Privacy and Data Protection Magazine

REVISTA CIENTÍFICA NA ÁREA JURÍDICA

N.º 08 – 2025
ONLINE

Direção Executiva
Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez

Universidade Europeia

PRIVACY AND DATA PROTECTION CENTRE

Privacy and Data Protection Magazine

Data: 2025

Publicações: anual

ESTATUTO EDITORIAL

1.º Objeto. A Revista Privacy and Data Protection Magazine é uma publicação científica que tem por objeto a Proteção de Dados Pessoais; Direitos Fundamentais; Direito de Propriedade Intelectual; Direito do Consumo; Direito da Saúde, Direito Digital e Inteligência Artificial.

2.º Princípios Deontológicos. Tudo o que, nesta Revista, se venha a publicar, obedecerá rigorosamente à metodologia científica do Direito e à sua praxis quotidiana, sem quaisquer ingredientes políticos ou religiosos. Assim, será sempre no respeito dos princípios deontológicos da imprensa periódica e da ética profissional que se pautará a orientação desta Revista.

3.º Propriedade. É proprietária da Revista a ENSILIS – Educação e Formação, Unipessoal Lda, detentora da Universidade Europeia, com sede na Quinta do Bom Nome, Estrada da Correia, n.º 53, 1500-210.

4.º Edição. A edição da Revista está a cargo da Universidade Europeia.

5.º Objetivo. A Revista visa contribuir para a criação e transmissão do conhecimento científico na área da Proteção de Dados Pessoais; Direitos Fundamentais; Direito de Propriedade Intelectual, Direito do Consumo, Direito da Saúde, Direito Digital e Inteligência Artificial.

6.º Direção Executiva e Editorial. A Revista é dirigida por uma diretora: Cristina Maria de Gouveia Caldeira, que é co-coordenadora do Privacy and Data Protection Centre, email: centro.dataprotection@universidadeeuropeia.pt

7.º Colaborações. A Revista publica em acesso aberto artigos doutrinários e outros estudos, legislação e jurisprudência comentadas e recensões de obras científicas.

8.º Conselho Editorial. Após revisão por pares, a seleção dos trabalhos a publicar é feita por um Conselho Editorial integrados por 6 especialistas de reconhecido mérito.

9.º Periodicidade. A Revista terá periodicidade anual.

10.º Secções. A Revista compreende quatro secções: (i) Artigos Doutrinários; (ii) Outros Estudos; (iii) Legislação e Jurisprudência Comentadas; (iv) Recensões.

11.º Sistema de Publicação. A Revista com publicação online em três línguas (português, inglês e espanhol), pretende ter um alcance nacional e internacional.

Universidade Europeia

PRIVACY AND DATA PROTECTION CENTRE

Ficha Técnica

Título
Privacy and Data Protection Magazine

Subtítulo
Revista Científica na Área Jurídica

Número
008

Ano de Publicação
2025

Afiliação
Privacy and Data Protection Centre Universidade Europeia

Conselho Editorial
Alexandra Chícharo das Neves
Ana Cristina Roque
Eduardo Vera-Cruz
Ingo Wolfgang Sarlet
Luís Filipe Coelho Antunes
Pedro Barbas Homem

Autores
Alexandre Sousa Pinheiro
Ana Felícia Santos
André Filipe da Fonseca Carreto Lopes
César Edgar Machado Penetro
Cláudia Alves Pratas
Cristina Maria de Gouveia Caldeira
Daniel Becker & Ludmilla Campos
Dennis Verbicaro
Duarte Rodrigues Nunes
Inês Filipa Leal Alverca
Isabelly Ribeiro Falcão Mendes
João Mateus
José Manuel Anjos Correia
Lizeth Dinis Simão
Lurdes Dias Alves
Maria Cláudia Cachapuz
Manuel David Masseno
Mesla L. Bambi
Oscar Valente Cardoso
Pedro Martins Proença
Renata Guilardi de Oliveira Castro
Rita Maria Colaço Neves
Suellen Assunção Abbade
Thamara Consul Gavazza

Prefácio
Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez

Direção Executiva
Cristina Maria de Gouveia Caldeira

ISSN
2184-920X

Número de Registo
127600

Propriedade
ENSILIS - Educação e Formação, Unipessoal, Lda., detida a 100% por Omnymission, Unip. Lda.

Chief Executive Officer
Carlos Bertrán

NIPC/NIF
504 669 788

Editor e Redação
Universidade Europeia, Quinta do Bom Nome, Estrada da Correia, 53, 1500-210, Lisboa

Índice

Prefácio 7

I Artigos Doutrinários 9

Novas reflexões sobre a esfera pública em tempos de novas tecnologias 10
Maria Cláudia Cachapuz

Dos ataques de ransomware na Convenção de Budapeste sobre o Crime Cibernético - um ensaio de qualificação alternativa, desde Portugal - 32
Manuel David Masseno

Inteligência Artificial e Arbitragem: Um Breve Estudo Sobre a Instrumentalização da Tecnologia em Procedimentos Arbitrais.....50
Daniel Becker e Ludmilla Campos

A conservação e utilização probatória de metadados após a Lei n.º 18/2024, de 5 de fevereiro 65
Rodrigues Nunes

