tudo por comandos de voz, que com o desenvolvimento da IA, o vocabulário e as capacidades continuarão a aumentar[120].

3.2. Dispositivos de entretenimento

O setor do entretenimento tem presenciado avanços significativos graças à Internet das Coisas. Os *smartphones,* cuja utilização já vem de alguns anos, desempenham um papel central ao desbloquear o potencial da IoT, pois fornecem a interface mais avançada (e a porta de entrada para alguns dispositivos) para aceder, gerir e controlar as nossas coisas[121]. Conectando-se constantemente e

[118] GREENGARD, Samuel, *Op. Cit.*, p. 113.
[119] GREENGARD, Samuel, *Op. Cit.*, p. 114.
[120] GREENGARD, Samuel, *Op. Cit.*, p. 114-115.
[121] CORCORAN, Peter, *Op. Cit.*, p. 66.

oferecendo poder de processamento, os *smartphones* têm também um papel crucial na recolha e monitorização de dados gerados pelos dispositivos IoT.

As atuais Smart TVs vão muito além da simples transmissão de conteúdo. Estas televisões inteligentes "são o cruzamento das televisões clássicas com um computador e estão cada vez mais omnipresentes", "oferecem um número cada vez maior de recursos, tais como, acesso à internet, *apps*, câmaras e microfones embutidos"[122] e interagem com outros dispositivos em casa. Os *smart speaker*s ou sistemas de áudio inteligentes, como colunas inteligentes com assistentes virtuais, desempenham um papel crucial na gestão do entretenimento em casa. São dispositivos móveis controlados por voz que utilizam a inteligência artificial e o processamento de linguagem natural para facilitar uma variedade de tarefas[123], como reproduzir listas de reprodução, ajustar o volume, obter informações sobre artistas, sobre a previsão do tempo[124] e controlar outros dispositivos conectados, proporcionando uma experiência de entretenimento mais fluida e intuitiva.

A internet das coisas transformou também a indústria dos jogos, destacando-se especialmente a introdução dos dispositivos de realidade virtual (RV) e realidade aumentada (RA). A colocação de sensores de movimento e de dispositivos de vestir possibilitou melhorar a experiência de jogo, tornando-se mais interativo e permitindo que os jogadores interajam não apenas entre si, mas também com o ambiente virtual em tempo real.[125] Existem também brinquedos inteligentes como bonecos e robôs inteligentes. Estes brinquedos interativos destinados às crianças respondem à sua voz e conversam com elas[126].

3.3. *Wearables* e dispositivos de saúde inteligentes

Os *Wearables* ou computação vestível refere-se a vestuário, como relógios, óculos, sapatos, anéis, por exemplo, que inclui sensores destinados a ampliar as suas funcionalidades. Os dispositivos de saúde inteligentes são dispositivos tecnológicos que são utilizados no corpo e que se tornaram indispensáveis para muitas pessoas[127]. Estes dispositivos não apenas monitoram a saúde e a condição física, mas também fornecem notificações imediatas e facilitam o acesso a informações importantes. Este tipo de dispositivos pode incorporar microfones, câmaras e sensores que podem gravar e transferir

[122] ANTUNES, Luís Filipe, *Op. Cit.*, p. 57.
[123] LUTZ, Christoph; NEWLANDS, Gemma, Privacy and smart speakers: A multi-dimensional approach, the information society, vol. 37, 147–162, 2021, disponível em https://www.tandfonline.com/doi/full/10.1080/01972243.2021.1897914, p.147.
[124] DUBOIS, Daniel J., *et al*, When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers, Proceedings on Privacy Enhancing Technologies, vol 4, 255–276, 2020 disponível em https://par.nsf.gov/biblio/10192512, p.255.
[125] *In* https://www.wearedevelopers.com/magazine/how-the-internet-of-things-impacts-game-development
[126] Grupo de trabalho internacional sobre a proteção de dados nas telecomunicações, Dispositivos inteligentes para crianças e os riscos para a privacidade, Fórum da Proteção de Dados, n.°6, 2019, p.40.
[127] SPENDER, A.; BULLEN, L., *et al*, Wearables and the internet of things: considerations for the life and health insurance industry, in British Actuarial Journal, vol. 24, 2019, disponível em https://www.cambridge.org/core/journals/british-actuarial-journal/article/wearables-and-the-internet-of-things-considerations-for-the-life-and-health-insurance-industry/56919A6812F5439BD4C49AC758C7CE63, p. 3.

dados para o fabricante de dispositivos, além disso, a disponibilidade de uma Interface de Programação de Aplicações (API – *Application Programming Interface*[128]) para dispositivos vestíveis desenvolve a criação de aplicações por terceiros que podem, deste modo, adquirir acesso aos dados recolhidos por esses dispositivos[129].

Os relógios inteligentes e as pulseiras fitness permitem contar os passos e distância percorrida e monitorizar a atividade física[130], têm sensores que permitem também medir a frequência cardíaca e rastrear os padrões de sono. Oferecem informações aos utilizadores sobre a sua saúde em tempo real. Por exemplo, o *Apple Watch* não só inclui um sofisticado monitor de atividade que regista os passos, a distância e o exercício, como também inclui um eletrocardiograma (ECG) de qualidade médica que permitiu que inúmeras pessoas descobrissem que tinham problemas cardíacos. Consegue também detetar quedas e chamar os serviços de emergência, medir os níveis de oxigénio no sangue, ajudar a acompanhar os ciclos menstruais e alertar os utilizadores quando expostos a níveis sonoros que podem prejudicar a sua audição.[131]

Os dispositivos médicos conectados também estão a tornar-se cada vez mais comuns. Dispositivos como monitores de glicose, medidores de pressão arterial, termómetros, balanças corporais, oxímetros e muito mais ligados por Bluetooth permitindo visualizar os dados por meio de uma aplicação num *smartphone* ou num *smartwatch*[132] e enviar esses dados diretamente a profissionais de saúde, de modo a apoiar o diagnóstico ou a monitorização de condições específicas dos pacientes e assim, possibilitando um acompanhamento mais preciso e eficaz[133].

3.4. Veículos inteligentes

A IoT tem modificado a forma como criamos e utilizamos os nossos veículos. Sistemas de navegação e computadores de bordo ligados a *smartphones* contêm inúmeras funções, incluindo a monitorização do nível de óleo e da pressão dos pneus, a introdução de um endereço no sistema de navegação e até mesmo o fecho e abertura de portas. Esses sistemas utilizam o comando de voz para combinar a funcionalidade do telemóvel e do veículo com a Internet. Um número crescente de veículos também suporta redes Wi-Fi móveis e várias funcionalidades que combinam a condução com a informática. Estas incluem a travagem automática, os avisos de saída da faixa de rodagem, ecrãs que

[128] Uma API consiste num conjunto de regras ou protocolos que permite às aplicações de software comunicar entre si para trocar dados, características e funcionalidades. https://www.ibm.com/topics/api.
[129] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Parecer 8/2014, *Op. Cit.*, p. 6.
[130] GREENGARD, Samuel, *Op. Cit.*, p. 115.
[131] GREENGARD, Samuel, *Op. Cit.*, p. 116.
[132] GREENGARD, Samuel, *Op. Cit.*, p. 116-117.
[133] SPENDER, A.; BULLEN, L., et al *Op. Cit.*, p. 3.

mostram dados e as funcionalidades de estacionamento automático que dependem de uma variedade de sensores[134].

Os sensores, câmaras e radares recolhem dados em tempo real para permitir funções como assistência ao estacionamento e, eventualmente, condução autónoma total. Os seus sistemas automatizados eliminarão a necessidade de estacionar manualmente um automóvel. Um motorista sairia do carro numa zona de carga/descarga de passageiros num aeroporto, num restaurante ou num centro comercial e o carro estacionaria automaticamente e voltaria ao passageiro quando lhe fosse ordenado[135].

Além disto, estes sensores nos carros inteligentes monitorizam o desempenho dos componentes, permitindo a identificação antecipada de problemas mecânicos, o que possibilita uma manutenção preventiva. No futuro, os veículos inteligentes lerão semáforos, os sinais de trânsito e navegarão pelas estradas utilizando sensores, satélites e dados da internet. Possivelmente através da utilização de *chips* de IA de ponta especializados, os automóveis aprenderão à medida que avançam e adaptar-se-ão ao seu ambiente e ao condutor e partilharão dados com outros veículos através da nuvem e da IoT[136].

[134] GREENGARD, Samuel, *Op. Cit.*, p. 122.
[135] GREENGARD, Samuel, *Op. Cit.*, p. 124-125.
[136] GREENGARD, Samuel, *Op. Cit.*, p. 123-124.

Capítulo III – Problemas dos dispositivos de consumo da IoT

Apesar dos muitos benefícios que nos trazem os dispositivos de consumo da Internet das Coisas, podem também trazer diversos danos, materiais e imateriais, sobre interesses juridicamente protegidos, pois à medida que a internet e estes dispositivos se tornam mais interligados, os riscos e perigos aumentam[137].

A incapacidade de gerir as complexidades da IoT gera uma grande inquietação, o que leva os legisladores a esforçarem-se por encontrar novas formas de resolver questões de privacidade, segurança e outros problemas decorrentes[138]. Portanto, a recolha alargada e omnipresente de dados, os algoritmos preditivos, a conetividade à internet e a opacidade geral da funcionalidade dos dispositivos ameaçam comprometer os benefícios da IoT, causando potenciais prejuízos aos consumidores[139]. Além disto, como as tecnologias IoT assentam em tecnologias em constante evolução, - big data, inteligência artificial e computação em nuvem – e com a implementação das redes móveis 5G[140], multiplicam-se os desafios para garantir a privacidade e salvaguardar a segurança.

1. Problemas de privacidade

A enorme recolha de dados pessoais pelos dispositivos de consumo da IoT tem criado sérias preocupações sobre a privacidade dos utilizadores. O esperável é que os dados recolhidos sirvam para beneficiar o proprietário do dispositivo, mas acabam por beneficiar também o fabricante ou o fornecedor do dispositivo. A recolha e utilização dos dados provenientes dos dispositivos torna-se uma questão de privacidade quando os indivíduos que são observados por esses dispositivos têm expetativas de privacidade diferentes, em relação ao âmbito e à utilização desses dados, de quem recolhe os dados[141].

---

[137] GREENGARD, Samuel, *Op. Cit.*, p. 171.

[138] CHIKE, Patrick Chike, The Legal Challenges of Internet of Things, 2017, disponível em https://www.researchgate.net/publication/322628457_The_Legal_Challenges_of_Internet_of_Things, p. 3.

[139] TSCHIDER, Charlotthe A., Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age, Denver Law Review, vol. 96, 2018, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3129557# , p.89.

[140] O 5G é a quinta geração de tecnologia de comunicação móvel, que sucede ao 4G e promete oferecer velocidades de internet significativamente mais rápidas, maior largura de banda e menor latência em comparação com as gerações anteriores. O 5G oferece vantagens importantes para a IoT devido à sua capacidade de suportar um número muito maior de dispositivos conectados simultaneamente, a capacidade de suportar taxas de dados mais elevadas e apresentar maior fiabilidade. Com o 5G, espera-se que a IoT se expanda ainda mais, permitindo a criação de redes mais densas e sofisticadas de dispositivos interconectados. Contudo, com estes avanços surgem desafios significativos em termos de privacidade e segurança. RIZOU, Stavroula, et al, GDPR interference with next generation 5G and IoT networks, IEEE Access, vol. 8, 2020, disponível em https://ieeexplore.ieee.org/document/9110555, p. 3.

[141] INTERNET SOCIETY, "The Internet of Things: An Overview. Understanding the issues and Challenges of a More Connecter World", 2015, disponível em https://www.semanticscholar.org/paper/THE-INTERNET-OF-THINGS-%3A-AN-OVERVIEW-Understanding-Rose-Eldridge/be5012a06734594bf3d06a0563c9c7619e5d906e, p.26.

As violações de dados ocorrem constantemente e o "derrame" de informações privadas traz enormes consequências para os indivíduos[142]. A complexidade da IoT e dos dados que nela residem mostra que há muitos pontos possíveis por onde os dados podem "derramar" ou "vazar". Os riscos envolvem a exposição pública indesejada de informações ou imagens e a incapacidade de saber para onde vão os dados ou como é que estão a ser usados ou abusados. À medida que a variedade, volume e velocidade dos dados aumentam, alimentados por novas fontes de dados provenientes de máquinas, sensores, câmaras, sistemas de armazenamento e de processamento de dados, os riscos de negligência ou abuso aumentam[143].

Os dispositivos de consumo da IoT e as aplicações e serviços conectados observam e recolhem muitos tipos de dados sobre nós, incluindo dados biométricos e relacionados com a saúde[144]. Os *wearables* permitem às organizações obter informações importantes e dados em tempo real sobre o nosso bem-estar físico, mental e emocional[145]. Uma pessoa que utilize um *smartwatch* que monitorize o seu movimento, o ritmo cardíaco ou outros fatores pode, com o algoritmo certo, detetar sinais de algum problema de saúde. Embora os dados transmitidos a partir de um dispositivo em específico possam parecer inofensivos e representar pouca ou nenhuma preocupação em termos de privacidade, os dados quando recolhidos a partir de vários pontos e fontes podem acabar por fornecer informações relevantes e sensíveis sobre uma pessoa[146]. Sendo assim, quando os fluxos de dados individuais são combinados ou relacionados com outros, é frequentemente criado um retrato digital mais invasivo do indivíduo do que aquele que é obtido a partir de um único fluxo de dados IoT[147].

A grande quantidade de informações recolhidas pelos dispositivos de consumo ligados entre si podem ser combinadas, analisadas e utilizadas, potencialmente sem a devida transparência, responsabilidade, segurança ou consentimento significativo[148]. A análise de *Big Data* aplicada a dados pessoais representa um risco de invasão de privacidade e esse risco é ampliado no caso da Internet das Coisas devido à maior escala da recolha de dados pessoais. A IoT exige *Big Data* e cria *Big Data*. Os dispositivos estão sempre ligados à internet e a criação de dados em tempo real requer

---

[142] A ameaça mais prevalecente para a privacidade trata-se da identificação, que envolve a associação de informações pessoais, como o nome e endereço, entre outros dados pessoais, ao utilizador. Este processo pode levar a outras ameaças, como o rastreamento e a criação de perfis. O utilizador pode ser identificado principalmente por reconhecimento de voz, impressões digitais ou câmaras de vigilância. Essa identificação pode ser utilizada para invadir a privacidade do utilizador. KARALE, Ashwin, The challenges of IoT addressing security, ethics, privacy, and laws, Internet of Things, vol. 15, 2021, disponível em https://www.sciencedirect.com/science/article/pii/S2542660521000640, p. 9.

[143] GREENGARD, Samuel, *Op. Cit.*, p. 191-192.

[144] ELVY, Stacy-Ann, Privacy and Security in the Connected Era, A Commercial Law of Privacy and Security for the Internet of Things, disponível em https://doi.org/10.1017/9781108699235.002, p.25.

[145] ELVY, Stacy-Ann, *Op. Cit.*, p. 37-38.

[146] GREENGARD, Samuel, *Op. Cit.*, p. 193.

[147] INTERNET SOCIETY, *Op. Cit.*, p.26.

[148] OFFICE OF THE PRIVACY COMMISION OF CANADA, The internet of things, An introduction to privacy issues with a focus on the retail and home environments, 2016, disponível em https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/iot_201602/, p. 16

armazenamento e análise. As análises de dados realizadas por *Big Data* melhoram a funcionalidade dos dispositivos de consumo e identificam as atualizações ou alterações necessárias para que os dispositivos sejam mais eficazes ou eficientes[149]. Além de que, os dispositivos conseguem assim recolher mais facilmente informações sobre as pessoas com um grau de especificidade e abrangência sem precedentes. Todavia, a agregação e a correlação desses dados podem criar perfis pormenorizados de indivíduos[150] que podem potenciar a discriminação ou outros danos. A sofisticação dessa tecnologia pode criar situações que expõem o indivíduo a danos financeiros, físicos, criminais ou de reputação[151].

Os dados dos dispositivos de consumo da IoT permitem às empresas recolher informações pormenorizadas sobre o nosso comportamento e podem transformar-nos em produtos e recursos empresariais[152]. Quando sensores ou câmaras estão omnipresentes e os dados que recolhem são transmitidos, torna-se possível identificar onde uma pessoa se encontra e o que está a fazer em determinado momento e, à medida que os avanços da computação e os algoritmos melhoram, os sistemas tornar-se-ão melhores a decifrar e a antecipar comportamentos[153]. Os fabricantes conseguem combinar dados criados pela IoT com outras informações dos utilizadores como por exemplo, os hábitos de compra, histórico de navegação na internet, entre outros comportamentos. E podem vender ou transferir esses dados para terceiros, podendo este tipo de dados revelarem-se muito lucrativos tanto para os fabricantes que vendem os dados como para as organizações que compram e utilizam esses dados para diferentes finalidades. Mesmo que as organizações utilizem programas de anonimização ou de desidentificação, quantos mais dados forem recolhidos maior é a probabilidade das informações privados e pessoais dos indivíduos serem expostas[154].

Existem normas sociais e expetativas de privacidade que diferem entre espaços públicos e espaços privados, e os dispositivos de consumo desafiam essas normas. Os dispositivos como as câmaras de segurança inteligentes, que normalmente funcionam em espaços públicos, estão a deslocar-se para espaços tradicionalmente privados, como a casa ou automóvel, nos quais as nossas expetativas de privacidade são muito diferentes[155]. Ao trazer estes dispositivos para as nossas casas, os

[149] TSCHIDER, Charlotthe A. *Op. Cit.*, 95.
[150] A definição de perfis envolve a recolha de informações sobre as atividade de um utilizador ao longo do tempo e a personalização da sua experiência online com base nesses dados. Tem sido bastante utilizada na internet para pesquisa, publicidade e comércio eletrónico. A definição de perfis acompanha as ações do utilizador através de cookies do navegador, a maior parte das vezes sem o seu consentimento explícito, o que leva a publicidade não solicitada. KARALE, Ashwin, *Op. Cit.*, p. 10.
[151] INTERNET SOCIETY, *Op. Cit.*, p.28.
[152] ELVY, Stacy-Ann, *Op. Cit.*, p. 28.
[153] GREENGARD, Samuel, *Op. Cit.*, p. 193.
[154] TSCHIDER, Charlotthe A. *Op. Cit.*, 95-96.
[155] INTERNET SOCIETY, *Op. Cit.*, p.27-28.

seus fabricantes e outros terceiros podem potencialmente aceder aos nossos dados domésticos, colocando simultaneamente as informações dos restantes membros da casa em risco[156]. As televisões inteligentes têm incorporadas programas de *software* e serviços interativos que permitem às empresas de tecnologia e aos fabricantes recolher dados sobre quase tudo o que é mostrado nas nossas *Smart TVs*, bem como os dados sobre outros dispositivos ligados a este tipo de televisões[157].

Em certas situações, o utilizador acaba por não estar ciente que um dispositivo está a recolher dados e a partilhá-los com terceiros. Este tipo de recolha de dados está a tornar-se cada vez mais comum nos dispositivos de consumo, como nas televisões inteligentes e dispositivos de videojogos. Estes produtos contêm também reconhecimento de voz ou funcionalidades de visão que os permite ouvir continuamente conversas ou observar a atividade numa sala e transmitir de forma seletiva estes dados a um serviço de nuvem para processamento, que por vezes inclui terceiros. As pessoas podem estar na presença deste tipo de dispositivos sem saberem que a sua conversa ou atividade está a ser observada e os seus dados recolhidos[158]. Os dispositivos domésticos inteligentes e as aplicações relacionadas com eles transmitem informações aos seus fabricantes e não é totalmente claro como é que os fabricantes tencionam utilizá-las e com quem podem ser partilhadas[159].

As nossas fotografias, gravações de voz e vídeos podem ser utilizadas para criar impressões de voz e de rosto que podem ser posteriormente usados para nos identificar ou até permitir que terceiros consigam distorcer informações sobre nós em seu benefício e se apropriem da nossa imagem, semelhança e identidade com mais facilidade. Os dados biométricos que os dispositivos de consumo da IoT recolhem, combinados com a tecnologia de aprendizagem automática, podem ser utilizados para criar *deepfakes* credíveis[160].