Desafios de Privacidade e Segurança no Setor Bancário: Uma Abordagem de Proteção de Dados 90
Lurdes Dias Alves

Além do Rótulo: Ética, IA e Off-Label no Tratamento das Doenças Neurodegenerativas.....114
Inês Filipa Leal Alverca

Consentimento informado e consentimento para o tratamento de dados pessoais na área da saúde: sinônimos ou institutos diferentes? 135
Thamara Consul Gavazza

Espaço Europeu de Dados de Saúde: Big Data de todos para todos. A oportunidade e obrigatoriedade da Inovação e Investigação.....163
César Edgar Machado Penetro

Moldura Ética da Inteligência Artificial aplicada à Área da Saúde 181
Rita Maria Colaço Neves

Consentimento ético em pesquisas científicas: a influência da literacia jurídica e digital na autonomia do titular de dados 207
Isabelly Ribeiro Falcão Mendes

A Inteligência Artificial e a Integridade das Decisões Clínicas: Desafios Éticos e Normativos 223
André Filipe da Fonseca Carreto Lopes

Direito ao Esquecimento na Sociedade em Rede: Contexto das Plataformas Digitais 243
José Manuel Anjos Correia

Concorrência Desleal: à luz dos Princípios Bíblicos.....260
Mesla L. Bambi

A impressão digital do culto religioso: da proteção jurídica da imagem dos menores online 278
Cláudia Alves Pratas

Direitos da propriedade industrial: Tutela da inovação no ordenamento jurídico português.....294
Lizeth Diniz Simão

A metamorfose do Direito global: uma análise sobre o seu sentido atual e/ou virtual 318
Suellen Assunção Abbade

Eficácia Diagonal da Proteção de Dados Pessoais.....337
Oscar Valente Cardoso

II LEGISLAÇÃO E JURISPRUDÊNCIA COMENTADA 353

Videovigilância em Contexto Laboral Comentário ao Acórdão do TRE de 26 de setembro de 2024.....353
Pedro Martins Proença e Manuel David Masseno

Considerações sobre o Regulamento dos Serviços Digitais - Regulamento (UE) 2022/2065 de 19 de outubro de 2022 370
Renata Guilardi de Oliveira Castro

III OUTROS ESTUDOS 375

Blockchain como Pilar para um Sistema Global de Propriedade Intelectual: Uma Abordagem Descentralizada e Universal.....376
João Mateus e Cristina Maria de Gouveia Caldeira

Dados pessoais – "o petróleo do século XXI" – os desafios e as ameaças à luz do cibercrime.....396
Ana Felícia Canilo Santos

IV Recensões 430

Prefácio

O presente número da revista *Privacy and Data Protection Magazine* afigura-se particularmente rico, abrangente e multifacetado, tanto no que concerne aos objetos materiais dos vários artigos como no que tange às perspetivas analíticas adotadas pelos distintos autores.

Nesta publicação, manifestam-se, de forma particularmente expressiva, as várias linhas de força temáticas que vêm traçando o rumo, de cinco anos, do Privacy and Data Protection Centre (PDPC) em que a nossa revista se insere: (i) Direitos Fundamentais e Cidadania Digital; (ii) Propriedade Intelectual, Direito da Saúde e Inovação; (iii) Proteção de Dados e Inteligência Artificial; (iv) Cibersegurança, Cibercrime, Ciberdefesa.

A mera apresentação dos títulos dos artigos é, em si mesma, eloquente: Novas reflexões sobre a esfera pública em tempos de novas tecnologias (Maria Cláudia Cachapuz); Dos ataques de ransomware na Convenção de Budapeste sobre o Crime Cibernético - um ensaio de qualificação alternativa, desde Portugal (Manuel Masseno); Algorithmic determinism: a real threat to consumer individuality (Dennis Verbicaro); Inteligência Artificial e Arbitragem: um breve estudo sobre a Instrumentalização da Tecnologia em Procedimentos Arbitrais (Daniel Becker & LudmillaCampos). A conservação e utilização probatória de metadados após a Lei n.º 18/2024, de 5 de fevereiro (Duarte Rodrigues Nunes); Desafios de Privacidade e Segurança no Setor Bancário: Uma Abordagem de Proteção de Dados (Lurdes Alves); Além do Rótulo: Ética, IA e Off-Label no Tratamento das Doenças Neurodegenerativas (Inês Alverca); Consentimento informado e consentimento para o tratamento de dados pessoais na área da saúde: sinônimos ou institutos diferentes? (Thamara Consul Gavazza); Espaço Europeu de Dados de Saúde: Big Data de todos para todos: a oportunidade e obrigatoriedade da Inovação e Investigação (César Edgar Penetro); Moldura Ética da Inteligência Artificial aplicada à Área da Saúde (Rita Maria Neves); Consentimento ético em pesquisas científicas: a influência da literacia jurídica e digital na autonomia do titular de dados (Isabelly Ribeiro Mendes); A Inteligência Artificial e a Integridade das Decisões Clínicas: Desafios Éticos e Normativos (André Filipe Lopes); Direito ao Esquecimento na Sociedade em Rede: Contexto das Plataformas Digitais (José Manuel Correia); Concorrência Desleal: à luz dos Princípios Bíblicos (Mesla Bambi); A impressão digital do culto religioso: da

proteção jurídica da imagem dos menores online (Cláudia Alves Pratas); Direitos da propriedade industrial: Tutela da inovação no ordenamento jurídico português (Lizeth Simão); A metamorfose do Direito global: uma análise sobre o seu sentido atual e/ou virtual (Suellen Assunção Abbade); A Eficácia Diagonal da Proteção de Dados Pessoais (Oscar Valente Cardoso).

A secção dedicada à "Legislação e Jurisprudência Comentada" oferece ao leitor duas temáticas atuais: *Videovigilância em Contexto Laboral - Comentário ao Acórdão do TRE de 26 de setembro de 2024* (Pedro Martins Proença); "Considerações sobre o Regulamento dos Serviços Digitais – Regulamento (UE) 2022/2065 de 19 de outubro de 2022" (Renata Guilardi de Oliveira Castro).

Em "Outros Estudos", aborda-se o "Blockchain como pilar de um sistema global de propriedade intelectual: uma abordagem descentralizada e universal" (João Mateus ; Cristina Maria de Gouveia Caldeira) e "*Dados pessoais – "o petróleo do século xxi" – os desafios e as ameaças à luz do cibercrime"* (Ana Felícia Santos);

Pela relevãncia de que reveste o tema da inteligência artificial apresenta-se a recenção da obra de Rachel Adams "The New Empire of AI", Polity Press, UK, 2025 (Alexandre Sousa Pinheiro).

Um profundo agradecimento a todos os que colaboraram na publicação da PDPM de 2025.

Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez

I Artigos Doutrinários

Novas reflexões sobre a esfera pública em tempos de novas tecnologias

Maria Cláudia Cachapuz[1]

Resumo

O texto busca identificar o impacto das novas fronteiras tecnológicas aos processos de comunicação e de interpretação jurídica, principalmente quando observados meios de tomada de decisão a partir de sistemas digitais, e a interferência desse fenômeno na formação da opinião pública determinante à política deliberativa. Investiga-se ainda o reflexo do emprego das novas tecnologias à construção de espaços públicos de compartilhamento de liberdades e de posições jurídicas de igualdade, avaliando-se alternativas de ação concreta para que sejam enfrentados os novos desafios tecnológicos e apresentadas soluções jurídicas institucionais que ainda permitam uma ponderação suficiente ao resgate da autonomia própria ao indivíduo e da ideia de autonomia pública dos cidadãos.

Palavras-chave: Direito digital; Esfera pública; Compartilhamento de liberdades; Autonomia.

[1] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

New reflections on the public sphere in times of new technologies

Abstract
The text aimes to identify the impact of new technological frontiers on communication and legal interpretation, especially when considering decision-making methods based on digital systems, and the interference of this phenomenon in the formation of public opinion, relevant to determine deliberative policy. It also investigates the impact of the use of new technologies on the construction of public spaces for sharing liberties and legal positions of equality, evaluating alternatives for concrete action to face new technological challenges and present institutional legal solutions that still allow sufficient consideration to restore the autonomy of the individual and the idea of public autonomy of citizens.

Kewwords: Digital law; Public sphere; Sharing liberties; Autonomy.

Nuevas reflexiones sobre la esfera pública en tiempos de las nuevas tecnologias

Resumen
El texto busca identificar el impacto de las nuevas fronteras tecnológicas en los procesos de comunicación e interpretación jurídica, especialmente cuando se observan métodos de toma de decisiones basados en sistemas digitales, y la injerencia de este fenómeno en la formación de la opinión pública que determina la política deliberativa. . También se investiga el reflejo del uso de las nuevas tecnologías en la construcción de espacios públicos para compartir libertades y posiciones jurídicas de igualdad, evaluando alternativas de acción concreta para que se puedan enfrentar nuevos desafíos tecnológicos y presentar soluciones jurídicas institucionales que aún permitan la consideración suficiente para rescatar la autonomía inherente al individuo y la idea de autonomía pública de los ciudadanos.

Palabras clave: Derecho digital; Esfera pública; Compartimento de libertades; Autonomía.

Introdução

Quando, inicialmente, chegou a haver um consenso pelo Parlamento Europeu, por meio de resolução normativa[2], no sentido de que fossem estabelecidas disposições de Direito Civil sobre Robótica, por ser "necessário criar uma definição geralmente aceite de robô e de Inteligência Artificial (IA) que seja flexível e não crie obstáculos à inovação" (Resolução 2015/2013 – INL)[3], de certa forma, observou-se que, mais do que uma margem de decisão, encontrava-se adotada uma tomada clara de posição, por parte da comunidade jurídica europeia – até então ainda resistente -, tendente ao estabelecimento de diretrizes gerais de cunho utilitarista no tema. Seria, como diria Habermas (2004b, p. 27), uma *praxis* adotada de acordo com os princípios da racionalidade voltada para fins específicos, no que se identificaria uma perigosa transigência sobre o estabelecimento de formas políticas de vida. Na medida em que não haveria como frear o avanço das novas tecnologias em razão dos desejos de progresso estabelecidos e impostos pelo próprio mercado, restaria apenas lidar com os prejuízos identificáveis para futuro, imaginando-se um ordenamento jurídico sustentado por um sistema de garantias[4].