1.1. O Consentimento

O consentimento do titular, enquanto base jurídica para o tratamento lícito, é uma das formas mais comuns de efetuar, na prática, o tratamento de dados pessoais e é uma das obrigações do responsável pelo tratamento provar esse consentimento[161]. Contudo, os dispositivos de consumo da IoT complicam o consentimento. Em muitas situações, um indivíduo pode não ter conhecimento do tratamento de dados. E esta falta de informação trata-se de um obstáculo significativo à manifestação

[156] ELVY, Stacy-Ann, *Op. Cit.*, p. 30.
[157] ELVY, Stacy-Ann, *Op. Cit.*, p. 36.
[158] INTERNET SOCIETY, *Op. Cit.*, p.26-27.
[159] OFFICE OF THE PRIVACY COMMISION OF CANADA, *Op. Cit.*, p. 20.
[160] ELVY, Stacy-Ann, *Op. Cit.*, p. 38.
[161] RIZOU, Stavroula, et al, GDPR interference with next generation 5G and IoT networks, IEEE Access, vol. 8, 2020, disponível em https://ieeexplore.ieee.org/document/9110555, p. 3.

de consentimento válido, uma vez que o titular dos dados tem que estar informado. Além disto, em algumas situações, a possibilidade de renunciar a determinados serviços ou funcionalidades de um dispositivo é mais um conceito teórico do que uma alternativa real. Isto conduz à dúvida de saber se o consentimento dado pelo utilizador pode ser considerado como um consentimento livre[162]. Fica em causa a verdadeira liberdade de escolha e capacidade individual e, em vez disso, é feita uma escolha imposta de uma forma objetiva.

Os mecanismos clássicos utilizados para obter o consentimento dos indivíduos podem ser difíceis de aplicar no contexto da Internet das Coisas, resultando num consentimento de "baixa qualidade" que se baseia na falta de informação ou na impossibilidade factual de conceder um consentimento ajustado em conformidade com as preferências expressas dos indivíduos[163]. Os fabricantes normalmente optam por apresentar os avisos e solicitar o consentimento por meio de uma aplicação ou *site* na internet, devido às restrições de espaço e de funcionalidade dos próprios dispositivos de consumo que tornam difícil ou impossível a exibição dessas informações de privacidade. Muitos dispositivos não têm um ecrã e não dispõem de mecanismos de entradas de dados, como os teclados ou ecrãs táteis.[164] Muitas vezes exigem a conetividade a um dispositivo móvel para que o utilizador concorde com os termos do aviso de privacidade, especialmente quando as definições do dispositivo podem ser controladas por esse dispositivo móvel. A maioria dos fabricantes acabam por fornecer avisos de privacidade desatualizados, imprecisos, enganadores ou difíceis de encontrar, em vez de incluir termos de privacidade na embalagem do dispositivo ou avisos colocados diretamente no próprio dispositivo.

Além disso, os dispositivos de consumo IoT perturbam também o modelo tradicional do consentimento informado, que inclui um aviso seguido imediatamente pelo consentimento, um modelo fixo que pode ser inadequado para um envolvimento dinâmico. Esses mecanismos clássicos de privacidade exigem normalmente que um indivíduo complete novamente qualquer aviso de privacidade aplicável e processo de consentimento após quaisquer alterações materiais. Este modelo, aplicado à IoT, cria preocupações de eficiência e razoabilidade quando os utilizadores têm de rever o aviso para proteger os seus próprios interesses de privacidade[165]. Os modelos de envolvimento dinâmico normalmente envolvem a recolha de dados, a sua utilização e a alteração algorítmica da tomada de decisões com base num agregado de dados recolhidos, que informa os algoritmos e,

[162] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Parecer 8/2014, *Op. Cit.*, p. 8.
[163] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Parecer 8/2014, *Op. Cit.*, p. 8.
[164] CHIKE, Patrick Chike, *Op. Cit.*, p. 16.
[165] TSCHIDER, Charlotthe A. *Op. Cit.*, 112.

subsequentemente, a implementação de novas funcionalidades do produto. Um modelo tradicional de aviso prévio seguido de consentimento não é compatível com as melhorias em tempo real precipitadas pela natureza "sempre ligada" dos dispositivos de consumo da IoT. Os fabricantes e os consumidores podem ficar presos num ciclo contínuo de avisos e consentimentos sempre que haja uma alteração material do sistema. Uma frequência elevada de alterações resultaria na aplicação contínua de avisos e na subsequente exigência de consentimento aos utilizadores dos produtos[166].

Um outro problema é que a maior parte das vezes os dispositivos de consumo funcionam em ambientes onde a proximidade expõe várias pessoas à mesma atividade de recolha de dados. Por exemplo, um sensor de localização geográfica num automóvel registaria os dados de localização de todos os ocupantes do veículo, e até seguir indivíduos em veículos próximos. Nestas circunstâncias, pode ser difícil ou impossível distinguir as preferências individuais de privacidade[167]. Frequentemente, os dispositivos de consumo não têm uma interface onde o utilizador possa configurar as preferências de privacidade e, em muitas configurações da IoT, os utilizadores não têm conhecimento ou controlo sobre a forma como os seus dados pessoais estão a ser recolhidos e usados. Isso cria uma disparidade entre as preferências de privacidade do utilizador e o comportamento de recolha de dados dos dispositivos. Caso seja possível desenvolver um mecanismo eficaz para permitir que um utilizador exprima o consentimento informado das suas preferências, esse mecanismo teria de lidar com o grande número de dispositivos de consumo que um utilizador tem de controlar. Não é realista pensar que um utilizador irá interagir diretamente com cada um dos dispositivos que encontra ao longo do dia para expressar as suas preferências de privacidade. Em vez disso, os mecanismos de interface de privacidade têm de ser escaláveis para a dimensão do problema da IoT, sem deixarem de ser abrangentes e práticos do ponto de vista do utilizador[168].

2. Problemas de segurança

A segurança dos dispositivos de consumo é uma preocupação crucial que não está a acompanhar o ritmo da inovação. A complexidade e a conetividade encontradas na IoT introduzem novas vulnerabilidades e à medida que ligamos cada vez mais dispositivos à internet, surgem novas oportunidades para explorar essas potenciais vulnerabilidades de segurança. Os novos desafios em termos de segurança cria novos problemas em termos de responsabilidade[169]. Não é claro quem é que

[166] TSCHIDER, Charlotthe A. *Op. Cit.*, 110-111.
[167] INTERNET SOCIETY, *Op. Cit.*, p.28.
[168] INTERNET SOCIETY, *Op. Cit.*, p.27.
[169] COMISSÃO EUROPEIA, Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da internet das coisas e da robótica, 2020, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0064, p. 19.

fica responsável pelas decisões de segurança quando é uma organização que concebe um dispositivo, outra que fornece o *software* componente, outra que opera a rede em que o dispositivo está integrado e outra que implementa o dispositivo[170].

Os dispositivos de consumo mal protegidos podem servir como pontos de entrada a ataques informáticos, permitindo que indivíduos mal-intencionados consigam reprogramar um dispositivo ou que o dispositivo deixe de funcionar. Os dispositivos mal concebidos podem expor os dados pessoais dos seus utilizadores ao roubo, deixando os fluxos de dados inadequadamente protegidos, e os dispositivos com falhas ou mau funcionamento podem também criar vulnerabilidades de segurança. Os custos competitivos e as limitações técnicas dos dispositivos impedem muitos fabricantes de criar características de segurança adequadas nestes dispositivos, criando potenciais vulnerabilidades de segurança e de manutenção a longo prazo[171]. A corrida para fornecer dispositivos IoT baratos pode resultar em dispositivos inseguros[172].

Um ataque com sucesso a um destes dispositivos interligado possibilita que um pirata informático consiga obter o controlo do dispositivo, mas também utilizá-lo como porta de entrada para obter acesso a vários tipos de informações pessoais[173]. Cada dispositivo que esteja mal protegido pode afetar a segurança da internet a um nível global e não apenas local. Por exemplo, um frigorífico ou televisão inteligente desprotegido nos EUA que esteja infetado com *malware* consegue enviar milhares de emails de spam nocivos para destinatários em todo o mundo utilizando a ligação Wi-Fi do proprietário do dispositivo[174]. Os piratas informáticos conseguem explorar qualquer vulnerabilidade de segurança de modo a ganhar o controlo dos dispositivos. Utilizando estes dispositivos "zombie" podem efetuar ataques de negação de serviço[175] em grande escala. A IoT apresenta uma variedade de riscos de segurança como, o ganho de acesso não autorizado e a utilização indevida de dados pessoais, a facilitação de ataques a outros sistemas e a criação de riscos para a segurança pessoal[176].

A segurança dos dispositivos de consumo não é absoluta, nem existe uma posição de seguro ou não seguro. Existem dispositivos totalmente desprotegidos, sem características de segurança, até

---

[170] CHIKE, Patrick Chike, *Op. Cit.*, p. 19.
[171] INTERNET SOCIETY, *Op. Cit.*, p.20-21.
[172] CHANDER, Anupam, The internet of things: both goods and services, World Trade Review, vol. 18, 2019, disponível em https://doi.org/10.1017/S1474745619000089, p.12.
[173] OFFICE OF THE PRIVACY COMMISION OF CANADA, *Op. Cit.*, p. 21.
[174] INTERNET SOCIETY, *Op. Cit.*, p. 21.
[175] Os ataques de negação de serviço são uma forma de ataque informático em que um indivíduo ou grupo mal-intencionado tenta sobrecarregar um sistema ou rede, de modo a torná-lo inacessível aos utilizadores. O objetivo principal deste ataque é interromper ou prejudicar o funcionamento normal de um serviço. Estes ataques podem ser realizados através de várias técnicas, como o envio de uma enorme quantidade de pedidos a um servidor específico, o que faz com que o servidor fique sobrecarregado e incapaz de processar todos os pedidos ou através da exploração de vulnerabilidades de software ou configurações inadequadas para atingir o mesmo objetivo.
[176] CHANDER, Anupam, *Op. Cit.*, p. 12.

sistemas altamente seguros com várias camadas de características de segurança[177]. Embora os consumidores esperem bens seguros e razoavelmente adequados, também preferem bens de baixo custo e de utilização simples[178]. Caso um utilizador não tolere um elevado grau de risco de segurança, como é o caso de uma pessoa com um dispositivo médico implantado com acesso à internet, então pode sentir-se justificado em gastar uma quantidade razoável de recursos para proteger o sistema ou dispositivos de ataques. Contudo, se a pessoa não estiver preocupada com a possibilidade do seu frigorifico ser "atacado" e utilizado para mandar spam, então poderá não se sentir compelido a pagar por um modelo que tenha uma conceção de segurança mais sofisticada, se isso tornar o aparelho mais caro[179].

Atualmente, os especialistas em segurança jogam um jogo contínuo do gato e do rato com os cibercriminosos. A cada nova ameaça ou ataque, as equipas de segurança esforçam-se para resolver o problema[180]. A variedade enorme de *hardware*, *software*, sistemas operativos, protocolos e métodos de comunicação cria lacunas e potenciais pontos de entrada. Já aconteceu *hackers* "entrarem" em monitores de bebés inteligentes, em televisões inteligentes e violarem a segurança de dispositivos médicos e automóveis. Isto pode gerar consequências graves caso um pirata informático decida, por exemplo, desativar os travões de um carro ou instruir um dispositivo médico para deixar de funcionar[181].

As capacidades que permitem que um dispositivo tenha uma função "inteligente" são baratas de incorporar e estão a tornar-se cada vez mais presentes em dispositivos que não necessitam dessas capacidades. Como é o caso dos dispositivos de consumo domésticos, como torradeiras e brinquedos de crianças onde são implementadas essa funcionalidade "inteligente". Uma razão pela qual a segurança é um problema nos dispositivos de consumo IoT é o facto de estarem a ser fabricados por empresas de bens de consumo que não são tradicionalmente conhecidas por fabricar *hardware* ou *software* informático. Estes dispositivos geralmente não são concebidos com a capacidade de serem atualizados após serem lançados no mercado. Enquanto os computadores ou *smartphones* possuem um sistema operativo complexo que pode ser regularmente atualizado para corrigir problemas de segurança, dando ao fabricante a oportunidade de proteger o dispositivo contra novas ameaças, os dispositivos de consumo são muitas vezes menos maleáveis e robustos. Consequentemente, estes

[177] INTERNET SOCIETY, *Op. Cit.*, p. 21.
[178] TSCHIDER, Charlotthe A., *Op. Cit.*, p.97-98.
[179] INTERNET SOCIETY, *Op. Cit.*, p. 21.
[180] GREENGARD, Samuel, *Op. Cit.*, p. 189-190.
[181] GREENGARD, Samuel, *Op. Cit.*, p. 190.

dispositivos podem não ser facilmente corrigidos ou atualizados[182]. Além disso, o facto de alguns desses dispositivos serem muito pequenos é também razão pela qual a segurança é inferior nesses dispositivos pois é difícil construir segurança suficiente num espaço físico pequeno[183].

Os investigadores da área da cibersegurança realizam constantemente análises de vulnerabilidade de produtos domésticos inteligentes e muitas dessas análises revelaram diversos riscos de segurança pessoal e de danos materiais. Os atacantes conseguem destrancar portas e cadeados IoT ou alterar temperaturas dos termóstatos inteligentes para além dos valores máximos de fábrica, por exemplo, o que põe em risco de dano as propriedades e causar possíveis lesões corporais. Os brinquedos inteligentes também causam grande preocupação em relação a exposição de informações de crianças[184]. Atualmente, os monitores para bebés são frequentemente fabricados com capacidades de ligação à internet para facilitar a monitorização remota do bebé através de dispositivos móveis, e piratas informáticos já utilizaram a fraca segurança desses dispositivos para comunicar diretamente com as crianças[185].

No caso dos *wearables*, a maior parte das pessoas não sabe que os seus dados são armazenados pelos fabricantes destes dispositivos. Estes dispositivos portáteis transmitem informações altamente privadas e infelizmente, são os primeiros a ser vítimas de potenciais ataques porque não dispõem de soluções de segurança necessárias devido aos seus recursos de *hardware* limitados. Ao transportar diariamente um *smartwatch* para uma corrida, o atacante conseguirá prever com precisão e descobrir a que horas o utilizador vai sair e para onde. Aqui, não só a segurança do utilizador está em causa, como também os seus dados de saúde privados[186].

Os sistemas biométricos da IoT usados para a autenticação, como o reconhecimento de voz e os scanners de impressões digitais, estão a ser cada vez mais utilizados. O problema é quando esses dados são roubados por um pirata informático que poderá utilizar esses dados para se fazer passar por outra pessoa e ter acesso a dados confidenciais, colocando a segurança dos utilizadores comprometida.

---

[182] PEPPET, Scott R., Regulating the Internet of Things: first steps towards managing Discrimination, Privacy, Security & Consent, Forthcoming Texas Law Review, 2014, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074, p.43-44.

[183] SIEGEL, Jeremy, When the Internet of Things Flounders: looking into GDPR-Esque Security for IoT devices in the United States from the consumers' perspective, Journal of High Technology Law, vol. 20, n.º1, 2020, disponível em https://bpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/5/1153/files/2020/01/Siegel-Final-PDF.pdf, p.200-202.

[184] TSCHIDER, Charlotthe A., *Op. Cit.*, p.120.

[185] TSCHIDER, Charlotthe A., *Op. Cit.*, p.121.

[186] KARALE, Ashwin, The challenges of IoT addressing security, ethics, privacy, and laws, Internet of Things, vol. 15, 2021, disponível em https://www.sciencedirect.com/science/article/pii/S2542660521000640, p. 5.

3. Problemas legais

A utilização de dispositivos IoT de consumo traz diversos desafios do ponto de vista regulamentar e jurídico. Em alguns casos, estes dispositivos amplificam questões jurídicas que já existiam anteriormente. Noutros casos, criam novas situações legais e preocupações sobre direitos que não existiam antes[187].

A internet e a tecnologia digital introduziram grandes alterações nos sistemas jurídicos de todo o mundo, que estão a lutar para acompanhar o avanço da tecnologia atual[188]. O ambiente legal em torno dos dispositivos IoT ainda está a evoluir e muitos problemas ainda necessitam de ser abordados e resolvidos. Um dos principais desafios é que, à medida que estas tecnologias se tornam cada vez mais omnipresentes, podemos ter pouco ou nenhum aviso ou consciência de que elas estão a ser utilizadas. E assim, será complicado para um cidadão garantir que alguém seja responsabilizado pela utilização dos seus dados e contestar a forma como essa informação é utilizada[189].

Além disto, a ausência de regulamentações claras pode levar a lacunas legais que dificultam a responsabilização de práticas inadequadas e, consequentemente, afetam a confiança dos consumidores. O risco de violações de dados causadas por dispositivos de consumo é elevado e, infelizmente, há uma série de obstáculos que impedem os consumidores lesados de obterem uma reparação adequada caso lesados por um deles[190]. De seguida, vamos analisar em específico alguns problemas legais causados pelos dispositivos de consumo da internet das coisas.

3.1. A discriminação

Os dados recolhidos pelos dispositivos de consumo, como anteriormente referido, podem facilmente traçar um retrato digital pormenorizado das pessoas que interagem com estes dispositivos e, estes dados podem ser utilizados tanto para fins benéficos como discriminatórios. A vasta quantidade de dados dos sensores dos dispositivos, quando combinada com a análise de *Big Data* ou aprendizagem automática, pode conduzir a conclusões inesperadas sobre os comportamentos dos consumidores[191].

No caso dos *wearables* ou dispositivos vestíveis, uma pessoa que use dispositivos de monitorização da condição física continuamente durante dias ou semanas, recolhe informações pormenorizadas sobre os seus movimentos e outros dados relevantes. Esses dados são analisados por

[187] INTERNET SOCIETY, *Op. Cit.*, p. 34.
[188] GREENGARD, Samuel, *Op. Cit.*, p. 199.
[189] OFFICE OF THE PRIVACY COMMISION OF CANADA, *Op. Cit.*, p. 23.
[190] SIEGEL, Jeremy, *Op. Cit.*, p.191.
[191] PEPPET, Scott R., *Op. Cit.*, p.28.

uma aplicação de *software* que serve para estimar as calorias queimadas, registar as horas de sono e a sua qualidade e, no geral, determinar o nível de fitness da pessoa. Esta análise é benéfica para o utilizador como forma de quantificar a sua atividade quanto pretende atingir um objetivo de boa forma física ou de perda de peso[192]. Contudo, esses dados podem igualmente ser utilizados de uma maneira discriminatória. Podem ser utilizados, por exemplo, para revelar o comportamento alimentar de uma pessoa, se tem insónias, se sofre de diabetes, se fuma ou se abusa de álcool ou drogas. Com isto, empregadores ou seguradoras podem acabar por ter acesso a esses dados e utilizá-los para tirar conclusões ou tomar decisões economicamente importantes, sem que os consumidores tenham conhecimento. Os dados recolhidos podem fornecer uma enorme quantidade de informações sobre a pessoa ao seu potencial empregador ou companhia de seguros, que podem ser utilizadas para recusar o emprego ou a candidatura[193].

Não é claro como diferentes combinações de dados podem ser utilizadas para discriminar no futuro. Os dados da IoT quando combinados com outros recursos podem ser utilizados para facilitar a discriminação, transformar os nossos comportamentos e modificar ações em tempo real para benefício das organizações. O potencial para o exercício de práticas discriminatórias pode ser ampliado pela qualidade, especificidade e volume dos dados produzidos pela IoT sobre os utilizadores. Os algoritmos de *Big data* conseguem examinar grandes quantidades de dados e procurar correlações de modo a determinar agrupamentos ou conjuntos de características relacionadas entre utilizadores. Contudo, estes algoritmos são suscetíveis de categorizar injustamente os utilizadores e de explorar as suas características[194].

A discriminação algorítmica é uma preocupação crescente à medida que a conexão entre os dispositivos de consumo inteligentes e a enorme recolha de dados se tornam cada vez mais presentes. Os principais problemas das decisões algorítmicas residem na sua opacidade, frequentemente resultando na falta de compreensão, até mesmo por parte dos fabricantes, das razões subjacentes às conclusões dos algoritmos. Além disso, os dados utilizados para alimentar esses algoritmos podem conter vícios desde a sua programação inicial ou serem influenciados posteriormente pela interação na rede. Essa situação pode ser originada por diversos motivos, incluindo preconceitos presentes nos dados utilizados para treinar os algoritmos, falhas na conceção dos próprios algoritmos, ou até mesmo

[192] INTERNET SOCIETY, *Op. Cit.*, p. 35.
[193] CHIKE, Patrick Chike, *Op. Cit.*, p. 12.
[194] INTERNET SOCIETY, *Op. Cit.*, p. 36.

decisões conscientes dos fabricantes. Isso torna as decisões automatizadas um terreno propício para a ocorrência de discriminação, especialmente contra os mais vulneráveis[195].

Sendo assim, temos uma situação de discriminação algorítmica quando os vários algoritmos, que alimentam os sistemas da IoT, tomam decisões que resultam num tratamento discriminatório ou injusto com base em características como a idade, género, classe social, entre outras. Um exemplo comum de discriminação algorítmica ocorre nos sistemas de reconhecimento facial. Se estes sistemas forem treinados predominantemente com imagens de pessoas de determinada etnia, podem depois ter dificuldade em reconhecer com precisão indivíduos de outras etnias, resultando num tratamento desigual[196].