Uma tentativa de correção de rumos, com atenuação da tônica tendente ao avanço do progresso em termos argumentativos, veio com as edições posteriores das Resoluções nº 2020/2012[5], 2020/14[6] e 2020/15[7], em que o Parlamento Europeu, mesmo timidamente – preocupando-se não em impedir o avanço tecnológico, mas em moderar o uso das novas tecnologias -, resgatou o

---

[2] Resolução do Parlamento Europeu, de 16.02.2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (Resolução 2015/2013 – INL), disponível em https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html. Acesso em 17.09.2024.

[3] Resolução do Parlamento Europeu, de 16.02.2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (Resolução 2015/2013 – INL), Introdução, alínea C, disponível em https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html. Acesso em 17.09.2024.

[4] Resolução do Parlamento Europeu, de 16.02.2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (Resolução 2015/2013 – INL), Introdução, alínea M, disponível em https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html. Acesso em 17.09.2024.

[5] Resolução do Parlamento Europeu, de 20.10.2020, que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas (Resolução 2020/2012 – INL), disponível em https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_PT.html. Acesso em 17.09.2024.

[6] Resolução do Parlamento Europeu, de 20.10.2020, que contém recomendações à Comissão sobre o regime de responsabilidade civil aplicável à inteligência artificial (Resolução 2020/2014 – INL), disponível em https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_PT.html. Acesso em 17.09.2024.

[7] Resolução do Parlamento Europeu, de 20.10.2020, que contém recomendações à Comissão sobre os direitos de propriedade intelectual para o desenvolvimento de tecnologias ligadas à inteligência artificial (Resolução 2020/2015 – INL), disponível em https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_PT.html. Acesso em 17.09.2024.

sentido de precaução frente aos avanço das técnicas de aplicação de produtos e serviços digitais nas relações entre os indivíduos. Nessa tarefa, buscou uma regulamentação estatal mais ampla, voltada a exigir alguns pressupostos de garantia, no âmbito das relações de comércio e de consumo, para a interferência na forma do desenvolvimento e de controle sobre produtos e serviços digitais que atuem inclusive por meio da aplicação de sistemas de IA.

Ainda assim, é nítida a preocupação da União Europeia de que se mantenha o desenvolvimento tecnológico com portas amplas[8], sob pena de atropelo econômico por outros grupos ou blocos de interesse. No fundo, mesmo havendo um receio considerável em relação a um descontrole humano sobre a autonomia dos processos digitais, há um medo ainda maior de que haja um descontrole efetivo, pela intervenção demasiada do Estado sobre a autonomia privada, da própria hegemonia comunitária na Europa e de sua possibilidade de concorrência efetiva no mercado internacional. Portanto, é também um problema de distribuição do controle tecnológico entre parceiros econômicos.

Seguindo essa mesma orientação de mercado, no plano filosófico, constata-se que, mesmo havendo uma preocupação de elucidar, do ponto de vista moral, os critérios adotados para analisar situações que possam enfrentar os temas (i) do igual interesse de cada um e (ii) do igualmente bom para todos em sociedade, não existe mais uma convicção segura do porquê prosseguir-se com um dever de permanecer moral a partir de uma ética universalista *a priori* (Habermas, 2004, p. 7). Como acentua Ferry, a pergunta que se mantém em aberto, na contemporaneidade digital, diz respeito a "como recuperar o controle do curso de um mundo que nos escapa e para fazer o quê?" (Ferry, 2015, p. 61).

Numa espécie de redefinição da extensão do conceito de autonomia – para alcançar uma ideia de controle compatilhado por entidades privadas do próprio mercado -, a partida hermenêutica acaba considerando a imposição necessária de uma realidade tecnológica de vida nova, aceita e compartilhada em sociedade.

E é dessa condição fático-jurídica, a partir de um certo receio sobre o que se esperar dos novos processos tecnológicos, que se vê a disciplina contemporânea para o estabelecimento de eventuais freios normativos, ponderados e negociados com o próprio mercado. Não há uma defesa clara à adoção de restrições jurídicas que atinjam o avanço tecnológico de forma direta – isso resultaria em uma contrariedade atual aos próprios interesses de progresso (Russell, 2021) -, mas apenas considerações quanto (i) à necessidade de regulação voltada ao campo dos efeitos, como é próprio ao instituto jurídico da responsabilidade civil; e (ii) à ampliação do ambiente em que reconhecidos os espaços de compartilhamento de liberdades (reais e virtuais) e os seres que os habitam (reais e virtuais).

---

[8] Resolução do Parlamento Europeu, de 20.10.2020, que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas (Resolução 2020/2012 – INL), Introdução, alínea B, disponível em https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_PT.html. Acesso em 17.09.2024.

Observando-se tal realidade empírica, portanto, analisa-se, primeiro, o impacto das novas fronteiras tecnológicas aos processos de comunicação e de interpretação jurídica, principalmente quando observados meios de tomada de decisão a partir de sistemas digitais, e a interferência desse fenômeno na formação da opinião pública determinante à política deliberativa. Na sequência, investiga-se o reflexo do emprego das novas tecnologias à construção de espaços públicos de compartilhamento de liberdades e de posições jurídicas de igualdade, avaliando-se alternativas de ação concreta para que sejam enfrentados os novos desafios tecnológicos e, em certa medida, identificadas soluções jurídicas institucionais que ainda permitam uma ponderação suficiente ao resgate da autonomia própria ao indivíduo e, com mais preocupação, a uma autonomia pública dos cidadãos (Habermas, 2023, p. 49).

1. Novas fronteiras tecnológicas e as alterações da esfera pública

Uma das questões centrais, pertinente aos conflitos de liberdade entre as pessoas nos espaços de convivência contemporâneos, diz respeito a uma ausência de interpretação, *a priori*, quanto à necessidade de que sempre se teste, preliminarmente, a possibilidade de uma universalização do exercício de uma liberdade quando em colidência com a liberdade de outrem. Principalmente em ambientes virtuais, em que identificada uma tendência à fragmentação dos processos comunicativos (Habermas, 2023, p. 62), observa-se maior dificuldade de compartilhamento de experiências que partam da compreensão prévia de que se deva conviver em uma comunidade moral, definida como um agrupamento de indivíduos livres e iguais, em que as pessoas se sintam obrigadas a tratar uns aos outros como fins em si mesmos.

Isto se dá porque a edição de normas mais recentes voltadas à disciplina de uso de novas tecnologias, inclusive junto à Comunidade Europeia[9], tem partido de pressupostos finalísticos bastante definidos, evidenciando um certo receio de como o indivíduo deve se comportar em face do cenário público (político, jurídico) existente e do ambiente (tecnológico) que está por vir. Como evidenciado nos preâmbulos das resoluções antes referidas, torna-se evidente de que se faz existente um consenso preliminar quanto (i) à possibilidade real de ultrapassagem da capacidade intelectual humana pelo desenvolvimento de uma racionalidade própria à robótica e quanto (ii) à necessidade de estabelecimento de garantias à (re)inserção do controle humano nos processos decisórios automatizados e definidos por operações algorítmicas. Um exercício jurídico, portanto, que não está mais centrado no teste da universalização das causas originárias desta necessidade de controle – o que se daria pela tônica normativa voltada à determinação de freios claros ao avanço dessa tecnologia -, mas que se traduz numa preocupação com o campo específico dos efeitos –

[9] Resolução do Parlamento Europeu, de 20.10.2020, que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas (Resolução 2020/2012 – INL), disponível em https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_PT.html. Acesso em 17.09.2024.

e, portanto, voltado com maior ênfase a análise reservada aos prejuízos decorrentes da utilização dessa tecnologia. Tal realidade nem mesmo nas perspectivas mais sombrias de Hannah Arendt – de que "o governo que não é nem da lei, nem dos homens, mas dos escritórios ou computadores autônomos, cuja dominação inteiramente despersonalizada pode vir a se tornar uma ameaça maior à liberdade e àquele mínimo de civilidade sem o qual nenhuma vida comunitária é concebível" (2004, p. 66) - seria imaginável como aceita de forma tão automática e natural, como uma simples consequência da evolução cultural e tecnológica da humanidade.

A construção de uma disciplina normativa, em tempos de automação e de produção em massa de produtos e serviços digitais, tem seguido, mesmo com aparente tempo de maturação disponível, idêntica exigência adaptativa de momentos de excepcionalidade de tomada de decisão por situações globais de emergência – como a recente experiência vivida em tempos de pandemia (Harari, 2023). Ou seja, tem imposto discussões *aceleradas* e *reativas* ao desenvolvimento tecnológico do mercado, por vezes sem a possibilidade de, mediante a reflexão universal necessária, ponderar quanto à efetiva necessidade e adequação do próprio desenvolvimento de determinado produto ou serviço. Ou como aponta Habermas, "justamente nas dimensões em que os limites são pouco definidos, precisamos traçar e impor fronteiras precisas" (2004b, p. 27).

Isso ficou bastante evidente, mais recentemente, quando um grupo de pesquisadores e de empreendedores da área cibernética (Harari, p. 2023) consentiu, por meio de uma carta-aberta à comunidade científica, em uma pausa de seis meses nos experimentos de grande impacto para o desenvolvimento de ferramentas de IA, justificando o ato como necessário a uma correta reflexão e planejamento sobre os caminhos da produção de IA. E, fundamentalmente, por reconhecer a mudança representativa dessa nova tecnologia aos rumos da humanidade. Independentemente das motivações de cada subscritor da carta, há um alerta relevante no gesto realizado, para fins políticos, em caráter universal, mesmo que possa, para muitos, representar apenas estratégia de atuação no próprio mercado.

Primeiro, por se tratar de um aviso que busca produzir consciência de que há razões suficientes para exigir-se da comunidade científica, em termos gerais, uma pré-compreensão que não esteja fundada num raciocínio estritamente pré-ético, como apontado por Peter Singer no seu *Ética Prática* (2009, p. 26). Ainda que exista escassez de meios e urgência no atendimento de demandas, o debate a ser enfrentado não pode ser resumido, exemplificativamente, à discussão rápida de a quem deva se entregar o respirador disponível seguindo-se o protocolo asséptico de realidades genéricas. Não se trata de um "ponto sem retorno", como alertaria Zygmunt Bauman (2013, p. 106), em termos interpretativos. Ao contrário, é necessário retomar o teste da universalização para a questão particular e compreender em que medida se dá a construção de um juízo deontológico suficiente e com pretensão de correção para o atendimento da situação em análise, observadas (i) as condições fáticas e jurídicas que se

apresentem para o caso e (ii) a conduta esperada e capaz de ser universalizada para situações assemelhadas em perspectiva futura.