3.2. A responsabilidade

A responsabilidade é um dos princípios fundamentais para a proteção da privacidade e dos dados pessoais. Os dispositivos IoT de consumo fazem surgir diversas questões de responsabilidade jurídica que devem ser consideradas. A questão-chave é: quem é o responsável caso uma pessoa seja prejudicada em resultado da ação ou inação de um dispositivo? A resposta é frequentemente complicada e, em muitos casos, não existe ainda muita jurisprudência que apoie determinada posição. Surgem então desafios complexos em termos de responsabilidade, já que os fabricantes e implementadores das tecnologias podem não conseguir antecipar todos os seus potenciais propósitos, contextos, usos e utilizadores[197].

Os dispositivos IoT de consumo funcionam de uma forma mais complexa do que um simples produto autónomo, o que leva a necessidade de considerar vários cenários de responsabilidade mais complicados. Por exemplo, é possível que os dispositivos de consumo sejam utilizados de formas não previstas pelos fabricantes. Um fabricante de dispositivos não pode razoavelmente efetuar testes de garantia do produto em todos os casos de utilização possíveis. Outro exemplo, podendo estes dispositivos ter uma longa vida útil, tornam-se suscetíveis a futuras ameaças à segurança que são desconhecidas atualmente. Por conseguinte, estes dispositivos podem ficar comprometidos e ser reprogramados de forma maliciosa para se danificarem a si próprios ou outros dispositivos, ou para revelarem informações sensíveis de forma despercebida. Existe também a possibilidade dos dispositivos IoT ligarem-se e interagirem com outros dispositivos IoT de formas não testadas e

[195] REQUIÃO, Maurício; COSTA, Diego Carneiro, Discriminação algorítmica: ações afirmativas como estratégia de combate, 2022, disponível em https://www.academia.edu/97882347/Discriminação_algorítmica_ações_afirmativas_como_estratégia_de_combate, p. 2.

[196] KLWINBERG, Jon, el al, Discrimination in the Age of Algorithms, Journal of Legal Analysis, Vol. 10, 2018, disponível em https://academic.oup.com/jla/article/doi/10.1093/jla/laz001/5476086?login=false, p. 116.

[197] SINGH, Jatinder, *et al*, Accountability in the Internet of Things (IoT): Systems, law & ways forward, *in* Computer, vol. 51, 2018, disponível em https://ieeexplore.ieee.org/document/8423131p. 3.

imprevistas. Com o gradual aumento da interoperabilidade destes dispositivos, eles serão capazes de criar conexões de rede entre si, que consequentemente, trará dificuldade para um fabricante ou utilizador de ter em conta todos os cenários potencialmente prejudiciais antes de instalar estes dispositivos[198].

A combinação entre diferentes componentes digitais num ecossistema complexo e com uma pluralidade de intervenientes, como é a Internet das Coisas, pode dificultar a determinação da origem de eventuais dados e dos responsáveis pelos mesmos. Esta complexidade torna muito difícil para as vítimas identificar a pessoas responsáveis e provar que reúne as condições necessárias para estabelecer o direito à indemnização[199]. Posto isto, é necessário dar resposta aos desafios relacionados com a responsabilidade para assegurar a proteção das vítimas e, assim, manter simultaneamente o equilíbrio com as necessidades de inovação tecnológica que contribuirá para criar confiança nestas tecnologias[200].

3.3. O fluxo de dados transfronteiriços

À medida que a rede de dispositivos de consumo da Internet das Coisas continua a expandir-se, surgem preocupações sobre o fluxo de dados transfronteiriços. Este fluxo de dados refere-se à transferência de dados pessoais entre fronteiras, o que levanta vários problemas, pois, o que é legal num país pode ser ilegal noutro. Estes problemas aumentam exponencialmente à medida que os dados se deslocam entre servidores, nuvens e dispositivos que residem em diferentes jurisdições, e tentar perceber onde residem os dados e quem tem direito sobre eles é uma tarefa quase impossível. A IoT acrescenta camadas adicionais de complexidade a um ambiente informático já de si complexo. A tentativa de compreender a origem dos dados e a forma como estes são alterados ou modificados ao longo de um percurso eletrónico cria enormes desafios[201].

Os dados recolhidos pelos dispositivos não podem ser impedidos de serem enviados através de fronteiras jurisdicionais. A internet ultrapassa as fronteiras jurisdicionais a todos os níveis e estes dispositivos utilizam a internet para comunicar. Os dispositivos podem recolher os dados numa jurisdição e transmitir esses dados para outra jurisdição para processamento e armazenamento. Podem também ligar-se automaticamente a outros dispositivos e sistemas e transmitir dados através de fronteiras internacionais sem o conhecimento do utilizador[202]. Além disso, as leis de proteção de dados

[198] INTERNET SOCIETY, *Op. Cit.*, p. 38.
[199] COMISSÃO EUROPEIA, *Op. Cit.*, p. 16.
[200] COMISSÃO EUROPEIA, *Op. Cit.*, p. 19.
[201] GREENGARD, Samuel, *Op. Cit.*, p. 200.
[202] CHIKE, Patrick Chike, *Op. Cit.*, p. 15.

na jurisdição onde o titular dos dados reside podem ser incompatíveis com as leis da jurisdição onde os dados são armazenados e processados[203].

Um dos principais problemas decorrentes do fluxo de dados transfronteiriço é a questão da privacidade e segurança dos dados. Com uma vasta quantidade de informações pessoais e sensíveis a serem transmitidas entre países, é essencial garantir que os dados sejam protegidos contra acessos não autorizados e uso indevido. Os dados serão possuídos, administrados e operados por várias pessoas e entidades, possivelmente em diferentes locais geográficos, cada uma com os seus próprios interesses, motivações, responsabilidades e compromissos[204]. As normas e expetativas em matéria de privacidade estão estreitamente relacionadas com o contexto social e cultural dos utilizadores, que variará de um grupo ou nação para outro. As disparidades nas leis de privacidade e proteção de dados entre diferentes países podem criar um ambiente confuso e complexo para empresas e utilizadores, criando desafios para a conformidade regulamentar e colocando as empresas em risco de violações legais.

3.4. O auxílio na aplicação da lei

Os dispositivos de consumo da IoT oferecem potenciais benefícios para a aplicação da lei e para a segurança pública, benefícios que vão desde a vigilância remota até à recolha de dados em tempo real. Estes dispositivos acrescentam olhos e ouvidos às nossas casas, carros e até mesmo aos nossos corpos, através dos sensores, câmaras, microfones e outras tecnologias, que estão constantemente a recolher dados e a enviá-los para os servidores de empresas para análise e armazenamento. Consequentemente, a polícia começa a pedir informação criada pelos dispositivos, o que traz implicações significativas para a privacidade.

A grande quantidade de dados que estes dispositivos geram permite às autoridades policiais analisar a proximidade de uma pessoa a um crime, avaliar as relações entre vítimas e suspeitos e até rever gravações de declarações incriminatórias. Os dispositivos de consumo e os dados que originam podem ser usados como ferramentas eficazes para combater o crime e trazer benefícios às autoridades policiais para melhorar a segurança pública. Como exemplo, a *On-Star Corporation*, uma subsidiária da empresa americana *General Motors*, forneceu à polícia dados de sensores de automóveis para ajudar na recuperação de carros roubado e desativar remotamente um veículo roubado[205]. Contudo, as

[203] INTERNET SOCIETY, *Op. Cit.*, p. 34.
[204] SINGH, Jatinder, *Op. Cit.*, p. 3.
[205] INTERNET SOCIETY, *Op. Cit.*, p. 37.

ramificações legais e sociais devem ser cuidadosamente consideradas, pois apresenta uma série de problemas que precisam ser cuidadosamente considerados de modo garantir um uso eficaz e ético.

Entre as potenciais causas de preocupação contam-se a omnipresença das atividades de monitorização de dados que podem revelar informações sensíveis sobre as casas, os movimentos e as interações das pessoas com os outros, o potencial para a discriminação algorítmica, bem como a potencial exposição inadvertida desses dados a terceiros mal-intencionados. Embora os dispositivos IoT, como as câmaras ou relógios inteligentes, possam ser benéficos para os agentes da autoridade na localização de criminosos, a forma como são utilizados pode também violar a privacidade dos consumidores[206].

Os dados recolhidos pelos dispositivos de consumo podem também muitas vezes servir de prova numa série de processos judiciais e, à medida que os dados se tornam mais prevalecentes, é provável que sejam cada vez mais utilizados em ações judiciais.[207] No entanto, um ponto crítico, é a questão da precisão, confiabilidade e integridade dos dados recolhidos pelos dispositivos de consumo da IoT, pois erros de interpretação ou falhas técnicas podem levar a erros judiciais, falsas identificações e ações injustas por parte das autoridades. Existe também o risco de os algoritmos de IA utilizados para analisar os dados recolhidos possam perpetuar preconceitos existentes, resultando em decisões discriminatórias, definição de perfis e tratamento injusto. Como os algoritmos da IA funcionam frequentemente de uma forma opaca, dificulta a compreensão dos seus processos de decisão. No sistema jurídico, a explicabilidade é crucial para garantir a responsabilização, permitindo que os indivíduos compreendam como as decisões são tomadas e as contestem, se necessário. Devem ser empregues esforços para desenvolver modelos de IA interpretáveis que possam fornecer explicações transparentes para os seus resultados[208].

4. Problemas de interoperabilidade

O primeiro requisito da conetividade à internet é que os sistemas "ligados" sejam capazes de "falar a mesma linguagem" de protocolos e codificações[209]. A variedade de padrões e protocolos de comunicação entre dispositivos IoT muitas vezes resulta em desafios significativos de interoperabilidade.

---

[206] CHIKE, Patrick Chike, *Op. Cit.*, p. 13-14.
[207] INTERNET SOCIETY, *Op. Cit.*, p.38.
[208] KABIR, Md. Shahin; ALAM, Mohammad Nazmul, IoT, Big Data and AI Applications in the Law Enforcement and Legal System: A Review, International Research Journal of Engineering and Technology, vol. 10, 2023, disponível em https://www.researchgate.net/publication/371155772_IoT_Big_Data_and_AI_Applications_in_the_Law_Enforcement_and_Legal_System_A_Review, p. 1785.
[209] INTERNET SOCIETY, *Op. Cit.*, p.29.

Verifica-se que um grande conjunto de dispositivos inteligentes, dotados de interfaces, serviços e capacidades computacionais próprias, tem vindo a surgir no mercado, sendo crucial garantir a interoperabilidade entre estes dispositivos e o seu ambiente envolvente. Os consumidores utilizam cada vez mais dispositivos conectados e serviços associados que são fabricados ou fornecidos por diferentes produtores e prestadores de serviços. Existe o risco de estes produtos serem colocados em ecossistemas limitados que podem ser problemáticos para os consumidores porque podem reduzir as suas possibilidades de escolha na prática. Por exemplo, um consumidor pode ter um frigorífico inteligente, um assistente digital e fechaduras inteligentes que funcionam em conjunto num ecossistema comum. Caso um consumidor compre um novo dispositivo conectado que seja incompatível com esse ecossistema, torna-se um problema[210].

Garantir a interoperabilidade, principalmente através de normas adequadas, e reduzir os aspetos problemáticos desses ecossistemas é importante do ponto de vista da segurança. Os consumidores podem querer substituir os seus produtos ligados nas suas casas por produtos concorrentes que sejam mais seguros, mas para isso têm que ter a certeza de que os produtos funcionarão em qualquer ecossistema. Por isso, os consumidores devem ter sempre a liberdade de escolher produtos sem receio de ficarem presos a um *software* ou *hardware* pertencente a um fabricante ou prestador de serviços específico[211].

Além disso, a falta de interoperabilidade pode constituir um grande obstáculo para a segurança, resiliência e estabilidade da IoT devido à ausência de padrões de segurança consistentes entre os diferentes dispositivos de consumo criados por diferentes fabricantes, no qual os seus *softwares* baseiam-se em tecnologias com padrões técnicos distintos. Isto pode causar vulnerabilidades de segurança, uma vez que cada dispositivo pode ter práticas de segurança variadas ou inadequadas, tornando-os alvos mais fáceis para os invasores. Padrões universais e esforços cooperativos são fundamentais para superar estas barreiras, garantindo que os dispositivos de diferentes fabricantes consigam trabalhar em conjunto de maneira harmoniosa. A interoperabilidade permite que a diversidade de dispositivos ligados à internet aumente[212].

Num ambiente totalmente interoperável, qualquer dispositivo seria capaz de ligar-se a qualquer outro dispositivo ou sistema e trocar informações como desejado. Contudo, na prática, a

---

[210] ENISA ADVISORY GROUP, Opinion Consumers and IoT Security, 2019, disponível em https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/ag-publications/final-opinion-enisa-ag-consumer-iot-perspective-09.2019, p. 9.

[211] ENISA ADVISORY GROUP, Opinion Consumers and IoT Security, *Op. Cit.*, p. 9.

[212] LEITE, Leandro Rogério Corrêa, Internet das Coisas (IoT): Vulnerabilidades de Segurança e Desafios, 2019, disponível em http://ric.cps.sp.gov.br/bitstream/123456789/3978/1/20192S_LEITELeandroRogérioCorrêa_OD0763.pdf, p. 30.

interoperabilidade é mais complexa. A interoperabilidade total em todos os aspetos de um produto técnico nem sempre é exequível, necessária ou desejável e, se for imposta artificialmente (por exemplo, através de mandatos governamentais), pode desincentivar o investimento e a inovação. Contudo, uma interoperabilidade que funcione bem e esteja bem definida pode estimular a inovação e proporcionar ganhos de eficiência aos fabricantes de dispositivos. A aplicação das normas e o desenvolvimento de novas normas abertas[213], quando necessário, ajudam a reduzir os obstáculos à entrada, facilitam novos modelos de negócio e criam economias de escala[214].

As barreiras propositadamente criadas para dificultar a troca de informações podem privar os utilizadores da internet da capacidade de se conectar, comunicar, partilhar e inovar. A interoperabilidade é valiosa tanto para o consumidor individual como para o utilizador empresarial destes dispositivos. Facilita a capacidade de escolher dispositivos com as melhores características pelo melhor preço e de os integrar para que funcionem em conjunto. Os compradores podem hesitar em comprar produtos e serviços IoT se enfrentarem inflexibilidade na integração, preocupações com dependência do fornecedor ou medo de obsolescência devido a alteração das normas[215].

É imperativo enfrentar os desafios mencionados para garantir um ambiente seguro, regulamentado e interoperável. A aceitação social, omnipresença e familiaridade dos dispositivos podem criar uma falsa sensação de segurança e encorajar as pessoas a divulgarem informações privadas ou sensíveis sem estarem plenamente conscientes ou terem noção das potenciais consequências de o fazerem[216]. E com a normalização dos dispositivos de consumo, há uma crescente "erosão da escolha" para os indivíduos que teriam preferido as suas versões "não inteligentes"[217]. É cada vez mais difícil encontrar dispositivos que não sejam ligados à internet e a cada dia que passa, ficamos mais dependentes desses dispositivos para serviços essenciais. No futuro, é provável que a nossa capacidade de realizar atividades diárias sem a utilização de dispositivos ou sistemas ligados à internet, diminua[218].

[213] As normas abertas formam a base da cooperação na sociedade moderna, pois possibilitam que as pessoas possam partilhar de forma livre todo o tipo de dados, evitando a dependência de fabricantes e fornecedores ou outras barreiras artificiais à interoperabilidade. Esta normas abertas promovem a escolha entre fornecedores e são implementáveis com software livre oferecendo assim livre concorrência no mercado. https://fsfe.org/freesoftware/standards/standards.pt.html.
[214] INTERNET SOCIETY, *Op. Cit.*, p.30.
[215] INTERNET SOCIETY, *Op. Cit.*, p.31.
[216] INTERNET SOCIETY, *Op. Cit.*, p.28.
[217] OFFICE OF THE PRIVACY COMMISION OF CANADA, *Op. Cit.*, p. 21.
[218] INTERNET SOCIETY, *Op. Cit.*, p. 21.

Capítulo IV – Meios de proteção contra os dispositivos de consumo da IoT

1. Introdução

A Internet das Coisas alterou a forma como interagimos com a tecnologia e, atualmente, produz conjuntos de dados cada vez maiores sobre o comportamento dos utilizadores. Por este motivo, é preciso encontrar formas de proteger a nossa privacidade de forma eficaz e lidar com as vulnerabilidades e riscos de segurança presentes na maior parte dos dispositivos de consumo da IoT e nos seus sensores associados[219] e encontrar formas de resolver os problemas legais decorrentes da sua utilização.

Em primeiro lugar, é essencial munir os consumidores de ferramentas necessárias para enfrentar os desafios da Internet das Coisas. É fundamental que todos os indivíduos compreendam quais são os seus direitos enquanto consumidores de produtos e serviços. Educar os utilizadores sobre os seus direitos é capacitá-los de fazerem escolhas informadas relativamente aos seus dados pessoais. É necessária a consciencialização dos utilizadores em relação às boas práticas que podem e devem adotar de modo a proteger a sua privacidade e os seus dados pessoais, mas também garantir que as suas ações e comportamentos não colocam os outros em risco. A educação dos consumidores sobre esses princípios e ferramentas está na vanguarda da consciencialização e participação bem-sucedidas na economia digital,[220] permitindo, assim, uma maior evolução da Internet das Coisas.

Contudo, a segurança não depende totalmente da forma como os consumidores gerem os seus próprios riscos de privacidade e segurança[221]. As organizações devem dar primazia a interfaces de fácil utilização, avisos de privacidade claros e mecanismos acessíveis de controlo e consentimento do utilizador. Ao promover a educação e a sensibilização dos utilizadores, as organizações podem fomentar uma cultura de privacidade e incentivar os indivíduos a participarem ativamente na proteção dos seus direitos de privacidade no contexto da IoT[222]. A capacitação dos utilizadores é fundamental, os titulares dos dados devem poder exercer os seus direitos e, assim, "deter o controlo" dos dados a todo o momento[223].

---

[219] PEPPET, Scott R., *Op. Cit.*, p.1.
[220] CONSELHO DA EUROPA, Digital Citizenship Education Handbook, 2022, disponível em https://www.coe.int/en/web/digital-citizenship-education/-/2022-edition-of-the-digital-citizenship-education-handbook, p.114.
[221] CONSELHO DA EUROPA, *Op. Cit.*, p.104.
[222] GDPR Compliance for Internet of Things (IoT) Devices: Privacy in a Connected World, disponível em https://www.gdpr-advisor.com/gdpr-compliance-for-internet-of-things-iot/.
[223] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Parecer 8/2014, *Op. Cit.*, p. 24.

Em segundo lugar, para enfrentar os vários desafios provenientes dos dispositivos de consumo da IoT, é necessário combinar métodos, estratégias e ferramentas disponíveis, abrangendo a tecnologia, leis e práticas profissionais. Se este esforço e colaboração ocorrerem, poderá resultar num quadro de privacidade prospetivo que incorpore uma ampla gama de normas, mecanismos de controlo e intervenientes. Criar-se-á um sistema de privacidade e proteção de dados pessoais que será maior, mais complexo, mais diversificado e potencialmente mais eficaz do que os direitos individuais de privacidade e proteção de dados[224].

2. Interação entre o Direito e a tecnologia

A privacidade é um conceito em constante evolução. Está fortemente moldado pela tecnologia e ligado diretamente com as evoluções sociais e expectativas normativas. À medida que integramos e operacionalizamos tecnologias cada vez mais omnipresentes nas nossas vidas, através do processo de normalização, passamos gradualmente a aceitar normas e valores diferentes[225]. A tecnologia digital atual tornou fundamental a necessidade de repensar a "privacidade", uma necessidade de examinar novamente os próprios conceitos e valores de privacidade com que a sociedade se preocupa. Isto poderá exigir que se saia do âmbito da lei da privacidade e da proteção de dados para outras áreas do Direito e da política em geral. A interação entre a tecnologia, o Direito e a sociedade é complexa e existe uma enorme diversidade de instrumentos disponíveis para ajudar a moldar os efeitos sociais da tecnologia na humanidade[226].

Deste modo, é importante promover a partilha de conhecimento e a integração entre o Direito e a tecnologia e, assim, adotar medidas técnicas de forma a apoiar a privacidade. Os contínuos avanços tecnológicos possibilitam ataques cada vez mais sofisticados não previstos na altura em que foram elaboradas diversas normas jurídicas muitas vezes ainda aplicáveis à proteção da privacidade. Será necessário desenvolver abordagens técnicas que sejam robustas contra novos tipos de ataques. Estas medidas tecnológicas devem ser criadas tendo em conta a conformidade com as normas e práticas jurídicas, de modo a garantir uma proteção da privacidade a uma grande escala[227].

Vários exemplos práticos já demonstraram que as soluções técnicas de privacidade emergentes, que incluem ferramentas sofisticadas de armazenamento, análise, divulgação de dados e controlo de acesso, podem atuar em conjunto com soluções legais e organizacionais de forma a gerir

[224] GASSER, Urs, Futuring Digital Privacy, Reimaging the Law/Tech interplay, Big Data and Global Trade Law, 2021, disponivel em https://doi.org/10.1017/9781108919234.013, p. 210-211.
[225] CONSELHO DA EUROPA, *Op. Cit.*, p. 110.
[226] GASSER, Urs, *Op. Cit.*, p. 201.
[227] GASSER, Urs, *Op. Cit.*, p.205.

melhor os riscos de privacidade. Como exemplos, temos o papel importante que a criptografia desempenha na segurança do acesso e armazenamento de dados, o desenvolvimento de formas técnicas que ajude a implementar o direito a ser esquecido através da eliminação eficaz dos registos de uma pessoa dos modelos de Aprendizagem Automática, o desenvolvimento da IA no sentido da transparência e responsabilização ou o desenvolvimento tecnológico de um armazenamento de dados pessoais que permite às pessoas exercerem um controlo sobre o local onde as informações que lhes dizem respeito são armazenadas e a forma como são acedidas[228].

A necessidade de uma maior interoperabilidade entre as abordagens tecnológicas e jurídicas não se limita a um nível mecânico de técnicas e ferramentas de preservação da privacidade e ultrapassa os esforços para exigir que as empresas protejam a privacidade incorporando-a na conceção dos seus dispositivos e nas práticas comerciais.

3. Abordagem jurídica de proteção da privacidade e dos dados pessoais

O desenvolvimento e a aplicação de normas de privacidade e de padrões de conformidade específicos para os dispositivos de consumo da Internet das Coisas é importante para que estes cumpram os requisitos mínimos de privacidade e segurança. Porém, não existem normas harmonizadas para a construção de dispositivos que ajudem a antecipar as preocupações com a proteção de dados, e a crescente consciencialização de que os dispositivos têm "fugas" de dados ou que podem ser facilmente pirateados e afetados por ataques generalizados de negação de serviço, contribuem para a diminuição da confiança dos utilizadores nestes dispositivos, sendo portanto, fundamental a criação de relações de confiança com os consumidores em relação à Internet das Coisas[229].

O Regulamento (UE) 2019/881 do parlamento europeu e do conselho, reforça a capacidade da Agência da União Europeia para a Cibersegurança ou ENISA para ajudar os Estados-Membros a enfrentar os riscos de cibersegurança. Esta lei aborda os dispositivos IoT, levando as autoridades a tomar medidas contra as vulnerabilidades da Internet das Coisas. Segundo o Considerando 2 deste Regulamento, "a digitalização e a conectividade estão a tornar-se características centrais num número cada vez maior de produtos e serviços e, com o surgimento da Internet das Coisas, espera-se que um número extremamente elevado de dispositivos digitais conectados seja implantado em toda a União durante a próxima década. Embora haja cada vez mais dispositivos conectados à internet, a segurança

[228] GASSER, Urs, *Op. Cit.*, p.207.
[229] URQUHART, Lachlan; *et al*, Demonstrably doing accountability in the Internet of Things, International Journal of Law and Information Technology, vol. 27, 2018, disponível em https://doi.org/10.1093/ijlit/eay015, p. 2.

e a resiliência não são suficientemente integradas na conceção, o que conduz a uma insuficiência a nível da cibersegurança". Portanto, este Regulamento inclui uma lista de disposições para regular e reforçar a segurança e a privacidade digitais do utilizador[230]. Em Portugal, foi implementado o Decreto-Lei n.º 65/2021, de 30 de Julho que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019.

Foi aprovado recentemente o Regulamento sobre a Inteligência Artificial, tornando-se o primeiro regulamento existente sobre IA, no qual cria regras harmonizadas em matéria de inteligência artificial. Este Regulamento tem como finalidade "melhorar o funcionamento do mercado interno e promover a adoção de uma inteligência artificial centrada no ser humano e de confiança, assegurando simultaneamente um elevado nível de proteção da saúde, da segurança e dos direitos fundamentais consagrados na Carta (...) contra os efeitos nocivos dos sistemas de IA na União, bem como apoiar a inovação", de acordo com o número 1 do artigo 1.º do regulamento. Segundo o número 2 do mesmo artigo, este regulamento estabelece "proibições de certas práticas de IA", "requisitos específicos para sistemas de IA de risco elevado e obrigações para os operadores desses sistemas", "regras de transparência harmonizadas para determinados sistemas de IA", "regras harmonizadas para a colocação no mercado de modelos de IA de finalidade geral", entre outras regras.

Portanto, este Regulamento contém salvaguardas para a Inteligência Artificial ao apresentar novas regras que proíbem certas aplicações de IA que ameaçam os direitos dos cidadãos, incluindo sistemas de caracterização biométrica baseados em características sensíveis, introduzindo, deste modo, limites à utilização de sistemas de identificação biométrica pelas autoridades policiais. É também feita a proibição da utilização da IA para manipulação e exploração de vulnerabilidades dos consumidores[231]. Sendo assim, este Regulamento poderá ter um impacto significativo no âmbito da Internet das Coisas pois, a implementação de normas de IA pode permitir que os dispositivos de consumo da IoT sejam implementados de forma mais segura e ética.

Além disso, foi realizada uma proposta de Regulamento sobre a Privacidade Eletrónica com o propósito de substituir a Diretiva sobre a Privacidade Eletrónica e Comunicações Eletrónicas de 2002. Esta proposta de Regulamento foca-se na privacidade dos dados, servindo para complementar o

[230] KARALE, Ashwin, *Op. Cit.*, p.12.

[231] Regulamento Inteligência Artificial: Parlamento aprova legislação histórica, disponível em https://www.europarl.europa.eu/news/pt/press-room/20240308IPR19015/regulamento-inteligencia-artificial-parlamento-aprova-legislacao-historica.

RGPD[232] e tem o objetivo de garantir e promover uma comunicação eletrónica segura de informações no sistema da Internet das Coisas que incorpore redes e dispositivos IoT[233]. Conforme o seu Considerando 12, "as máquinas e dispositivos conectados comunicam cada vez mais entre si mediante a utilização de redes de comunicações eletrónicas. A transmissão de comunicações máquina-máquina implica o envio de sinais através de uma rede e, por conseguinte, constitui normalmente um serviço de comunicações eletrónicas. A fim de assegurar a plena proteção dos direitos à privacidade e à confidencialidade das comunicações, e para promover uma Internet das Coisas segura e de confiança no mercado único digital, é necessário esclarecer que o presente regulamento deve aplicar-se à transmissão de comunicações máquina-máquina".

Como se pode ver, a UE tem estado sempre à frente no que diz respeito às preocupações com a privacidade e proteção de dados dos seus cidadãos. Para proteger os dados pessoais colocados em risco pelos contínuos avanços tecnológicos foi implementado, como já anteriormente referido, o RGPD, que assumiu uma importância indiscutível. O RGPD é, nos dias de hoje, o diploma principal no âmbito da proteção de dados no ordenamento jurídico nacional e europeu[234]. E é o esforço mais abrangente do mundo até à data para alinhar as regras de proteção de dados dos países com as capacidades modernas da tecnologia digital, desempenhando um papel fundamental na salvaguarda dos direitos de privacidade no domínio da IoT. Devido às extensas capacidades de recolha e processamento dos dados dos dispositivos de consumo, garantir a conformidade com o RGPD é essencial para proteger a privacidade do utilizador. A conformidade com o RGPD facilita amenizar os riscos associados a acessos não autorizados, à violação de dados e à utilização incorreta de informações pessoais, promovendo, deste modo, práticas responsáveis de tratamento de dados[235].

O âmbito territorial do RGPD é amplo, abrangendo todas as organizações que recolhem, processam e armazenam dados pessoais de indivíduos residentes na UE, independentemente da localização da organização, de acordo com o artigo 3.º do RGPD.

Todavia, aplicar normas de privacidade e proteção de dados em sistemas da Internet das Coisas trata-se de uma tarefa complicada. Especificar as obrigações detalhadas de responsabilidade e conformidade teoricamente aplicáveis aos responsáveis pelo tratamento de dados é a maior parte das vezes difícil ou até impossível. A natureza diversificada da Internet das Coisas dificulta o

[232] Declaração 03/2021 sobre o Regulamento Privacidade Eletrónica, disponível em https://www.edpb.europa.eu/system/files/2021-06/edpb_statement_032021_eprivacy_regulation_pt.pdf, p.1.
[233] KARALE, Ashwin, *Op. Cit.*, p.12.
[234] SOUSA, Daniela Rodrigues de, A Proteção de Dados Pessoais do Consumidor, Estudos de Direito do Consumo, vol. III, Almedina, 2023, p. 255.
[235] GDPR Compliance for Internet of Things (IoT) Devices: Privacy in a Connected World, disponível em https://www.gdpr-advisor.com/gdpr-compliance-for-internet-of-things-iot/.

estabelecimento de um quadro de conformidade uniforme que acomode os seus requisitos específicos. Além disso, certas regras podem não ser compatíveis com muitos processos baseados na IoT. Como exemplo, temos os sistemas que utilizam aprendizagem automática para facilitar as decisões automatizadas, em que torna difícil fornecer "informações úteis relativas à lógica subjacente" (alínea g), n.º 2, artigo 14.º do RGPD)). Da mesma forma, a ideia de que os indivíduos podem insistir na eliminação dos seus dados pessoais em determinadas circunstâncias – o "direito a ser esquecido" – pode não ser viável em muitos ambientes distribuídos, como o da Internet das Coisas[236].

Portanto, os dispositivos IoT de consumo apresentam características únicas que causam dificuldades para a existência de conformidade com o RGPD. Contudo, atualmente existem diversos meios para facilitar a conformidade com o RGPD, pois surgem cada vez mais novas ferramentas técnicas que podem ajudar os responsáveis pelo tratamento dos dados a cumprirem as suas obrigações legais. As organizações devem avaliar e supervisionar continuamente os seus dispositivos de consumo e é importante o estabelecimento de práticas claras de governação no âmbito do desenvolvimento, implementação e utilização dos dispositivos de consumo. No entanto, é preciso ter em conta que a existência de uma conformidade perfeita num sistema complexo que é a Internet das Coisas é, provavelmente, impossível de atingir[237] mas, não impede que sejam realizados diversos esforços para que se proteja ao máximo os utilizadores através de uma Internet das Coisas mais "atenta à privacidade".

Sendo assim, de forma a existir conformidade com o RGPD é necessário o cumprimento dos diversos princípios previstos no artigo 5.º do RGPD. Relativamente ao princípio da legalidade, lealdade e transparência, os dispositivos de consumo devem processar os dados pessoais de forma legal, justa e transparente. Para isto, as organizações necessitam de uma base legal válida para o tratamento de dados pessoais, como o consentimento do titular dos dados, a execução de um contrato, o cumprimento de uma obrigação jurídica, a proteção de interesses vitais do titular dos dados, interesse público ou interesses legítimos do responsável pelo tratamento ou por terceiros, como previsto nas alíneas a) a f) do n.º 1 do artigo 6.º do RGPD. De modo a cumprir os princípios da limitação da finalidade e minimização dos dados, os dispositivos devem recolher e processar dados pessoais apenas para fins determinados, explícitos e legítimos. E os dados não devem ser processados posteriormente de forma incompatível com esses objetivos. Sendo assim, as empresas têm de garantir que os dados recolhidos são adequados, relevantes e limitados ao que é necessário para os objetivos pretendidos

[236] SINGH, Jatinder, *Op. Cit.*, p. 7.
[237] SINGH, Jatinder, *Op. Cit.*, p. 7.

(alíneas b) e c) do artigo 5.º do RGPD). Aqui, o propósito é a minimização dos dados e o desencorajamento da recolha excessiva e indiscriminada de dados pessoais[238].

O consentimento só constitui um fundamento jurídico adequado se for oferecido ao titular dos dados uma verdadeira opção de aceitar os termos propostos ou recusá-los sem ser prejudicado. Caso o consentimento seja obtido com conformidade com o RGPD, trata-se de um instrumento que permite aos titulares dos dados controlarem se os dados pessoais que lhes dizem respeito vão ser tratados ou não[239]. Portanto, as organizações devem obter o consentimento livre, específico, informado e explícito dos indivíduos para o tratamento dos seus dados pessoais, de modo que os utilizadores dos dispositivos tenham o devido controlo sobre os seus dados e a possibilidade de retirar o consentimento a qualquer altura sem prejuízo. As políticas de informação e consentimento devem focar-se em informações que sejam de fácil entendimento para o utilizador e não devem limitar-se a uma política geral de privacidade presente no sítio Web dos responsáveis pelo tratamento[240].

Deste modo, é importante as empresas garantirem que os mecanismos de consentimento sejam claros e de fácil utilização e que permitem às pessoas fazerem escolhas pormenorizadas relativamente ao tratamento dos dados pessoais. E é neste sentido que os fabricantes dos dispositivos de consumo da IoT devem dar prioridade ao desenvolvimento de interfaces de fácil utilização que possibilitem aos indivíduos gerir mais facilmente as suas preferências de privacidade, fornecer opções de consentimento granulares[241] e permitir a retirada do consentimento. Estes mecanismos de controlo devem ser intuitivos, de forma a permitir aos utilizadores exercer os seus direitos ao abrigo do RGPD, incluindo os direitos de acesso, retificação, restrição e apagamento dos seus dados pessoais[242]. Com a existência de uma interface partilhada, os utilizadores poderiam alterar as preferências granulares em todos os produtos simultaneamente, incluindo utilizações secundárias como a partilha de dados, restrições à transparência e venda de dados[243].

A transparência do tratamento é um requisito fundamental do RGPD que tem o objetivo de criar confiança nos processos que afetam os utilizadores fazendo com que estes compreendam, e caso seja necessário, se oponham a esses processos. A transparência está intrinsecamente ligada ao princípio da responsabilidade, uma vez que este princípio exige a transparência das operações de tratamento para

[238] GDPR Compliance for Internet of Things (IoT) Devices, *Op. Cit.*
[239] CEPD, Diretrizes 05/2020 relativas ao consentimento na acessão do regulamento 2016/679, adotadas em 4 de maio de 2020, disponível em https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt, p.5.
[240] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Parecer 8/2014, *Op. Cit.*, p. 24.
[241] Uma vez que um serviço pode abranger diversas operações de tratamento para mais do que uma finalidade, os titulares dos dados devem poder escolher quais são as finalidades que aceitam e não ter que dar consentimento para um conjunto de finalidades de tratamento. CEPD, Diretrizes 05/2020, *Op. Cit.*, p.14.
[242] GDPR Compliance for Internet of Things (IoT) Devices, *Op. Cit.*
[243] TSCHIDER, Charlotthe A., *Op. Cit.*, p.139.

que os responsáveis pelo tratamento possam comprovar o cumprimento das suas obrigações no termos do RGPD[244].

A transparência deve ser aplicada ao longo do ciclo de vida do tratamento dos dados: antes ou no início do tratamento dos dados, ou seja, quando os dados pessoais são recolhidos junto do titular dos dados ou obtidos de outra forma; ao logo de todo o período de tratamento; e, por fim, em momentos específicos enquanto o tratamento está em curso, por exemplo, quando ocorrem violações de dados ou alterações materiais ao tratamento[245]. A transparência é, portanto, essencial no processo de recolha, tratamento e utilização dos dados pessoais. E é fundamental para permitir os direitos de controlo, na medida em que as pessoas em causa não podem exercê-los se não souberem quem são os responsáveis pelo tratamento e os que estão a fazer com os seus dados[246].

As informações sobre o tratamento devem ser fornecidas de forma "concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples", conforme o artigo 12.º do RGPD. Posto isto, os fabricantes dos dispositivos de consumo devem fornecer avisos de privacidade claros e concisos que expliquem como os dados pessoais são recolhidos, tratados e utilizados. Estes avisos de privacidade devem ser acessíveis facilmente e ser de fácil compreensão para os utilizadores, através da utilização de linguagem simples em vez de termos técnicos. As informações essenciais, como os tipos de dados recolhidos, as finalidades do tratamento e os períodos de conservação dos dados, devem todos ser comunicados de forma proeminente aos utilizadores para garantir a transparência e a tomada de decisões informadas[247].

3.1. Privacidade

De modo a garantir a privacidade e proteger os dados pessoais devem ser incorporadas a Proteção de Dados desde a Conceção e por Defeito (PDdCD) no desenvolvimento de dispositivos de consumo da IoT. A principal obrigação da PDdCD consiste na aplicação de medidas adequadas e garantias necessárias que proporcionem uma aplicação eficaz dos princípios da proteção de dados e, consequentemente, dos direitos e liberdades dos titulares dos dados desde a conceção e por defeito[248].

Conforme o número 1 do artigo 25.º do RGPD, "tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento de dados,

[244] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Orientações relativas à transparência na acessão do Regulamento 2016/679, revistas e adotadas pela última vez em 11 de abril de 2018, disponível em https://ec.europa.eu/newsroom/article29/items/622227/en, p. 5.
[245] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Orientações relativas à transparência, *Op. Cit.*, p.6.
[246] URQUHART, Lachlan; *et al*, *Op. Cit.*, p. 22.
[247] GDPR Compliance for Internet of Things (IoT) Devices, *Op. Cit.*
[248] CEPD, Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados deste a Conceção e por Defeito, adotadas em 20 de outubro de 2020, disponíveis em https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en, p. 4.

bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e incluir as garantias necessárias no tratamento, de uma forma que cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados".

Portanto, o artigo 25.º n.º 1 estipula que os responsáveis pelo tratamento devem considerar a privacidade desde a conceção e por defeito logo aquando do planeamento de uma nova operação de tratamento e também continuamente no momento do tratamento, ao reverem com regularidade a eficácia das medidas e das garantias escolhidas[249]. O responsável pelo tratamento deve aplicar as medidas técnicas e organizativas adequadas destinadas a aplicar os princípios da proteção de dados e a integrar as garantias necessárias no tratamento, a fim de cumprir os requisitos e proteger os direitos e as liberdades dos titulares dos dados. Além disso, é exigido aos responsáveis pelo tratamento que tenham conhecimento e se mantenham a par dos avanços tecnológicos[250].

Uma garantia e medidas técnicas ou organizativas podem ser qualquer coisa, pois existem diversos meios que podem adequar-se ao tratamento em questão, dependendo do contexto e dos riscos associados. Alguns exemplos são: a pseudonimização dos dados; o armazenamento dos dados pessoais num formato estruturado e apenas legível por máquina; a possessão de sistemas de deteção de programas maliciosos; dar permissão aos titulares dos dados de intervir no tratamento; o estabelecimento de sistemas de gestão da segurança da informação e da privacidade, obrigando contratualmente os fornecedores a aplicar práticas específicas de minimização dos dados, entre outros[251].

Relativamente ao número 2 do artigo 25.º, este dispõe que "o responsável pelo tratamento aplica as medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados

[249] CEPD, Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados deste a Conceção e por Defeito, *Op. Cit.*, p. 4.
[250] CEPD, Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados deste a Conceção e por Defeito, *Op. Cit.*, p. 8.
[251] CEPD, Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados deste a Conceção e por Defeito, *Op. Cit.*, p. 6-7.

pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares".

O termo "por defeito" no tratamento de dados pessoais refere-se às escolhas a realizar relativamente aos valores de configuração ou às opções de tratamento que são estabelecidas ou estipuladas num sistema de tratamento, tais como uma aplicação de *software*, serviço ou dispositivo. O responsável pelo tratamento deve escolher e ser responsável pela aplicação de definições e opções de tratamento por defeito de forma que apenas o tratamento estritamente necessário para cumprir a finalidade definida e legítima seja realizado por defeito. Portanto, por defeito, o responsável pelo tratamento não deve recolher mais dados do que os necessários, não deve tratar os dados recolhidos mais do que o necessário para as suas finalidades, nem deve armazenar os dados durante mais tempo do que o necessário, sendo obrigado a determinar de forma prévia para que finalidades específicas, explícitas e legítimas os dados pessoais são recolhidos e tratados[252].

A utilização da PDdCD é aplicada pelos responsáveis pelo tratamento, no entanto, outros intervenientes, como subcontratantes e os fabricantes dos produtos, serviços e aplicações, que não são diretamente referidos no artigo 25.º, podem igualmente considerar as orientações úteis na criação de produtos e serviços que estejam em conformidade com o RGPD e que permitem aos responsáveis pelo tratamento de dados cumprir as suas obrigações em matéria de proteção de dados[253].