Segundo, é preciso ter claro que o estabelecimento de princípios gerais a toda normatividade nova deva igualmente passar por um reexame das questões pertinentes aos direitos de personalidade em termos universais – pela capacidade de ser válido a todos os que se dispõem ao compartilhamento desses novos espaços de liberdade -, ainda que exigido um condicionamento prévio, embora cauteloso, à aceitação de ausência de freios aos avanços tecnológicos. A exigência de uma capacidade reflexiva, para a construção de juízos, em termos volitivos e normativos, conduz, justamente, à dupla dinâmica de enfoque em relação à dimensão de autonomia à pessoa - como individualidade e como intersubjetividade -, aproximando a discussão filosófica do campo de análise da liberdade em termos jurídicos.

Em parte, é o que defende, como premissa, a disciplina da Resolução 2020/2012 (INL), do Parlamento Europeu, quando pressupõe que toda a regulamentação de novas tecnologias deva observar uma "inteligência artificial antropocêntrica e antropogênica"[10], destacando uma correção de rumos em relação à premissa de iguais interesses, quando se trate da adoção ou aplicação de produtos de cultura produzidos por seres biológicos. Um desafio complexo, porque não chega a impedir o progresso científico, mas também não quer permitir o exercício de qualquer liberdade tecnológica sem freios. A questão premente é a de como transformar essa precaução em prática universalista efetiva. Como ressalta Sandel (2013), quando a ciência avança mais depressa do que a compreensão moral – inclusive para a observância dos reflexos desses avanços em termos jurídicos -, os seres humanos lutam para articular seu mal-estar.

Este incômodo só existe porque há o sentimento de ameaça sempre presente quanto aos fins que o próprio ser humano, em sociedade, pretende ver alcançados no exercício de sua liberdade. Não é, necessariamente, uma inquietação decorrente do avanço tecnológico em si mesmo, mas do que é feito desse progresso em perspectiva futura. E, portanto, de como lidar com estruturas morais que são capazes de afetar tanto a natureza das coisas, como o que é produto do mundo de cultura: "O desafio é identificar como essas práticas reduzem a nossa humanidade" e, por isso mesmo, ameaçam aspectos de liberdade e de "florescimento" (Sandel, 2013, p. 35) do que se reconhece como humano na contemporaneidade.

Pertencem a Jürgen Habermas (2023) as reflexões mais recentes e maduras sobre o impacto das novas tecnologias à vida de relação das pessoas, em que conferida relevância à visualização de uma alteração significativa à estruturação da esfera pública e do espaço de relacionamento social disposto,

---

[10](item 2 das considerações iniciais): [10"](...)Dessa forma, respeitar a dignidade humana, a autonomia e a autodeterminação dos indivíduos, prevenir danos, promover a equidade, a inclusão e a transparência, eliminar os preconceitos e a discriminação, nomeadamente em relação a grupos minoritários, respeitar os princípios de limitação das externalidades negativas da tecnologia utilizada, de explicabilidade das tecnologias e de garantia de que as tecnologias existem para servir as pessoas e não para as substituir ou decidir por elas, com o objetivo último de aumentar o bem-estar para todos os seres humanos."

principalmente, por meio de plataformas digitais. A análise de Habermas é voltada à percepção do risco oferecido por uma fragmentação do processo comunicativo de agir, em que todos os participantes do espaço de comunicação – "leitores, ouvintes, espectadores" – "podem assumir espontaneamente o papel de autores" (Habermas, 2023, p. 29) e, com isso, compartilharem o exercício de liberdades públicas informativas com iguais pressupostos formativos. No caso, o risco não diz respeito à abertura proporcionada pelo processo – desejada desde sempre (Habermas, 1984, p. 127) -, e sim à formação de uma nova mídia, disposta em ambiente digital semipúblico, que "gira em torno de si mesma", deformando "a percepção da esfera pública como tal" (Habermas, 2023, p. 29). Não por outro motivo, percebe-se a preocupação de que essa nova mídia, por ter ingerência direta sobre a formação de opinião pública, desempenhe papel de destaque, em termos políticos e jurídicos, para uma "formação inclusiva da vontade" individual e coletiva (Habermas, 2023, p. 39).

O tema é relevante, contemporaneamente, em face das inúmeras possibilidades geradas pela quantidade de dados que podem ser processados de forma digital e as conexões estabelecidas a partir desses dados para o estabelecimento de determinados fins. Aferir um número exato de possibilidades de conexões, no ambiente digital, é tarefa inexequível. Tal dificuldade parte desde a identificação dos dados e de suas origens, em bancos públicos e privados, até o controle das conexões realizadas entre as diversas informações e suas finalidades de uso e aplicação. A partir da utilização de bancos informativos para fins de pesquisa e da geração de conteúdo por produtos de inteligência artificial, não há mais nem certeza quanto à autenticidade de informações que transitam na rede e que dados possam ser considerados, por titularidade, de determinado autor. Em termos de propriedade intelectual e direitos autorais, este, inclusive, tem sido um dos temas mais desafiadores, no momento, ao intérprete jurídico (Ody, 2023, p. 120).