O artigo 35.º do RGPD introduz a noção de Avaliação do Impacto sobre a Proteção de Dados (AIPD). Uma AIPD consiste num processo criado para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos. Por outras palavras, permite avaliar os riscos para a privacidade e ajudam a identificar e atenuar potenciais preocupações com a recolha dos dados, armazenamento, controlos de acesso e práticas de partilha de dados[254].

O artigo 35.º do RGPD dispõe no seu número 1 que "quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas

[252] CEPD, Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados deste a Conceção e por Defeito, *Op. Cit.*, p. 13.
[253] CEPD, Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados deste a Conceção e por Defeito, *Op. Cit.*, p. 5.
[254] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679, revistas e adotadas pela última vez em 4 de outubro de 2017, disponível em https://ec.europa.eu/newsroom/article29/items/611236/en, p. 4.

singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais".

A AIPD é um meio de gestão de risco que complementa o contexto da Proteção de Dados desde a Conceção, avaliando o risco de cada tratamento relativamente a uma iniciativa específica. Pode ser realizada no caso de uma avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis ou operações de tratamento em grande escala de dados sensíveis, previstos no artigo 9.º do RGPD. Se o resultado de uma AIPD indicar um risco elevado, aumenta a obrigação do responsável pelo tratamento de consultar a autoridade de controlo competente antes de qualquer tratamento[255]. A utilização destas avaliações é importante para compreender como os dispositivos de consumo podem afetar a privacidade do utilizador, ao fornecerem uma análise de risco completa.

As organizações devem estabelecer um procedimento de resposta a violações de dados bem definido para detetar, responder e mitigar violações que envolvam os dispositivos de consumo. Isto engloba o estabelecimento de planos de resposta a incidentes, a realização de auditorias de segurança periódicas e a formação de pessoal para identificar e responder prontamente a potenciais violações. Em caso de violações de dados, as organizações devem seguir os requisitos de notificação de uma violação de dados previstos no artigo 33.º do RGPD, notificando a autoridade de controlo e os indivíduos afetados sem demora injustificada[256].

3.2. Segurança

No contexto da segurança, as obrigações de segurança do tratamento são impostas pelos artigos 25.º e 32.º do RGPD[257]. Deve ser aplicada a Cibersegurança desde a Conceção e por Defeito. A Cibersegurança desde a Conceção significa que todos os produtos conectados e serviços associados devem incorporar funcionalidades de cibersegurança adequadas aos dispositivos IoT de consumo desde uma fase inicial e ao longo de todo o seu processo de conceção e antes de serem colocados no mercado. No caso da Cibersegurança por Defeito significa que, entre a diferentes opções de segurança, as definições de um produto ligado ou serviço associado devem aplicar, como configuração por defeito, a opção mais segura[258]. Por exemplo, se um dispositivo tiver características de conetividade, esta deve ter, por defeito, uma proteção de confidencialidade adequada. De modo a garantir um elevado nível de

[255] RIZOU, Stavroula, *et al, Op. Cit.*, p. 4.
[256] GDPR Compliance for Internet of Things (IoT) Devices, *Op. Cit.*
[257] SILVA, Nuno Sousa e; PINTO, Benedita Cunha, Internet das Coisas (IoT) Alguns Desafios Jurídicos, Estudos de Direito do Consumo, vol. III, Almedina, 2023, p. 584.
[258] ENISA ADVISORY GROUP, Opinion Consumers and IoT Security, 2019, disponível em https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/ag-publications/final-opinion-enisa-ag-consumer-iot-perspective-09.2019, p. 5.

Segurança desde a Conceção e por Defeito, deve ser estabelecido um conjunto adequado de requisitos mínimos de acordo com o nível de cibersegurança necessários para o produto e o serviço associado no seu ambiente específico. E qualquer produto conectado e serviço associado colocado no mercado deve estar vinculado a esses requisitos[259].

A conectividade presente nos dispositivos de consumo da IoT deve ter um interrutor para ligar/desligar. Cada vez mais produtos apresentarão características de conetividade, contudo, nem todos esses produtos precisam de estar ligados para desempenhar as suas funções básicas (por exemplo, um frigorífico). Por conseguinte, é importante garantir que a conetividade dos produtos, quando esta não faz parte da função/objetivo principal do produto, possa ser facilmente desligada. A possibilidade de desligar os produtos ligados deve ser considerada uma caraterística essencial da cibersegurança, porque elimina as vulnerabilidades decorrentes da conetividade dos produtos e reduz a complexidade para o utilizador[260].

O Regulamento (UE) 2019/881 do parlamento europeu e do conselho de 17 de abril de 2019 estabelece um quadro para a criação de sistemas de certificação da cibersegurança na UE, encarregando a ENISA de os preparar, a pedido da Comissão Europeia ou dos Estados-Membros. De acordo com o Considerando 65 do Regulamento, "a certificação da cibersegurança desempenha um papel importante no aumento da confiança e segurança". A introdução de sistemas de certificação para a certificação de vários tipos de produtos de consumo da Internet das Coisas e serviços associados será um processo demorado e, devido ao seu carácter voluntário, a sua aceitação pelas empresas continua a ser pouco clara. Os consumidores que comprarem um produto certificado terão de ser informados sobre a política de apoio à cibersegurança e também receberão recomendações sobre como configurar os seus dispositivos de forma segura. No entanto, a certificação também acarreta o risco de impedir um ritmo rápido de inovação no desenvolvimento de novos produtos/serviços, uma vez que as novas versões podem exigir tempo e custos para uma nova certificação[261].

Além do problema de os dispositivos de consumo da Internet das Coisas carecerem muitas vezes de características de segurança básicas, também não são atualizados ou podem não ser atualizados. Isto expõe os consumidores a numerosos riscos de cibersegurança. Um elemento essencial do princípio da Cibersegurança desde a Conceção e por Defeito é a exigência de que os

[259] ENISA ADVISORY GROUP, *Op. Cit.*, p. 6.
[260] ENISA ADVISORY GROUP, *Op. Cit.*, p. 8-9.
[261] ENISA ADVISORY GROUP, *Op. Cit.*, p. 6.

produtos sejam constantemente atualizados durante o seu tempo de vida útil[262]. Outro elemento importante é a divulgação das vulnerabilidades. Os fabricantes de produtos de consumo IoT e serviços associados devem adotar políticas de gestão das vulnerabilidades com o objetivo de reduzir os riscos de falhas de segurança para os consumidores. Estas políticas devem incluir uma notificação obrigatória aos utilizadores sempre que a vulnerabilidade represente um risco crítico para a sua segurança e/ou proteção. Qualquer notificação deve incluir um conjunto de recomendações simples para minimizar o risco da vulnerabilidade[263].

O Regulamento sobre a Inteligência Artificial estabelece regras que permitem garantir que os dispositivos de consumo IoT que incorporem IA estejam seguros contra ciberataques, protegendo tanto os dados como a funcionalidade dos dispositivos. Conforme o artigo 15.º do regulamento, "os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que alcancem um nível apropriado de exatidão, solidez e cibersegurança e apresentem um desempenho coerente em relação a tais aspetos durante o seu ciclo de vida".

3.3. Discriminação

O RGPD desempenha um papel importante na proteção contra a discriminação na IoT, ao estabelecer princípios claros de proteção de dados, incluindo o direito de acesso, retificação e apagamento dos seus dados, fornecendo aos utilizadores um maior controlo sobre os seus dados, e assim, reduzindo o risco de discriminação. A proibição, pelo RGPD, da tomada de decisões automatizadas, incluindo a definição de perfis, que afetam significativamente os indivíduos, a menos que haja consentimento explícito ou base legal para fazê-lo, ajuda a diminuir risco de discriminação algorítmica, garantindo que os utilizadores não sejam prejudicados por decisões automatizadas injustas ou discriminatórias. Estas preocupações estão refletidas especialmente nos artigos 21.º e 22.º do RGPD. O artigo 21.º (direito de oposição) introduz o direito das pessoas se oporem ao tratamento, incluindo a definição de perfis, em qualquer altura. O artigo 22.º refere-se à tomada de decisões automáticas, incluindo a definição de perfis e estabelece que o "titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar".

Conforme o Considerando 71 do RGPD, "a fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados (...) o responsável pelo tratamento deverá utilizar

[262] ENISA ADVISORY GROUP, *Op. Cit.*, p. 7.
[263] ENISA ADVISORY GROUP, *Op. Cit.*, p. 11.

procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos".

De acordo com a Declaração Europeia sobre os direitos e princípios digitais, "todas as pessoas devem poder beneficiar das vantagens da inteligência artificial, fazendo escolhas próprias e informadas no ambiente digital, estando simultaneamente protegidas contra os riscos e danos para a saúde, segurança e os direitos fundamentais". Para que isto aconteça é necessário "assegurar a transparência sobre a utilização de algoritmos e inteligência artificial e a garantir que as pessoas sejam capacitadas e informadas quando interagem com eles" e "garantir que os sistemas algorítmicos se baseiam em conjuntos de dados adequados para evitar a discriminação ilegal e permitir a supervisão humana dos resultados que afetam as pessoas".

Os consumidores devem receber informações sobre as decisões automatizadas tomadas, ter possibilidade de se opor ao processamento automatizado e de corrigir informações que possam levar a um resultado injusto. A divulgação das informações deve ser realizada de forma clara e não numa linguagem de aviso de privacidade que seja facilmente ignorada, de modo que os consumidores tenham a oportunidade de pôr em prática os seus direitos em tempo útil para evitar danos. Esta abordagem aumenta a transparência e o controlo dos consumidores sobre os seus dados, o que é benéfico tanto para os grupos historicamente discriminados como para os consumidores que, individualmente, possam sofrer de um resultado prejudicial[264].

Uma das principais abordagens para mitigar a discriminação proveniente da Internet das Coisas é, portanto, através da transparência algorítmica. Trata-se de uma opção para melhorar a justiça algorítmica, uma vez que os algoritmos utilizados nos dispositivos de consumo IoT a maior parte das vezes operam de forma opaca, o que resulta em decisões discriminatórias e injustas. Ao estabelecer-se requisitos de transparência, como a divulgação dos critérios e dos dados utilizados nos algoritmos, permite-se uma análise crítica e a identificação de possíveis preconceitos[265].

[264] TSCHIDER, Charlotthe A., *Op. Cit.*, p. 137.
[265] TSCHIDER, Charlotthe A., *Op. Cit.*, p.136.

As atividades de processamento automatizado que representem um "alto risco" para os consumidores devido ao potencial para resultados discriminatórios ou injustos devem ser divulgadas pelos fabricantes antes da recolha de dados e exigir que os utilizadores dos dispositivos IoT consintam explicitamente nas atividades de processamento[266]. Todavia, o tratamento de dados pode também conduzir a preconceitos inesperados porque as potenciais relações entre categorias de dados, muitas vezes reveladas apenas através da agregação e ligação de conjuntos de dados diferentes, podem não ser conhecidas no momento da recolha dos dados. Devem ser implementadas ferramentas como a auditoria algorítmica ética para detetar a discriminação e ser considerados esquemas de auditoria interna para prevenir a discriminação de grupos protegidos, mas também para proteger vítimas de discriminação imprevistas[267].

O Regulamento sobre a IA exige que os algoritmos de inteligência artificial utilizados sejam transparentes e explicáveis. Os dispositivos de consumo que incorporem sistemas de IA devem cumprir determinados requisitos de transparência. Segundo o número 1 do artigo 13.º do Regulamento sobre a IA, "os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira a assegurar que o seu funcionamento seja suficientemente transparente para permitir aos responsáveis pela implantação interpretar os resultados do sistema e utilizá-los de forma adequada". Segundo o Considerado 27, "a transparência significa que os sistemas de IA são desenvolvidos e utilizados de forma a permitir uma rastreabilidade e explicabilidade adequadas, sensibilizando ao mesmo tempo os seres humanos para o facto de estarem a comunicar ou a interagir com um sistema de IA, informando devidamente os responsáveis pela implantação das capacidades e limitações desse sistema de IA e informando as pessoas afetadas dos direitos que lhes assistem".

É importante haver uma avaliação crítica da proveniência dos dados. As organizações responsáveis pelo desenvolvimento de dispositivos devem utilizar dados de qualidade e que sejam diversos, isto é, representativos de várias sociedades, garantindo desta forma a consideração de uma gama ampla de perspetivas e experiências. Portanto, ao criarem os dispositivos, os fabricantes devem ter a equidade como uma consideração central. Conforme o mesmo Considerando 27 do Regulamento da IA, a "diversidade, não discriminação e equidade indica que os sistemas de IA são desenvolvidos e utilizados de forma a incluir diferentes intervenientes e a promover a igualdade de acesso, a igualdade de género e a diversidade cultural, evitando simultaneamente efeitos discriminatórios e enviesamentos injustos que sejam proibidos pelo direito da União ou pelo direito nacional".

[266] TSCHIDER, Charlotthe A., *Op. Cit.*, p. 136.
[267] WACHTER, Sandra, WACHTER, Sandra, The GDPR and the Internet of Things: A Three-Step Transparency Model, Law, Innovation and Technology, 2018, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3130392. p. 20.

Portanto, para proteger os utilizadores, os responsáveis pelo tratamento devem descrever abertamente os possíveis riscos de discriminação dos sistemas da IoT, através da notificação, avaliação do impacto da proteção de dados ou políticas de privacidade, mostrar que tipo de mecanismos estão em vigor para limitar previsões e pressuposições imprecisas ou indesejadas (por exemplo, modelos de consentimento ágeis, opções de exclusão da definição de perfis, transparência algorítmica e ferramentas antidiscriminação na tomada de decisões automatizada e definição de perfis) e, por fim, mostrar planos de emergência transparentes para atenuar os riscos de discriminação se o sistema por comprometido[268].

3.4. Responsabilidade

A responsabilidade é dos requisitos mais importantes do RGPD[269]. A necessidade de introduzir a responsabilização na IoT é motivada pela sua natureza opaca dos fluxos de dados, pelos mecanismos de consentimento inadequados e pela falta de interfaces que permitam ao utilizador controlar o comportamento dos dispositivos[270].

As organizações devem estabelecer linhas claras de responsabilidade, incluindo avaliações regulares, auditorias e formação do pessoal sobre práticas de proteção de dados e privacidade. Como já mencionado, o artigo 25.º do RGPD introduz a Proteção de Dados desde a Conceção e, aí, pressupõe a adoção de medidas técnicas que permitam demonstrar o cumprimento do princípio da responsabilidade. Porém, sendo o RGPD tecnologicamente neutro, não oferece qualquer perspetiva aos fabricantes de sistemas sobre a forma de introduzir a responsabilidade no ecossistema tecnológico em geral ou na IoT, em particular[271]. No caso das AIPD, estas são instrumentos importantes em matéria de responsabilização, uma vez que auxiliam os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas apropriadas para assegurar a conformidade com o RGPD[272].

A utilização de diversas medidas técnicas pode ajudar a permitir a responsabilização no ambiente da Internet das Coisas, ao complementar e reforçar mecanismos de responsabilização, como as normas e leis. Portanto, para alinhar a IoT em movimento com as preocupações legais e regulamentares, os meios técnicos podem auxiliar: no controlo (para determinar o que acontece), ao

[268] WACHTER, Sandra, *Op. Cit.*, p. 15.
[269] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, disponível em https://ec.europa.eu/newsroom/article29/items/612053/en, p. 32.
[270] URQUHART, Lachlan; *et al*, *Op. Cit.*, p. 24.
[271] URQUHART, Lachlan; *et al*, *Op. Cit.*, p. 15.
[272] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) *Op. Cit.*, p. 4.

permitir passos ativos de modo a cumprir obrigações ou exercer direitos; e/ou na auditoria (tornar visível o que acontece ou o que aconteceu), fornecendo provas ou explicações para indicar a natureza dos sistemas e as suas operações em tempo de execução, o que permite ações de resposta e recursos[273].

Os mecanismos de controlo permitem tomar medidas proativas para cumprir as responsabilidades de cada um, enquanto o aumento da transparência sobre os sistemas e os dados fornece informações e provas para uma tomada de informações mais informada, gerindo o funcionamento do sistema, ajudando nas investigações e contribuindo para responsabilizar as entidades. A realização de auditorias regulares permite ajudar a identificar quaisquer lacunas de privacidade e segurança, avaliar a eficácia das medidas implementadas e identificar áreas de melhoria. Ao avaliar e abordar proativamente os riscos de privacidade e segurança, os fabricantes e programadores podem atenuar as potenciais vulnerabilidades e melhorar a conformidade com o RGPD[274].

Como previamente mencionado, muitos dos dispositivos de consumo da IoT são dotados de inteligência artificial, – embutida para realizar determinadas tarefas, como o reconhecimento facial ou de voz, por exemplo – tornando a opacidade uma característica presente nesses dispositivos e sensores associados. Essa opacidade pode dificultar a compreensão do processo de tomada de decisão (o chamado "efeito de caixa negra"). À medida que os algoritmos da IA se tornam cada vez mais avançados e são utilizados em áreas críticas é imperativo criar condições que permitam os seres humanos compreender o que levou o sistema a tomar determinadas decisões algorítmicas. Isso seria particularmente importante para efeitos de fiscalização, pois daria às autoridades a possibilidade de identificarem responsáveis pelos comportamentos e escolhas dos sistemas de IA[275].

Neste sentido, o Regulamento sobre a Inteligência Artificial define mecanismos de responsabilidade para fabricantes. Segundo o Considerando 72 do regulamento, de forma a "dar resposta às preocupações relacionadas com a opacidade e a complexidade de determinados sistemas de IA e ajudar os responsáveis pela implantação a cumprir as obrigações que lhes incumbem por força do presente regulamento, deverá ser exigida transparência aos sistemas de IA de risco elevado antes de serem colocados no mercado ou colocados em serviço. Os sistemas de IA de risco elevado deverão ser concebidos de forma a permitir aos responsáveis pela implantação compreender a forma como

[273] SINGH, Jatinder, *Op. Cit.*, p. 8.
[274] SINGH, Jatinder, *Op. Cit.*, p. 8.
[275] COMISSÃO EUROPEIA, *Op. Cit.*, p. 10.

funciona o sistema de IA, avaliar a sua funcionalidade e compreender os seus pontos fortes e limitações".

3.5. Fluxo de dados transfronteiriços

As informações recolhidas pelos dispositivos IoT de consumo podem ser partilhadas com diversas entidades, como fornecedores de serviços terceiros, plataformas de nuvem e outros dispositivos ligados, sendo complicado gerir estes fluxos de dados, garantir a minimização dos dados e rastrear a base legal para partilha dos dados. A organizações têm, portanto, que compreender de forma clara como é que os dados circulam e estabelecer mecanismos para garantir a conformidade com os princípios do RGPD ao longo do ciclo de vida dos dados[276].

A transferência de dados pessoais para fora da UE é proibida, a não ser que o país que recebe os dados tenha sido considerado "adequado" à legislação europeia em matéria de proteção de dados ou que as empresas disponham de algum mecanismo apropriado. Portanto, caso os dados pessoais recolhidos pelos dispositivos IoT sejam transferidos para países fora da UE/EEE (Espaço Económico Europeu), as organizações devem garantir a existência de salvaguardas adequadas. Isto inclui a utilização de mecanismos como cláusulas contratuais-tipo aprovadas pela UE ou o recurso a regras vinculativas das empresas ou outros mecanismos aprovados para transferências transfronteiriças de dados. As organizações devem também considerar os requisitos legais específicos e os regulamentos de privacidade dos países onde os dispositivos IoT são implantados ou acedidos, garantindo a conformidade com as leis internacionais de proteção de dados aplicáveis. O RGPD, mesmo sendo um regulamento europeu, acaba por ter um impacto internacional[277].

As organizações devem também realizar um inventário de dados e fazer um mapeamento do fluxo de dados. Através da realização de um inventário de dados será possível identificar e documentar os dados pessoais recolhidos, tratados e armazenados pelos seus dispositivos IoT. Isto engloba a compreensão dos tipos de dados, as fontes, os destinatários e as transferências de dados envolvidas. Em relação ao mapeamento do fluxo de dados, ajuda a verificar o movimento dos dados dentro do ecossistema da IoT. O que possibilita às organizações identificar potenciais riscos e garantir a conformidade com os requisitos do RGPD[278].

[276] GDPR Compliance for Internet of Things (IoT) Devices, *Op. Cit.*
[277] RIZOU, Stavroula, *et al, Op. Cit.*, p. 4.
[278] GDPR Compliance for Internet of Things (IoT) Devices, *Op. Cit.*

3.6. Auxílio na aplicação da lei

Ao utilizar dispositivos IoT, a polícia consegue ter uma visão cada vez maior dos locais onde as pessoas vão e o que dizem, o que se torna incompatível com o direito à privacidade, e de outros direitos, como o da liberdade de expressão. Para enfrentar os problemas decorrentes da utilização dos dispositivos de consumo no auxílio na aplicação da lei é essencial garantir a conformidade com o RGPD. As autoridades devem operar dentro dos limites estabelecidos pelo RGPD ao aceder e utilizar dados pessoais nas suas investigações, de modo a garantir que os direitos dos indivíduos estejam protegidos. É importante estabelecer orientações claras sobre a recolha, o armazenamento, o acesso e a retenção de dados para garantir que as informações pessoais e sensíveis sejam adequadamente protegidas e apenas utilizadas para fins legítimos[279]. O uso dos dados provenientes dos dispositivos de consumo deve ser proporcional e justificado para os casos em questão.

Também é importante que haja transparência e responsabilidade relativamente aos algoritmos utilizados, isto compreende a divulgação dos critérios, das fontes de dados e dos processos de tomada de decisão envolvidos. Os profissionais da área jurídica e as partes interessadas devem ter a possibilidade de contestar e questionar os resultados produzidos por estes algoritmos. Além disso, é fundamental dar formação e educação adequada aos profissionais do setor jurídico, agentes relacionados com a aplicação da lei e outras partes interessadas sobre as implicações, limitações e considerações éticas das tecnologias. O que promoverá a tomada de decisões informadas, a utilização responsável e uma melhor compreensão dos potenciais riscos associados aos dispositivos IoT[280].

É também necessário estabelecer mecanismos de auditoria independentes para avaliar a equidade, a exatidão e a transparência dos algoritmos de IA utilizados na aplicação da lei. Estas auditorias devem avaliar o impacto dos algoritmos em diferentes grupos demográficos, identificar preconceitos e sugerir melhorias para mitigar quaisquer efeitos adversos. Apesar dos sistemas que incorporam IA possam automatizar certas tarefas, a supervisão e responsabilização humanas devem continuar a ser centrais no sistema jurídico e de aplicação da lei. Os profissionais humanos devem ser responsáveis pela tomada de decisões críticas, analisar os resultados gerados por IA e resolver qualquer problema ou erro que possa surgir. O quadro jurídico deve definir de forma clara os papéis, as responsabilidades e as limitações dos sistemas de IA nestes domínios[281].

[279] KABIR, Md. Shahin; ALAM, Mohammad Nazmul, *Op. Cit.*, p. 1785.
[280] KABIR, Md. Shahin; ALAM, Mohammad Nazmul, *Op. Cit.*, p. 1786.
[281] KABIR, Md. Shahin; ALAM, Mohammad Nazmul, *Op. Cit.*, p. 1786.

Neste domínio importa a Diretiva (UE) 2016/680 que "estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública". Conforme o artigo 10.º desta Diretiva, o tratamento de dados pessoais que revelem características sensíveis sobre os titulares dos dados "só é autorizado se for estritamente necessário, se estiver sujeito a garantias adequadas dos direitos e liberdades do titular dos dados" e se "for autorizado pelo direito da União ou de um Estado-Membro; se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular; ou se estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados".

O Regulamento sobre a Inteligência Artificial apresenta diversas normas relativas à utilização de ferramentas de IA pelas autoridades responsáveis pela aplicação da lei, uma vez que segundo o considerando 59 considera-se que "tendo em conta o papel e a responsabilidade das autoridades responsáveis pela aplicação da lei, as suas ações que implicam certas utilizações dos sistemas de IA são caracterizadas por um grau substancial de desequilíbrio de poder e podem conduzir à vigilância, detenção ou privação da liberdade de uma pessoa singular, bem como ter outras repercussões negativas nos direitos fundamentais garantidos pela Carta. Em particular, se não for treinado com dados de alta qualidade, não cumprir os requisitos adequados em termos de desempenho, de exatidão ou solidez, ou não tiver sido devidamente concebido e testado antes de ser colocado no mercado ou em serviço, o sistema de IA pode selecionar pessoas de uma forma discriminatória, incorreta ou injusta" e afirma que "a exatidão, a fiabilidade e a transparência são particularmente importantes para evitar repercussões negativas, manter a confiança do público e assegurar a responsabilidade e vias de recurso eficazes".

O não cumprimento das normas do RGPD conduz a potenciais consequências jurídicas e financeiras para as empresas. As autoridades de controlo têm o poder de impor coimas significativas por violações do regulamento e estas sanções podem ter um impacto na estabilidade financeira e nas operações futuras de uma empresa. Por exemplo, podem causar danos à reputação da marca e na confiança dos seus clientes. Além disto, uma situação de incumprimento do RGPD pode atrair um maior controlo regulamentar. Caso uma empresa viole o RGPD, pode levar a investigações e auditorias por parte das autoridades de controlo. As empresas podem ser obrigadas a afetar recursos para colaborar com as autoridades reguladoras, responder a inquéritos e retificar quaisquer problemas de

conformidade identificados. Se o incumprimento se repetir pode resultar numa maior investigação e em ações de aplicação mais rigorosas por parte das entidades reguladoras[282]. A conformidade com o RGPD é da maior importância para os dispositivos de consumo, pois permite garantir a proteção dos direitos de privacidade dos indivíduos e manter a confiança nas tecnologias da Internet das Coisas.

4. Medidas técnicas de proteção da privacidade e dos dados pessoais

De forma a proteger os consumidores, os profissionais informáticos, juntamente com os legisladores e outros decisores políticos devem definir e estimular a aplicação de práticas adequadas de segurança e privacidade. A implementação de práticas recomendadas de conformidade com o RGPD ajuda os fabricantes a produzirem dispositivos de consumo que dão prioridade aos direitos dos utilizadores e à proteção dos seus dados pessoais. Atualmente, como são adequadas diferentes precauções em diferentes condições, não é possível especificar um conjunto de regras universais para garantir a privacidade e segurança da Internet das Coisas. Contudo, é possível especificar um conjunto de princípios gerais ou de boas práticas, isto é, medidas de segurança ou privacidade amplamente aceites pelos profissionais técnicos como benéficas ou necessárias[283].

As Tecnologias de Proteção da Privacidade (PET – *Privacy-Enhancing Technologies*) foram criadas para desenvolver mecanismos técnicos em resposta aos desafios em matéria de privacidade e proteção de dados relacionados às novas Tecnologias da Informação e Comunicação (TIC). Inicialmente, centravam-se na proteção da identidade e nos meios tecnológicos para minimizar a recolha e tratamento dos dados sem perder a funcionalidade de um sistema. Contudo, o âmbito destas tecnologias de proteção da privacidade alargou-se ao longo do tempo para incluir técnicas de criptografia, técnicas de análise que preservam a privacidade, ferramentas de gestão de dados, entre outras[284].

Estas tecnologias podem desempenhar um papel significativo na conformidade dos dispositivos de consumo da IoT com o RGPD. Foi depois da década de 90 que as PET começaram a ser integradas de uma forma mais abrangente nas tecnologias, desde a sua fase inicial de conceção. Isto significa que a privacidade começou a ser considerada desde o início do seu desenvolvimento, tanto na forma como os sistemas são projetados, isto é, na especificação e arquitetura subjacente, como nas práticas comerciais associadas. A privacidade desde a conceção promove uma abordagem holística para gerir os desafios à privacidade que resultam de uma vasta gama de tecnologias emergentes ao longo dos

[282] GDPR Compliance for Internet of Things (IoT) Devices, *Op. Cit.*
[283] CORSER, George, Internet of Things (IoT) security best practices, IEEE Internet Technology Policy Community White Paper, 2017, disponível em https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf, p.2.
[284] GASSER, Urs, *Op. Cit.*, p.203.

seus ciclos de vida[285]. Embora as PET possam não reduzir drasticamente o risco para os consumidores em todas as circunstâncias, quando aplicadas adequadamente a conjuntos de dados holísticos em vez de elementos de dados específicos, as tecnologias de proteção de privacidade reduzirão provavelmente os riscos para a privacidade e de segurança[286].

Entre as várias técnicas de preservação da privacidade propostas pelos investigadores, a criptografia continua a ser a técnica mais promissora e amplamente utilizada para preservar a privacidade[287]. A utilização de algoritmos criptográficos ajuda a proteger a comunicação entre os servidores e dispositivos IoT, de modo a garantir que os dados transmitidos sejam ilegíveis para as pessoas sem autorização. Ou seja, os dados são codificados de tal forma que apenas podem ser lidos pelas partes autorizadas. A encriptação é efetuada para garantir a integridade dos dados[288].

De seguida, irão ser mencionadas algumas boas práticas e tecnologias que poderão ajudar na resolução dos diversos problemas provenientes dos dispositivos de consumo da IoT.

4.1. Autenticação

A autenticação é um dos principais requisitos de segurança na IoT, em que para poderem usar as aplicações e/ou serviços os utilizadores têm que se autenticar. O principal objetivo da autenticação é verificar a identidade de uma entidade. Dependendo do número de fatores ou credenciais necessárias, o processo de autenticação é designado por autenticação de fator único (SFA), autenticação de dois fatores (2FA) ou autenticação multifactor (MFA). Considera-se um fator ou credencial: algo que a entidade é, por exemplo, dados biométricos como a retina, o rosto, impressões digitais; algo que possui, por exemplo, um cartão de identificação; ou algo que conhece, como por exemplo, uma palavra-passe ou PIN[289].

Os dispositivos de consumo IoT não devem utilizar credenciais de nome de utilizador/palavra-passe que sejam fáceis de adivinhar e não devem incluir *back doors* e definições de modo de depuração, isto é, credenciais secretas estabelecidas pelo programador do dispositivo porque, se forem adivinhadas, podem ser usadas para piratear muitos dispositivos. Portanto, cada dispositivo deve ter um nome de utilizador/palavra-passe pré-definidos únicos e, de preferência redefiníveis pelo utilizador. As palavras-passe escolhidas devem ser fortes o suficiente para resistir aos métodos de força bruta,

[285] GASSER, Urs, *Op. Cit.*, p.203-204.
[286] TSCHIDER, Charlotthe A., *Op. Cit.*, p.138.
[287] KANNIAPPAN, Jayashree; BABU, R., An Extensive Survey of Privacy in the Internet of Things, Chapter 4, 2021, disponível em https://www.researchgate.net/publication/352202787_An_Extensive_Survey_of_Privacy_in_the_Internet_of_Things, p. 89-90.
[288] KANNIAPPAN, Jayashree; BABU, R., *Op. Cit.* p. 93.
[289] MÜLLER, Belinda, Authentication, Trends in Data Protection and Encryption Technologies, Springer, 2023, disponível em https://link.springer.com/book/10.1007/978-3-031-33386-6, p. 171-172.

sendo também recomendável a utilização da autenticação de dois fatores, que exige que o utilizador, para além da palavra-passe, utilize também outra forma de autenticação que não dependa do conhecimento do utilizador, como por exemplo, um código aleatório enviado por SMS ou por email[290].

A utilização da autenticação adaptativa ou autenticação baseada em risco é fundamental no caso dos dispositivos de consumo, na qual os algoritmos de aprendizagem automática avaliam continuamente o risco da autenticação sem incomodar o utilizador ao exigir a autenticação. Ou seja, ajusta os requisitos de autenticação com base em fatores contextuais e comportamentos em tempo real e minimiza a frustração do utilizador ao evitar solicitações de autenticação excessivas quando o risco é baixo. Em vez de se aplicar um conjunto fixo de critérios para todos os utilizadores ou situações, a autenticação adaptativa avalia o risco de cada tentativa de acesso e adapta o nível de segurança necessário para permitir ou negar o acesso. Se o risco for elevado, será pedido ao utilizador (ou *hacker*) um *token*[291] multifactor para continuar a ter acesso[292], dificultando o acesso a indivíduos mal-intencionados.

A título de exemplo, no caso de um termóstato inteligente, ajusta dinamicamente o nível de segurança com base no contexto e comportamento do utilizador. Se o membro de uma família ajusta a temperatura da casa usando o seu *smartphone* num horário normal, o acesso é permitido sem a necessidade de autenticação adicional. Caso aconteça em horários fora do comum ou com dispositivos que não são conhecidos, o sistema exige uma autenticação adicional. Esta abordagem oferece uma segurança mais forte sem prejudicar a conveniência e adaptando-se continuamente às condições de uso para proteger os dispositivos contra acessos não autorizados.

4.2. Atualizações de segurança

Muitas vezes as vulnerabilidades de segurança apenas são descobertas depois dos dispositivos serem implementados. Portanto, esses dispositivos devem ser passíveis de correção ou atualização. Porém, atualmente, os vendedores e fabricantes dos dispositivos têm pouco incentivo financeiro para garantir atualizações contínuas dos dispositivos, uma vez que as receitas provêm da venda do dispositivo e não da sua manutenção. Também é prejudicial a tendência de os fabricantes criarem dispositivos que se tornam rapidamente obsoletos, a fim de maximizar o lucro através de vendas contínuas. Além disso, muitas vezes os dispositivos não são concebidos ou configurados de forma

[290] CORSER, George, *Op. Cit.*, p.7.
[291] Um *token* trata-se de uma espécie de certificado digital que é utilizado para identificar, autenticar e autorizar a partilha de informações entre diferentes partes de uma forma segura.
[292] CORSER, George, *Op. Cit.*, p.7.

eficiente para responder a atualizações e não sendo passíveis de atualização, logo, não têm meios para se tornarem seguros[293].

Por conseguinte, é fundamental os fabricantes de dispositivos de consumo darem prioridade ao lançamento atempado de atualizações e correções de *software* para resolver vulnerabilidades de segurança e, assim, proteger os dispositivos contra potenciais violações de dados. A realização destas atualizações de uma forma regular ajuda a garantir que os dispositivos permaneçam seguros, mantendo a integridade e a confidencialidade dos dados pessoais. Os fabricantes de dispositivos devem assumir um papel ativo no fornecimento de informações pormenorizadas sobre as correções e atualizações, bem como sobre os riscos de segurança e as preocupações com a privacidade, garantindo que os utilizadores sejam informados sobre as alterações de política, funcionalidade e segurança. Devem-se manter transparentes e abertos em relação ao ciclo de vida dos dispositivos, especialmente em termos de políticas de serviço e de manutenção, incluindo o período de tempo durante o qual tencionam prestar assistência aos seus dispositivos[294]. Sendo assim, quando um dispositivo de tornar obsoleto e deixar de ser atualizado, o fabricante deve notificar o utilizador e certificar-se de que ele tem conhecimento disso. Todas as partes interessadas que sejam suscetíveis de serem afetadas pela vulnerabilidade em causa também devem ser informadas[295].

4.3. Testes de penetração

Os testes de penetração são fundamentais para a segurança. Trata-se de uma medida preventiva que consiste numa diversidade de ferramentas legítimas que identificam e exploram os pontos fracos de uma organização[296]. Estes testes resumem-se à simulação de um ataque informático a um sistema, rede ou aplicação para identificar e explorar vulnerabilidades de segurança. O objetivo é avaliar a eficácia dos meios de defesa de uma organização. Além disto, permite verificar a capacidade de detetar e responder às tentativas de intrusão. Um teste de penetração avançado procurará todas as lacunas e problemas presentes nos sistemas. Durante estes testes, os profissionais de segurança utilizam diversas ferramentas e técnicas para explorar as vulnerabilidades, que podem incluir exploração de falhas de *software*, tentativas de acesso não autorizado, engenharia social ou outros meios utilizados por indivíduos mal-intencionados. Os testes de penetração devem ser realizados de forma ética e com o consentimento explícito da organização[297]. Estes testes podem, portanto, ser

[293] CORSER, George, *Op. Cit.*, p.4.
[294] CORSER, George, *Op. Cit.*, p.5.
[295] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Parecer 8/2014, *Op. Cit.*, p. 25.
[296] CHOW, Emily, Ethical Hacking & Penetration Testing, IT Research Paper, 2011, disponível em https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=cf5080aad2d688f81a3d2666ed90bcecef18964a , p. 1.
[297] *In* https://www.diazerosecurity.com.br/pt/blog/teste-de-penetracao-ethical-hacking-definicoes-diferencas-usos

realizados para avaliar a segurança dos dispositivos de consumo IoT ao identificar possíveis vulnerabilidades e ajudar a diminuir os ataques informáticos.

4.4. Mecanismos técnicos para realização de auditoria

Para haver responsabilidade é preciso haver transparência. Para tal, os mecanismos técnicos de auditoria têm um papel importante pois ajudam a explicar a natureza dos sistemas. Na realização da auditoria antes da implementação de um dispositivo, existem diversas metodologias de teste e trabalhos em curso sobre métodos de verificação de *software* que garantem que o *software* satisfaz uma especificação. A aplicação dessas metodologias e testes antes da implementação ajudam a identificar e minimizar os riscos, assegurando que os dispositivos sejam seguros e conformes com os requisitos regulatórios. Um exemplo de testes que podem ser realizados são os de simulação[298].

Relativamente à realização de auditoria após a implementação de um sistema ou dispositivo, os registos realizados são úteis para a responsabilização, indicando o que aconteceu e quem esteve envolvido. É feito um registo detalhado de todas as atividades e eventos ocorridos, ao mesmo tempo que é realizado um controlo em tempo real do comportamento e desempenho dos dispositivos IoT. Os registos adequados incluem o fluxo de dados, bem como outros aspetos do funcionamento do dispositivo, abrangendo os contextos em que os processos estavam a funcionar e as políticas de gestão aplicadas. Saber o que registar é um desafio, tal como é regular o acesso às informações de auditoria, especialmente quando os registos são partilhados, uma vez que os próprios dados de auditoria podem ser sensíveis e implicar obrigações[299].

Deste modo, os mecanismos técnicos para a realização de auditoria desempenham um papel importante na garantia de responsabilidade na Internet das Coisas, ao fornecerem os métodos e ferramentas necessárias para verificar, monitorizar e analisar as atividades e o desempenho dos dispositivos de consumo da IoT.

4.5. Métodos de gestão do fluxo de dados

O costume é existir pouca visibilidade ou meios de controlo sobre os dados quando são transferidos ou acedidos por outra parte. Contudo, os métodos mais recentes que acompanham o fluxo de dados de ponta a ponta, para além-fronteiras técnicas e administrativas, são bastante promissores. O registo dos fluxos de dados entre componentes permite identificar quem está envolvido, onde está localizado e o que aconteceu. Isto permite facilitar a responsabilização, ao fornecer provas. Por

[298] SINGH, Jatinder, *Op. Cit.*, p. 9-10.
[299] SINGH, Jatinder, *Op. Cit.*, p. 10.

exemplo, a forma como os dados são recolhidos e subsequentemente processados ou algum comportamento impróprio, como a divulgação injustificada de dados pessoais. Permite também auxiliar na gestão dos riscos, na investigação e na repartição de responsabilidades, revelando quais as interações que conduziram a uma fuga de dados, a um dano físico ou outra falha qualquer[300].

Estão em desenvolvimento diversos trabalhos sobre métodos de gestão proativa dos dados à medida que estes atravessam fronteiras. Estes meios envolvem geralmente a associação de uma política de gestão dos dados e/ou dos seus agentes de processamento, que deve ser aplicada e respeitada de extremo a extremo. Isto ajudará os consumidores e as organizações a gerir os dados ao longo das cadeias de processamento da Internet das Coisas. Estão relacionados os avanços na criptografia homomórfica que permite a computação de dados encriptados. À medida que essas técnicas se tornam mais presentes, é provável que influenciem o fluxo de dados e a política de gestão. Os mecanismos de rastreamento e gestão do fluxo de dados podem ajudar na conformidade da IoT com o RPGD. Contudo, é necessária mais investigação sobre a gestão de registos de comprovação de dados (o que é capturado, o volume, o acesso), a sua apresentação de forma significativa e a especificação e gestão da política, dos contextos e da complexidade dos meios de governar a troca de dados de ponta a ponta[301].

Quanto à criptografia homomórfica, esta é uma técnica de criptografia que permite realizar operações matemáticas em dados encriptados sem a necessidade de os desencriptar primeiro. O resultado obtido será o mesmo que se o cálculo tivesse sido efetuado em texto simples. Por exemplo, num ambiente de computação em nuvem os dados podem continuar encriptados ao mesmo tempo que são processados em ambientes remotos, permitindo que as empresas e os utilizadores mantenham a privacidade dos seus dados. Ou seja, esta técnica permite pedir a um terceiro, como um fornecedor de serviços, que efetue operações sobre os dados que aloja de um cliente, mas sem ver esses dados.