Ainda em 2009, a plataforma de pesquisa do Google pôde antecipar a expansão da gripe H1N1, nos Estado Unidos da América, delimitando as regiões de maior alcance da doença, justamente pelo cruzamento de dados extraídos de bilhões de consultas realizadas, diariamente, pelos usuários. A extração dos dados estatísticos, segundo Viktor Mayer-Schönenberger e Kenneth Cukier (2013), ocorreu mediante o cruzamento de informações disponíveis, termos de consultas realizadas na plataforma e registros obtidos junto aos Centros de Controle e Prevenção de Doenças norte-americanos. Ou seja, com acuidade suficiente, o Google possibilitou conhecer antecipadamente os prováveis locais de maior disseminação da doença para futuro, identificando, para uma situação de emergência, critério relevante à tomada de decisão necessária (Mayer-Schönberger; Cukier, 2013, p. 2).

Por isso, o entusiasmo inaugural causado pelo *Big Data*, decorrente da percepção de que o armazenamento e cruzamento de dados informativos em larga escala oferece fácil acesso a uma quantidade massiva de dados (Boyd; Crawford, 2012, p. 673), cede espaço atualmente a uma preocupação quanto ao controle do processamento de toda e qualquer informação que esteja

associado a uma pretensão estratégica de interferência na formação de opinião pública deliberativa. Não se trata, nem mais, da preocupação com um controle relacionado unicamente ao surgimento (*input*) e à recepção ou entrega da informação ao destinatário final (*output*). Ou mesmo de uma pretensão estratégica que esteja relacionada ao condicionamento da vontade individual do sujeito por preferências específicas do mercado – no consumo, na publicidade, no trabalho. É, fundamentalmente, a percepção de que o atual nível de fluxo de informações, a partir do emprego de novas tecnologias, oferece a possibilidade estratégica de impulsionamento e direcionamento orientado da informação, com capacidade suficiente para, *no processo*, formar uma opinião pública deliberativa suficiente à legitimação da finalidade pretendida.

Como refere Habermas (2023, p. 55), a tônica desta preocupação não está mais centrada em como efetuar o correto monitoramento – inclusive para o estabelecimento de freios normativos específicos - do momento de coleta e alimentação do processo informativo (*input*) e do momento em que se estabelece a extração de dados do produto final (*output*). Para essas atividades, há uma descarga cognitiva suficiente com condições de compreensão do fenômeno informativo e de como deve estar capacitado o ordenamento jurídico com respostas institucionais aparentemente suficientes, voltadas à publicidade, transparência, inclusão e acessibilidade dos sistemas. O desafio atual está voltado, mais precisamente, em como gerenciar o *throughput*, estabelecendo-se "o alcance e a qualidade deliberativa da oferta" (Habermas, 2023, p. 55) informativa.

Para além das questões relativas ao acesso e à finalidade da informação, passa a ser essencial compreender que a formação da opinião pública – e de seus reflexos no âmbito de estruturação da própria esfera pública político-jurídica - encontra-se, cada vez mais, conectada à forma como se potencializa, estrategicamente, no processo digital, a informação desejada e que, por diversos fatores, passa a representar, formalmente, o interesse de uma maioria. Em outras palavras, a democracia representativa, a partir de um projeto de sociedade normativamente estabelecido, é substituída, na experiência empírica, por um processo dirigido de comunicação digital, que forma opinião pública de massa e decide por meio de *trend topics*.

Se, num primeiro momento de assombro frente às novas tecnologias, proteger a esfera privada era o que instigava o intérprete no debate jurídico – de forma a que se oferecesse disciplina normativa suficiente e ampla para a gestão de utilização de dados pessoais informativos armazenados -, conseguir, na contemporaneidade, controlar a interferência das novas tecnologias empregadas no processo deliberativo, a partir da formação correta da opinião pública universal, no âmbito da esfera pública, é o desafio que se impõe para fins hermenêuticos. Por isso a pertinência do pensamento de Hannah Arendt quando, ainda em meados do século XX, sem a potencialização conhecida dos processos digitais, observava o caráter híbrido da esfera social – ou semipública (Habermas, 2023, p. 29) - e a sua aptidão para ser utilizada como espaço de manobra totalitária (Arendt, 1989, 401) junto às massas. Uma esfera híbrida, abrangida pelo social - com potencial à discriminação e à identificação em

grupos -, mas que, de forma alguma, para a manutenção de ideais de liberdade e de igualdade jurídicas, pode contaminar os espaços próprios (i) ao que é da esfera pública, no campo político; e (ii) ao que é da esfera privada, regida pela exclusividade (Arendt, 2004, p. 273).