Este tipo de criptografia permite a criação de novos serviços através da eliminação de barreiras à privacidade que impedem a partilha de dados ou aumentando a segurança dos serviços existentes. No caso de dados sensíveis, como informações de saúde presentes em dispositivos de saúde inteligentes, devido a preocupações de privacidade relativas a este tipo de informações, pode ser difícil realizar análises sobre estes dados através de fornecedores de serviços terceiros. Contudo, estas preocupações de privacidade podem ser reduzidas se o prestador de serviços puder operar com os

[300] SINGH, Jatinder, *Op. Cit.*, p. 9.
[301] SINGH, Jatinder, *Op. Cit.*, p. 9.

dados encriptados. E mesmo que o sistema do prestador de serviços seja comprometido, os dados continuarão seguros[302]. Este tipo de criptografia pode ser uma tecnologia transformadora para reforçar a confiança digital[303].

Deste modo, a criptografia homomórfica permite que as organizações tratem dos dados sensíveis recolhidos pelos dispositivos de consumo sem os expor, protegendo a identidade dos indivíduos ao mesmo tempo que permite a análise e a utilização dos dados para fins legítimos. A utilização deste tipo de criptografia permite demonstrar que os dados são mantidos seguros durante todo o seu ciclo de vida.

4.6. Aprendizagem Automática

A Aprendizagem Automática, em inglês, *Machine Learning*, é uma disciplina algorítmica da inteligência artificial que utiliza técnicas para conferir inteligência a dispositivos e computadores. Os métodos de Aprendizagem Automática incluem a Aprendizagem Supervisionada, Não Supervisionada e por Reforço[304]. A AA é importante no contexto da Internet das Coisas porque um ambiente rico em sensores pode produzir dados importantes para a construção de modelos destinados a obter eficiências e a impulsionar a automatização. As técnicas de AA desempenham um papel importante na análise e extração de conhecimentos a partir da enorme quantidade de dados produzidos pelos dispositivos de consumo da IoT[305].

Contudo, a AA traz diversos desafios por ser complexa e opaca. Por isso, abordar os aspetos do efeito caixa negra da aprendizagem automática é uma área de investigação em crescimento. Isto inclui, os já mencionados métodos de auditoria para expor o funcionamento interno dos modelos, processos e razões para a tomada de determinadas decisões e, métodos de controlo para, por exemplo, evitar a parcialidade e a discriminação[306]. Neste aspeto, são relevantes a natureza e as fontes dos dados utilizados para criar os modelos de Aprendizagem Automática, os dados a que os modelos de AA são aplicados e os efeitos das decisões. Isto é importante para os sistemas da IoT porque os dados podem provir e ser processados por uma variedade de fontes e os resultados/decisões da AA podem afetar direta ou indiretamente os outros sistemas" [307].

---

[302] HUBAUX, Jean-Pierre, Homomorphic Encryption, Trends in Data Protection and Encryption Technologies, Springer, 2023, disponível em https://link.springer.com/book/10.1007/978-3-031-33386-6, p. 35-36.
[303] HUBAUX, Jean-Pierre, *Op. Cit.*, p.38.
[304] EL-SOFANY, Hosam, *et al*, Using machine learning algorithms to enhance IoT system security, Scientific Reports, 2024, disponivel em https://www.nature.com/articles/s41598-024-62861-y, p. 7.
[305] EL-SOFANY, Hosam, *Op. Cit.*, p. 5.
[306] SINGH, Jatinder, *Op. Cit.*, p. 10.
[307] SINGH, Jatinder, *Op. Cit.*, p. 11.

As técnicas de AA devem ser utilizadas em conjunto com outras medidas de segurança para oferecer uma segurança completa para os dispositivos de consumo. Por exemplo, a AA pode ajudar a garantir a privacidade dos dados recolhidos pelos dispositivos, pois os seus algoritmos podem ser implementados recorrendo à criptografia homomórfica[308].

A capacidade em tempo real de um sistema de deteção de intrusões de dispositivos IoT é essencial para garantir a segurança. A AA, com o seu rápido desenvolvimento, tem criado diversas ferramentas de deteção e prevenção de intrusões no âmbito dos dispositivos IoT e os seus algoritmos oferecem vantagens únicas quando comparadas com os métodos de deteção tradicionais, pois podem aprender padrões e regras complexos a partir de grandes volumes de dados. Além disso, com a existência de amostras de várias intrusões e comportamento anómalos, é fornecido dados para treino da AA, garantindo o seu melhor desempenho[309].

Os algoritmos de AA podem também aprender o comportamento dos dispositivos IoT de consumo e dos utilizadores e ao analisar os padrões de utilização dos dispositivos conseguem criar perfis de comportamento previsíveis. Deste modo, a AA pode exigir autenticação adicional ou alertar para um acesso ilegítimo quando um dispositivo ou utilizador se desvia consideravelmente do perfil aprendido. Os modelos de AA podem detetar atividade invulgar utilizando dados em tempo real, o que ajuda a detetar violações de segurança, como o acesso não autorizado ou atos maliciosos[310]. Ao treinar modelos de AA para reconhecer padrões ou comportamentos anormais nos dados dos sensores permite-se identificar anomalias ou potenciais violações de segurança[311].

Outra característica, é a possibilidade de a AA melhorar a gestão dos riscos através do fornecimento de informações precisas e atempadas sobre potenciais riscos e perigos. Ao analisar os dados recolhidos de diversos sensores ou câmaras dos dispositivos de consumo, os algoritmos de AA podem prever falhas de equipamento ou necessidades de manutenção e podem analisar dados históricos e em tempo real de sensores da IoT para prever potenciais falhas antes que ocorram. Com a ajuda da AA, as empresas podem tomar medidas preventivas para resolver problemas que possam surgir, evitando períodos de inatividade[312] e reduzindo avarias inesperadas. Além disso, permite aos investigadores analisar o *firmware* e *software* IoT em busca de vulnerabilidades, o que ajuda os

[308] EL-SOFANY, Hosam, *Op. Cit.*, p. 5.
[309] XU, Bayi, *et al*, IoT Intrusion Detection System Based on Machine Learning, Electronics, 2023, disponivel em https://www.mdpi.com/2079-9292/12/20/4289, p. 1-2.
[310] EL-SOFANY, Hosam, *Op. Cit.*, p. 2.
[311] EL-SOFANY, Hosam, *Op. Cit.*, p. 5.
[312] MOFFA, Anthony, A Guide to AI and IoT, 2024, disponível em https://www.ptc.com/en/blogs/iiot/ai-and-iot.

fabricantes a reparar as vulnerabilidades antes da implementação ou a fornecer rapidamente correções de segurança[313].

Contudo, é fundamental a realização de análises detalhadas das decisões algorítmicas para garantir que essas não sejam discriminatórias e desenvolver técnicas que aumentam a transparência desses algoritmos, como a explicabilidade das decisões, que pode ajudar a entender como as decisões são tomadas e, assim, facilitar a responsabilização e evitar a discriminação. A IA explicável (XAI – *Explainable Artificial Intelligence*[314]), é um exemplo de técnicas de AA existentes que podem ser utilizadas para tornar transparente o processo de tomadas de decisões. Estas técnicas podem ser utilizadas para detetar preconceitos presentes nos dados e nos algoritmos, o que tornará mais fácil a correção desses preconceitos e garantir que os dispositivos de consumo funcionem de forma mais justa.

4.7. Computação Multipartida Segura

A Computação Multipartida Segura (CMS), em inglês, *Secure Multiparty Computation*, é uma técnica da área da criptografia que permite que as partes efetuam uma computação conjunta sobre os seus dados de forma a que nenhuma entidade individual tenha de entregar explicitamente um conjunto de dados a qualquer outra[315]. Por outras palavras, permite que um grupo de partes calcule uma função mantendo em conjunto as suas entradas privadas em segredo. Esta técnica possibilita que várias partes colaborem no processamento de dados sem revelar informações sensíveis entre si, sendo útil nos casos em que diferentes organizações necessitam de partilhar dados sem comprometer a privacidade dos utilizadores[316].

Existem muitas situações em que vários dispositivos de consumo têm de comunicar entre si para realizar uma tarefa ou analisar dados, deste modo, a CMS possibilita que partilhem informações de forma segura, garantido que apenas os resultados finais sejam revelados, sem expor os dados originais. Esta técnica permite aos fabricantes dos dispositivos de consumo garantir a conformidade com as normas do RGPD, ao proteger a privacidade dos dados dos utilizadores durante todo o ciclo de vida dos dados.

---

[313] EL-SOFANY, Hosam, *Op. Cit.*, p. 2.

[314] A Inteligência Artificial Explicável (XAI) consiste num conjunto de processos e métodos que permite aos utilizadores humanos compreenderem e confiarem nos resultados criados pelos algoritmos de aprendizagem automática. *In* https://www.ibm.com/topics/explainable-ai.

[315] GASSER, Urs, *Op. Cit.*, p.207.

[316] MERINO, Louis-Henri; CABRERO-HOLGUERAS, José, Secure Multi-Party Computation, Trends in Data Protection and Encryption Technologies, Springer, 2023, disponível em https://link.springer.com/book/10.1007/978-3-031-33386-6, p.89.

4.8. Ambientes de Execução Confiável

Um Ambiente de Execução Confiável, em inglês, *Trusted Execution Environment* (TEE), trata-se de uma área segura de processadores centrais ou dispositivos que permitem a execução segura e isolada de código e processamento de dados[317]. Estes ambientes garantem a confidencialidade e a integridade de dados altamente sensíveis em todos os seus estados, isto é, em repouso, em circulação e em utilização. Os TEE têm o objetivo de proporcionar isolamento em tempo de execução, a entrada/saída fiável e armazenamento seguro dos dados[318]. Quaisquer dados no TEE não podem ser lidos ou alterados por qualquer código fora desse ambiente e os dados apenas podem ser manipulados dentro do TEE por um código devidamente autorizado[319].

Os Ambientes de Execução Confiável podem ser uma forma de solução para os problemas de responsabilidade provenientes da Internet das Coisas, fornecendo as bases para a criação de garantias técnicas em muitos componentes e domínios administrativos. Por exemplo, os TEE podem ajudar na Computação Multipartida Segura, permitindo a verificação de que um determinado código foi executado e que não houve fuga de dados críticos. Isto permite facilitar a análise de Aprendizagem Automática com preservação da privacidade que ocorre através de funções acordadas sem relevar os próprios dados. Em termos gerais, os TEE fornecem as bases para a criação de regimes robustos de auditoria e de aplicação de políticas de controlo[320]. Ou seja, têm uma capacidade única de oferecer um ambiente seguro e isolado onde operações críticas podem ser executadas, monitorizadas e controladas de forma confiável.

Os TEE permitem que as organizações possam realizar auditorias detalhadas das atividades realizadas dentro do TEE, incluindo o acesso aos dados protegidos e as operações realizadas com esses dados. Relativamente às políticas de controlo, os TEE podem ser utilizados para aplicar políticas de controlo de acesso e autorização de forma segura, garantindo que apenas os utilizadores e dispositivos autorizados tenham acesso aos dados protegidos pelo TEE. Isto ajuda as organizações a controlar quem pode aceder aos dados e a garantir que apenas operações autorizadas sejam realizadas. Estas políticas podem ser implementadas dentro do TEE de forma flexível, permitindo que as organizações definam e ajustem as permissões de acesso de acordo com as necessidades específicas do sistema e dos utilizadores. O desenvolvimento desta tecnologia continua a aumentar e

[317] SINGH, Jatinder, *Op. Cit.*, p.11.
[318] SOMMERHALDER, Maria, Trusted Execution Environment, Trends in Data Protection and Encryption Technologies, Springer, 2023, disponível em https://link.springer.com/book/10.1007/978-3-031-33386-6, p.95.
[319] *In* https://learn.microsoft.com/pt-pt/azure/confidential-computing/trusted-execution-environment
[320] SINGH, Jatinder, *Op. Cit.*, p.11.

desempenhará, cada vez mais, um papel importante na garantia do princípio da responsabilidade estabelecido pelo RGPD[321].

Esta tecnologia é essencial para garantir que os dispositivos de consumo operem de uma maneira mais segura e confiável num ambiente que se encontra cada vez mais interligado e suscetível a ameaças de segurança. A título de exemplo, no caso de uma câmara de segurança doméstica inteligente, através de um TEE é possível proteger as transmissões de vídeo ou áudio ao encriptar os dados dentro de um ambiente seguro, o que garante que esses vídeos e áudios gravados sejam inacessíveis a hackers, mantendo a privacidade dos utilizadores e impedindo que as imagens sejam intercetadas ou manipuladas.

4.9. Arquiteturas Federadas

Uma arquitetura federada consiste numa abordagem e computação distribuída que acentua a autonomia e o controlo de componentes individuais, permitindo-lhes trabalhar em conjunto sem problemas. Por outras palavras, é um modelo de integração e colaboração onde múltiplas entidades independentes trabalham juntas, partilhando recursos e informações, mas mantendo a sua autonomia. Permite que cada componente defina as suas próprias regras e decisões pois, cada entidade mantém o controlo sobre os seus próprios dados e funcionalidades. Com uma arquitetura federada, os dispositivos de consumo podem operar de uma forma autónoma em redes locais, reduzindo a dependência a um servidor central. Os dados ao serem processados localmente, em vez de serem enviados para um servidor central, reduz a exposição dos dados durante a sua transmissão e diminui o risco de ataques informáticos. Além disso, permite a adaptabilidade e escalabilidade em resposta à evolução dos requisitos e das tecnologias e facilita a expansão adicionando novas entidades à federação[322].

A implementação de arquiteturas de sistemas mais federados, em que a computação e o armazenamento são empurrados para "mais perto" dos ambientes locais que servem é importante tendo em conta o âmbito da Internet das Coisas. Estão a surgir nuvens mais pequenas ou computação de borda, que podem mediar os dispositivos dentro de uma casa ou de uma divisão. Os fatores que impulsionam a federação incluem as considerações relativas ao desempenho, à latência e à transmissão para servir as interações locais de ambientes físicos com capacidade para a IoT, evitando as despesas gerais das infraestruturas de computação em nuvem mais tradicionais ("distantes")[323].

[321] SINGH, Jatinder, *Op. Cit.*, p.12.
[322] *In* https://www.castordoc.com/data-strategy/federated-architecture.
[323] SINGH, Jatinder, *Op. Cit.*, p. 8.

Com a vantagem da arquitetura distribuída e da proximidade dos utilizadores finais, a computação de borda pode proporcionar uma resposta mais rápida e uma maior qualidade de serviço para as aplicações IoT[324]. Estas arquiteturas federadas são promissoras para melhorar a responsabilização da IoT, permitindo um maior controlo e poder de ação. Por exemplo, uma nuvem dedicada à casa de uma pessoa pode permitir-lhe ditar o seu funcionamento, como os dados são partilhados e que dados são enviados para além das fronteiras locais, por exemplo, para um fornecedor de serviços[325].

4.10. Blockchain

O interesse na tecnologia Blockchain tem vindo a aumentar cada vez mais ao longo dos anos. A Blockchain ou Tecnologia de Registo Distribuído, em inglês, *Digital Ledged Techonology* (DLT), consiste num sistema descentralizado utilizado para gerir uma estrutura de dados baseada em blocos[326]. Esta tecnologia permite implementar livros-razão distribuídos[327], e pode ser aplicada a diversas áreas, sempre que for necessário manter bases de dados de registo de operações sobre bens e serviços de valor reconhecido, efetuadas por múltiplas entidades, sem necessidade de confiança mútua, sem recorrer a intermediários de entidade terceiras, e legíveis e/ou pesquisáveis por todos os membros da comunidade[328].

A implementação da Blockchain na área da IoT permite resolver alguns dos maiores problemas dos dispositivos de consumo. As *Permissioned Blockchains* são um tipo de Blockchain que não são acessíveis ao público, ou seja, apenas podem aceder utilizadores com permissão. Esses utilizadores somente podem executar ações específicas que lhes sejam concedidas e devem autenticar-se através de certificados ou através de outros meios digitais[329]. A utilização desta tecnologia permite fornecer um registo transparente e imutável de transações, garantindo a integridade dos dados e possibilitando que os utilizadores tenham mais controlo sobre as suas informações pessoais. A Blockchain pode ser utilizada para rastrear dados de sensores, assegurar a identidade e autenticação de dispositivos de consumo, realizar transferências seguras de dados e registar todo o tipo de operações[330]. Possibilita o aumento da transparência através de mecanismos de auditoria fiáveis e estabelece um registo "imutável" que pode funcionar além-fronteiras, melhorando a gestão dos fluxos de dados. Esses

[324] LIN, Jie, *et al*, A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications, IEEE Internet of Things Journal, Vol. 4, 2017, disponivel em https://ieeexplore.ieee.org/document/7879243, p.1125.
[325] SINGH, Jatinder, *Op. Cit.*, p. 9.
[326] GASSER, Linus; HUBAUX, Jean-Pierre, Blockchain, Trends in Data Protection and Encryption Technologies, Springer, 2023, disponível em https://link.springer.com/book/10.1007/978-3-031-33386-6, p.141.
[327] Também pode-se designar por livros de registo distribuídos.
[328] BOAVIDA, Fernando; BERNARDES, Mário, Introdução à Criptografia, FCA - Editora de Informática, 2019, p.241-242.
[329] *In* https://www.investopedia.com/terms/p/permissioned-blockchains.asp.
[330] BOAVIDA, Fernando; BERNARDES, Mário *Op. Cit.*, p. 258.

mecanismos de auditoria poderiam registar provas do funcionamento do sistema, do fluxo de dados e das interações dos componentes, potencialmente de ponta a ponta[331]. ´

As particularidades da Blockchain poderá ser, então, uma combinação ideal para a IoT. As características descentralizadas, transparentes e invioláveis da Blockchain podem melhorar a gestão de dados, a gestão de serviços, a gestão de dispositivos e a segurança da IoT[332]. A Blockchain controla, verifica, regista e protege o armazenamento e a utilização dos dados da IoT e a sua fiabilidade e robustez inerente garante a confiança e a segurança dos dados tanto para os utilizadores como para os fornecedores de serviços[333]. Deste modo, garante a privacidade uma vez que apenas as entidades com privilégios adequados podem aceder a blocos específicos de informação. Reduz o risco de ciberataques, pois impedem o roubo e a alteração de todo o tipo de dados. Facilita o controlo de acesso aos dados, estando os dados restringidos às entidades autorizadas. E, por fim, através da rastreabilidade das transações possibilita a total transparência no acesso aos dados, por todas as partes envolvidas[334].

A ideia de dispositivos de consumo da IoT que sejam implementados respeitando a privacidade e segurança, através da utilização destas boas práticas e tecnologias avançadas não é, todavia, fácil. Deve-se reconhecer que, apesar das promessas e potencial destas tecnologias, existem sempre muitos desafios e pressões que podem comprometer os resultados pretendidos. No mundo real, é exigido muitas vezes aos criadores dos dispositivos que reduzam os custos de produção e que criem produtos o mais rapidamente possível, de modo a existir dispositivos mais acessíveis e competitivos no mercado. Como já mencionado anteriormente, isto pode resultar em problemas de privacidade e falhas de segurança. A maior parte das vezes os próprios consumidores tendem a priorizar o custo do dispositivo em detrimento da segurança ao comprar um dispositivo, o que reflete uma combinação de fatores económicos, falta de consciencialização e influências de marketing.

Porém, é possível minorar estes problemas através de incentivos fiscais, por exemplo. Os governos podem oferecer incentivos às empresas para que estas invistam em privacidade e segurança. Uma outra forma, poderá ser através da oferta de programas de educação aos fabricantes dos dispositivos sobre a importância da privacidade e da segurança. Quanto aos consumidores, as

[331] SINGH, Jatinder, *Op. Cit.*, p. 10.
[332] CUI, Pinchen, *et al*, Blockchain in IoT: Current Trends, Challenges, and Future Roadmap, Journal of Hardware and Systems Security, 2019, disponível em https://link.springer.com/article/10.1007/s41635-019-00079-5, p. 359.
[333] CUI, Pinchen, *Op. Cit.*, p. 347.
[334] BOAVIDA, Fernando; BERNARDES, Mário *Op. Cit.*, p. 259.

campanhas de conscientização pública podem ter um impacto positivo ao educar os utilizadores sobre os perigos dos dispositivos de consumo IoT e a melhor maneira de os utilizar.

A utilização destas tecnologias não deixa de ser um ponto crucial para garantir a segurança e a privacidade pois permitem mitigar os riscos associados aos dispositivos de consumo. A pesquisa e o desenvolvimento de novas soluções tecnológicas são essenciais para acompanhar as ameaças em evolução. Além disto, a existência dos regulamentos e de uma fiscalização rigorosa é também outro meio para garantir que todos os dispositivos de consumo atendam aos padrões mínimos de segurança e privacidade. Deve-se assegurar que as organizações que laçam um produto de forma apressada no mercado, em detrimento de medidas de segurança, sejam posteriormente penalizados por isso[335]. Portanto, seria importante que os fabricantes equilibrassem as pressões existentes com a necessidade de criar dispositivos seguros e confiáveis. Através de uma inovação responsável, torna-se possível fomentar a confiança e a satisfação dos consumidores e, deste modo, garantir uma adotação mais rápida e maior da IoT[336].

[335] DEAN, BENJAMIN C., An exploration of strict products liability and the internet of things, Center for Democracy and Technology, 2018, disponível em https://cdt.org/insights/report-strict-product-liability-and-the-internet-of-things/, p.10.
[336] DEAN, BENJAMIN C., *Op. Cit.*, p. 19.

Conclusões

1. De modo a adaptar-se ao contínuo desenvolvimento da tecnologia, o conceito de privacidade teve que evoluir para adequar-se às novas tecnologias. Assim, tornou-se fundamental a necessidade de repensar a "privacidade" surgindo, desta maneira, um novo conceito de vida privada, com o objetivo de abranger novas realidades relacionadas com estas inovações tecnológicas.

2. Para a garantir a privacidade dos indivíduos e proteger os seus dados pessoais dessas contínuas inovações tecnológicas foram implementadas diversas normas, regulamentos e leis, tendo o direito à privacidade e o direito à proteção de dados sido modelado ao longo do tempo. O RGPD foi o regulamento mais importante a ser implementado nesse contexto, pois tem o propósito de prevenir os riscos para os direitos fundamentais decorrentes dos avanços tecnológicos.

3. Das diversas inovações tecnológicas destaca-se, então, a Internet das Coisas, que consiste na ligação à internet de diversos dispositivos. A Internet das Coisas engloba diversos dispositivos de consumo que se encontram cada vez mais presentes no nosso dia-a-dia, como dispositivos de entretenimento, vestíveis, para a casa ou para o carro, que transformaram a vida dos utilizadores através da sua interatividade e automatização e com a promessa de um futuro mais eficiente e com padrões de vida mais elevados. E está previsto que o número de dispositivos continue a aumentar rapidamente ao longo dos anos. Contudo, surgem diversos problemas da utilização desses dispositivos que tem impacto significativo nas nossas vidas e que estão a aumentar cada vez mais à medida que o número de dispositivos "ligados" aumentam. De modo a enfrentar esses problemas verifica-se que é essencial a colaboração entre diferentes partes interessadas, abrangendo empresas, os fabricantes de dispositivos, reguladores e utilizadores, sendo necessário combinar métodos, estratégias e ferramentas disponíveis, que incluam a lei, a tecnologia e práticas profissionais.

4. Garantir a conformidade dos dispositivos de consumo com as diversas normas existentes, em especial com o RGPD, é fundamental para salvaguardar a privacidade, a segurança e proteger os indivíduos dos diversos problemas legais decorrentes da IoT. O RGPD desempenha um papel crucial na proteção dos direitos de privacidade e de proteção de dados no âmbito da Internet das Coisas ao estabelecer diversos princípios fundamentais e direitos dos titulares dos dados. Em primeiro lugar, verifica-se que é essencial a realização da Proteção de Dados deste a Conceção e por Defeito e das Avaliações de Impacto sobre a Proteção de dados para que, respetivamente, sejam aplicadas medidas adequadas que proporcionam uma aplicação eficaz dos princípios da proteção de dados e dos direitos

dos titulares desde a conceção e por defeito e, para avaliar os riscos para a privacidade e ajudar a identificar e atenuar potenciais preocupações com a recolha dos dados, armazenamento, controlos de acesso e práticas de partilha de dados.

5. Nota-se que a transparência é dos requisitos mais importantes, pois, a existência de transparência ajuda a resolver os problemas de responsabilidade, de fluxos de dados transfronteiriços, de discriminação e do auxílio dos dispositivos na aplicação da lei. Com a transparência gera-se confiança nos processos que envolvem os utilizadores, fazendo que estes os compreendem e, se necessário, que se opunham a esses processos. Além disso, a transparência é fundamental para que os indivíduos exerçam o seu direito de controlo e, quando devidamente informados sobre os tipos de dados recolhidos e sobre a finalidade do tratamento, garante-se uma tomada de decisões informada. Através da divulgação dos critérios e dos dados utilizados e da sua origem, permite-se realizar uma análise crítica e a identificação de preconceitos existentes. Portanto, a transparência permite que os utilizadores compreendam como os seus dados são recolhidos, utilizados e protegidos, promovendo, assim, uma relação de confiança com os fabricantes e prestadores de serviços.

6. Além disso, é importante que os consumidores tenham consciência dos riscos da utilização dos dispositivos de consumo de modo a fazerem decisões informadas, por isso, devem ser educados sobre os riscos destes produtos para garantir a sua segurança. E se utilizarem estes dispositivos devem ter cuidados e conhecimento de quais os seus direitos e de como os usar corretamente de forma a garantir a sua privacidade e proteger os seus dados pessoais.

7. A implementação de práticas recomendadas de conformidade com o RGPD ajuda os fabricantes a produzirem dispositivos de consumo que dão prioridade aos direitos dos utilizadores e à proteção dos seus dados pessoais. E foi neste sentido que foram criadas diversas Tecnologias de Proteção da Privacidade de forma a dar resposta aos desafios em matéria de privacidade e proteção de dados e que foram integradas nas tecnologias desde a sua fase inicial de conceção. Enquanto algumas destas tecnologias ainda se encontram em desenvolvimento, outras já são recomendadas como as melhores práticas a serem implementadas[337].

8. Nesta dissertação são mencionadas algumas boas práticas e tecnologias que podem ser aplicadas para proteger a privacidade e os dados pessoais. Apesar dos avanços já realizados, muitas técnicas ainda estão por descobrir e por aplicar. A maioria das medidas técnicas mencionadas podem ser aplicadas desde o início e por defeito nos dispositivos, cumprindo o princípio da Proteção de Dados

[337] GASSER, Urs, *Op. Cit.*, p.207.

Pessoais desde a Conceção ou por Defeito. Deste modo, é garantida a conformidade com o RGPD, o que contribui para o aumento da confiança dos consumidores na Internet das Coisas.

9. As tecnologias emergentes, como a Blockchain e a AA, oferecem um potencial significativo para combater os problemas dos dispositivos de consumo da Internet das Coisas. Contudo, à medida que estas evoluem, é fundamental adaptar e alinhar simultaneamente as regulamentações nacionais e internacionais, pois ao passo que as tecnologias se desenvolvem aparecem novos desafios. Tendo o ambiente regulamentar em torno da privacidade e da proteção de dados de se adaptar e progredir continuamente para abordar os problemas emergentes. Foi neste sentido que para acompanhar o contínuo desenvolvimento da IA, foi aprovado o Regulamento sobre a IA, no qual as suas normas poderão ter um impacto significativo no contexto da Internet das Coisas, uma vez que muitos dispositivos de consumo IoT incorporam sistemas de Inteligência Artificial.

10. É importante admitir que apesar da existência de diversas leis e regulamentos e de várias tecnologias que têm como objetivo garantir a privacidade e segurança, no mundo real, não é uma tarefa fácil. Existem sempre desafios e pressões que colocam em causa o propósito dessas leis e tecnologias. Contudo, podem ser realizados esforços de modo a minimizar esses problemas através de fiscalizações, incentivos fiscais e educação dos fabricantes e consumidores.

11. Uma vez que a Internet das Coisas funciona a um nível mundial, considera-se a harmonização das leis de privacidade e proteção de dados fundamental. As organizações que criam e implementam dispositivos da IoT em diversas jurisdições têm que navegar em quadros jurídicos diferentes e, por isso, devem ser realizados esforços para a realização de uma harmonização global das leis privacidade e proteção de dados. As organizações devem acompanhar os desenvolvimentos internacionais e ajustar as suas estratégias de conformidade com o RGPD para se alinharem com as normas de privacidade globais. Portanto, é essencial o estabelecimento de normas internacionais para a privacidade e segurança dos dispositivos, facilitando a conformidade e a interoperabilidade entre os diferentes sistemas e regulamentações[338]. É neste sentido que o artigo 50.º do RPGD defende uma "cooperação internacional no domínio da proteção de dados pessoais".

12. Conclui-se que a existência de dispositivos de consumo da Internet das Coisas que cumpram de forma rigorosa as diversas normas e leis existentes, e em especial, os requisitos do RGPD e que sejam implementados utilizando medidas tecnológicas adequadas permite garantir a privacidade, a segurança e proteger os utilizadores dos restantes problemas da IoT. Assim, promove-se a confiança

[338] GDPR Compliance for Internet of Things (IoT) Devices, *Op. Cit.*

dos consumidores nesta tecnologia. Ao mesmo tempo, é importante a existência de um equilíbrio entre a privacidade e segurança com a inovação, garantindo que a Internet das Coisas seja uma tecnologia que possa continuar a evoluir e contribuir para um futuro mais conectado e confiável.

Bibliografia

ABDI, Noura, *et al*, Privacy Norms for Smart Home Personal Assistants, 2021, disponível em https://dl.acm.org/doi/abs/10.1145/3411764.3445122;

ALMEIRA, José Maria Fernandes, Breve história da INTERNET, disponível em https://repositorium.sdum.uminho.pt/bitstream/1822/3396/1/INTERNET.pdf;

ANTUNES, Luís Filipe, A Privacidade no Mundo Conectado da Internet das Coisas, *in* Forum de Dados, n.º 2, 2016;

BOAVIDA, Fernando; BERNARDES, Mário, Introdução à Criptografia, FCA - Editora de Informática, 2019;

BUTTARELLI, Giovanni, Inteligência Artificial, Robótica, Privacidade e Proteção de Dados, Forum de Dados, n.º 4, 2017

CANOTILHO, Gomes; MOREIRA, Vital, Constituição da República Portuguesa Anotada, Volume I, Coimbra Editora, 2007;

CEPD, Diretrizes 05/2020 relativas ao consentimento na acessão do regulamento 2016/679, adotadas em 4 de maio de 2020, disponível em https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt;

CEPD, Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados deste a Conceção e por Defeito, adotadas em 20 de outubro de 2020, disponíveis em https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en;

CHANDER, Anupam, The internet of things: both goods and services, World Trade Review, vol. 18, 2019, disponível em https://doi.org/10.1017/S1474745619000089;

CHIKE, Patrick Chike, The Legal Challenges of Internet of Things, 2017, disponível em https://www.researchgate.net/publication/322628457_The_Legal_Challenges_of_Internet_of_Things;

CHOW, Emily, Ethical Hacking & Penetration Testing, IT Research Paper, 2011, disponível em https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=cf5080aad2d688f81a3d2666ed90bcecef18964a;

COMISSÃO EUROPEIA, Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da internet das coisas e da robótica, 2020, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0064;

CONSELHO DA EUROPA, Digital Citizenship Education Handbook, 2022, disponível em https://www.coe.int/en/web/digital-citizenship-education/-/2022-edition-of-the-digital-citizenship-education-handbook;

CORCORAN, Peter, The Internet of Things, why now, and what's next?, IEEE Consumers Electronics Magazine, 2015, disponível em https://ieeexplore.ieee.org/document/7353271;

CORDEIRO, António Barreto Menezes, Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019, Edições Almedina, 2022;

CORREIA, Victor, Da Privacidade, Significado e Valor, Edições Almedina, 2018;

CORREIA, Victor, Sobre o Direito à Privacidade, O Direito, ano 146, n.º 1, 2014, disponível em https://www.academia.edu/es/6106718/Sobre_o_direito_à_privacidade;

CUI, Pinchen, *et al*, Blockchain in IoT: Current Trends, Challenges, and Future Roadmap, Journal of Hardware and Systems Security, 2019, disponível em

https://link.springer.com/article/10.1007/s41635-019-00079-5;

DEAN, BENJAMIN C., An exploration of strict products liability and the internet of things, Center for Democracy and Technology, 2018, disponível em https://cdt.org/insights/report-strict-product-liability-and-the-internet-of-things/;

DUBOIS, Daniel J., *et al*, When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers, Proceedings on Privacy Enhancing Technologies, vol 4, 255–276, 2020 disponível em https://par.nsf.gov/biblio/10192512;

EL-SOFANY, Hosam, et al, Using machine learning algorithms to enhance IoT system security, Scientific Reports, 2024, disponivel em https://www.nature.com/articles/s41598-024-62861-y;

ELVY, Stacy-Ann, Privacy and Security in the Connected Era, A Commercial Law of Privacy and Security for the Internet of Things, disponível em https://doi.org/10.1017/9781108699235.002;

FARINHO, Domingos Soares, Intimidade Da Vida Privada e Media no Ciberespaço, Edições Almedina, 2006;

FILHO, Mauro Faccioni, Internet das Coisas, UnisulVirtual, 2016, disponível em https://www.researchgate.net/publication/319881659_Internet_das_Coisas_Internet_of_Things;

FUSTER, Gloria González, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer, 2014;

GARCIA Marques; MARTINS Lourenço, Direito da Informática, Edições Almedina, 2000;

GASSER, Urs, Futuring Digital Privacy, Reimaging the Law/Tech interplay, Big Data and Global Trade Law, 2021, disponivel em https://doi.org/10.1017/9781108919234.013;

GREENGARD, Samuel, The Internet of Things, The MIT Press Essencial Knowledge Series, 2021;

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679, revistas e adotadas pela última vez em 4 de outubro de 2017, disponível em

https://ec.europa.eu/newsroom/article29/items/611236/en;

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Orientações relativas à transparência na acessão do Regulamento 2016/679, revistas e adotadas pela última vez em 11 de abril de 2018, disponível em https://ec.europa.eu/newsroom/article29/items/622227/en;

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, disponível em https://ec.europa.eu/newsroom/article29/items/612053/en;

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Parecer 8/2014 sobre os recentes desenvolvimento na Internet das Coisas, adotado em 16 de setembro de 2014, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_pt.pdf;

Grupo de trabalho internacional sobre a proteção de dados nas telecomunicações, Dispositivos inteligentes para crianças e os riscos para a privacidade, Fórum da Proteção de Dados, n.º6, 2019;

INTERNET SOCIETY, “The Internet of Things: An Overview. Understanding the issues and Challenges of a More Connecter World”, 2015, disponível em

https://www.semanticscholar.org/paper/THE-INTERNET-OF-THINGS-%3A-AN-OVERVIEW-Understanding-Rose-Eldridge/be5012a06734594bf3d06a0563c9c7619e5d906e;

KABIR, Md. Shahin; ALAM, Mohammad Nazmul, IoT, Big Data and AI Applications in the Law Enforcement and Legal System: A Review, International Research Journal of Engineering and Technology, vol. 10, 2023, disponível em

https://www.researchgate.net/publication/371155772_IoT_Big_Data_and_AI_Applications_in_the_Law_Enforcement_and_Legal_System_A_Review;

KANNIAPPAN, Jayashree; BABU, R., An Extensive Survey of Privacy in the Internet of Things, Chapter 4, 2021, disponível em

https://www.researchgate.net/publication/352202787_An_Extensive_Survey_of_Privacy_in_the_Internet_of_Things;

KARALE, Ashwin, The challenges of IoT addressing security, ethics, privacy, and laws, Internet of Things, vol. 15, 2021, disponível em

https://www.sciencedirect.com/science/article/pii/S2542660521000640;

KAUR, Jashanpreet, Safeguarding privacy in internet of things, Mohd Abdul Hafi, 2022;

KHARE, Shivanjali; TOTARO, Michael, Big Data in IoT, 2019, disponível em https://ieeexplore.ieee.org/abstract/document/8944495;

KLWINBERG, Jon, el al, Discrimination in the Age of Algorithms, Journal of Legal Analysis, Vol. 10, 2018, disponível em

https://academic.oup.com/jla/article/doi/10.1093/jla/laz001/5476086?login=false;

LEITE, Leandro Rogério Corrêa, Internet das Coisas (IoT): Vulnerabilidades de Segurança e Desafios, 2019, disponível em

http://ric.cps.sp.gov.br/bitstream/123456789/3978/1/20192S_LEITELeandroRogérioCorrêa_OD0763.pdf

LIN, Jie, *et al*, A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications, IEEE Internet of Things Journal, Vol. 4, 2017, disponivel em https://ieeexplore.ieee.org/document/7879243, p.1125.

LUTZ, Christoph; NEWLANDS, Gemma, Privacy and smart speakers: A multi-dimensional approach, the information society, vol. 37, no. 3, 147–162, 2021, disponível em https://www.tandfonline.com/doi/full/10.1080/01972243.2021.1897914;

Manual da Legislação Europeia sobre Proteção de Dados, abril de 2018, disponível em https://fra.europa.eu/pt/publication/2022/manual-da-legislacao-europeia-sobre-protecao-de-dados-edicao-de-2018

MONIZ, Graça Canto, Manual de Introdução à Proteção de Dados Pessoais, Edições Almedina, 2023;

MOREIRA, Teresa, A privacidade dos trabalhadores e as novas tecnologias de informação e comunicação : contributo para um estudo dos limites do poder de controlo eletrónico do empregador, Tese de Doutoramento, Universidade do Minho, 2010, disponível em

https://repositorium.sdum.uminho.pt/handle/1822/10470

MOTA PINTO, Paulo, "A proteção da vida privada na jurisprudência do Tribunal Constitucional", disponível em https://www.tribunalconstitucional.pt/tc/conteudo/files/textos/textos0202035.pdf

MULDER, Valentin, *et al*, Trends in Data Protection and Encryption Technologies, Springer, 2023, disponível em https://link.springer.com/book/10.1007/978-3-031-33386-6;

OFFICE OF THE PRIVACY COMMISION OF CANADA, The internet of things, An introduction to privacy issues with a focus on the retail and home environments, 2016, disponível em https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/iot_201602/;

PEPPET, Scott R., Regulating the Internet of Things: first steps towards managing Discrimination, Privacy, Security & Consent, Forthcoming Texas Law Review, 2014, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074;

REQUIÃO, Maurício; COSTA, Diego Carneiro, Discriminação algorítmica: ações afirmativas como estratégia de combate, 2022, disponível em

https://www.academia.edu/97882347/Discriminação_algorítmica_ações_afirmativas_como_estratégia_de_combate;

RIZOU, Stavroula, et al, GDPR interference with next generation 5G and IoT networks, IEEE Access, vol. 8, 2020, disponível em https://ieeexplore.ieee.org/document/9110555;

SIEGEL, Jeremy, When the Internet of Things Flounders: looking into GDPR-Esque Security for IoT devices in the United States from the consumers' perspective, Journal of High Technology Law, vol. 20, n.º1, 2020, disponível em https://bpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/5/1153/files/2020/01/Siegel-Final-PDF.pdf;

SILVA, Diana; MALTA, Mariana; VASCONCELOS, Paulo, Desafios da Privacidade nos Assistentes Virtuais Pessoais, 2022, disponível em https://www.iscap.pt/ebusiness-rj/index.php/mne-rj/article/view/194;

SILVA, Nuno Sousa e; PINTO, Benedita Cunha, Internet das Coisas (IoT) Alguns Desafios Jurídicos, Estudos de Direito do Consumo, vol. III, Almedina, 2023, pp. 565-599.

SINGH, Jatinder, *et al*, Accountability in the Internet of Things (IoT): Systems, law & ways forward, *in* Computer, vol. 51, 2018, disponível em https://ieeexplore.ieee.org/document/8423131;

SOUSA, Daniela Rodrigues de, A Proteção de Dados Pessoais do Consumidor, Estudos de Direito do Consumo, vol. III, Almedina, 2023, pp. 247-291.

SPENDER, A.; BULLEN, L., *et al*, Wearables and the internet of things: considerations for the life and health insurance industry, in British Actuarial Journal, vol. 24, 2019, disponível em https://www.cambridge.org/core/journals/british-actuarial-journal/article/wearables-and-the-internet-of-things-considerations-for-the-life-and-health-insurance-industry/56919A6812F5439BD4C49AC758C7CE63,

TSCHIDER, Charlotthe A., Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age, Denver Law Review, vol. 96, 2018, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3129557#;

TURUNEN, Markku, *et al*, Interaction and Humans in Internet of Things, 2015, disponível em https://www.researchgate.net/publication/281643568_Interaction_and_Humans_in_Internet_of_Things;

URQUHART, Lachlan, *et al;* Demonstrably doing accountability in the Internet of Things, International Journal of Law and Information Technology, vol. 27, 2018, disponível em https://doi.org/10.1093/ijlit/eay015;

VÉLIZ, Carissa, "Privacidade é poder, por que razão e como devemos recuperar o controlo dos nossos dados, Bertrand Editora, 2022;

WACHTER, Sandra, The GDPR and the Internet of Things: A Three-Step Transparency Model, Law, Innovation and Technology, 2018, disponível em

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3130392;

XU, Bayi, et al, IoT Intrusion Detection System Based on Machine Learning, Electronics, 2023, disponivel em https://www.mdpi.com/2079-9292/12/20/4289;