O que diferencia a situação identificada por Arendt (1959) - quando reivindicado um confinamento da esfera social a um espaço híbrido entre o público e o privado - da visualização de uma nova mudança estrutural da esfera pública, como em Habermas (2023), é precisamente a constatação, mais recente, de que a fragmentação do processo comunicativo, por meio dos avanços tecnológicos e da adoção de uma mídia digital, tem permitido, pela experiência empírica e estrategicamente configurada, o aceite de contaminação da esfera pública. E essa contaminação da esfera pública ocorre, no seu âmbito político, pela discriminação social, de forma que se passe a substituir o teste moral da universalização de condutas (razão prática) pela medição direta de *likes* em plataformas digitais (razão empírica), confundindo-se o espaço híbrido da esfera social (ética prática) com o que é destinado à universalização de condutas. Nessa perspectiva, para fins de confirmação estratégica de um espaço editado – inclusive em termos deliberativos -, o teste da universalização de condutas não se configura mais como uma condição *a priori* estabelecida, permitindo que se considere a possibilidade de formação de um raciocínio pré-ético, fundado numa tomada de decisão interessada e que, portanto, envolva "a maior possibilidade de maximização dos interesses dos afetados" (Singer, 2009, P. 26) como premissa de onde se parta. Um raciocínio filosófico que, no extremo, permite que sejam criados apenas "mundos próprios confirmados de maneira intersubjetiva", capazes de conferir a essas "ilhas de comunicação o posto epistêmico de *esferas públicas concorrentes*" (Habermas, 2023, 67).

Quando se desiste da possibilidade de universalização *a priori* e permite-se reconhecer uma condição de "esfera pública editada" (Habermas, 2023, 68), em que a tomada de decisão tenha sida configurada pelo mercado e pelo desenvolvimento tecnológico, alguns problemas passam a ser identificados pelo conflito identificado entre "esferas públicas concorrentes" (Habermas, 2023, 77), a saber: (i) a estimulação a explicações fundadas em teorias conspiratórias de um espaço público em relação a outro, inclusive para estimular a alteração de lógica de compreensão em relação ao que é diferente ou estranho à realidade própria; (ii) o acúmulo de *fake news,* gerando uma deformação generalizada de percepção à esfera pública política ou jurídica, nem mais permitindo ao indivíduo o teste da universalização *a priori*; (iii) a incapacidade de percepção dos cidadãos sobre o que realmente importa na tomada de decisão para a formação de opinião pública concorrente, mediante o estabelecimento de opiniões que não estejam mais "qualitativamente filtradas" (Habermas, 2023, 79). A questão passa a ser, portanto, como evitar que se alcance uma realidade de polarização de esferas concorrentes, atenuando, numa certa medida, o conflito entre o exercício de liberdades ou de posições de igualdade concorrentes.

2. O conflito na nova esfera pública e a normatividade: dois caminhos

O estabelecimento de esferas públicas concorrentes, como apontado em Habermas (2023, 79), não é a origem exclusiva de uma nova mudança estrutural da esfera pública. Não há como se afirmar que seja este, necessariamente, o motivo de uma despolitização do cidadão ou de degradação da opinião pública formativa. Segundo Habermas, o que explica essa perda de função de uma esfera pública política (Arendt, 2004, 272) é a combinação "do uso comercial da rede digital, por um lado, e a disseminação global do programa econômico neoliberal, por outro" (Habermas, 2023, 79). Uma correção de rumos só teria efeito quando aplicada uma disciplina normativa suficiente em termos de regulamentação do processo digital que abranja o serviço prestado pelas plataformas digitais, a exemplo do Regulamento (UE) 2022/2065, mas com capacidade de distinguir também uma responsabilização direta pelo impulsionamento – e não mera veiculação - de conteúdo promovido por essas plataformas. Isso implica reconhecer que a ausência de regulamentação suficiente é capaz de conduzir à formação de esferas públicas concorrentes que apenas reforçam, em cada espaço, a inclusão de semelhantes, sem qualquer promoção à diversidade de desejos, opiniões, vontades entre integrantes de um mesmo grupo: de forma polarizada, só há uma "inclusão assimiladora das vozes consoantes em seu próprio horizonte do suposto 'saber' – contudo, sem filtragem profissional – circunscrito para preservar a identidade" (Habermas, 2023, 76).

Partindo-se do pressuposto de que não se pretende estimular o comportamento polarizado das esferas pela adoção de um pensamento pré-ético[11], dois caminhos se afigurariam possíveis na pretensão de normatização dos conflitos que envolvem informação e novas abordagens tecnológicas. O primeiro, tem em conta uma realidade fática admitida, preliminarmente, a partir de um contexto de consenso quanto a avanços tecnológicos, em que se evidencia um teste pela universalização condicionada de comportamentos e pela partilha de responsabilidade entre partícipes. Nesse caminho, há um movimento no sentido de efetuar-se um teste moral *a priori,* em que pressuposta a aceitação de manutenção de uma esfera pública politicamente estruturada – e distinta do âmbito social -, muito embora se identifique um universo interessado e mais restrito de atuação estatal para a busca de uma solução ao conflito individual, mas ainda não preocupado com os potenciais prejuízos em relação ao atingimento de uma esfera pública política desde logo. É, portanto, uma via que, juridicamente, permite alguns freios institucionais, mas mede riscos de controle à própria atuação de um poder institucional por interesses previamente definidos pelo mercado.

O segundo caminho pressupõe, de forma mais conservadora, a restauração do estado das coisas com maior intervenção de um poder estatal, sendo central a preocupação de proteção à autodeterminação individual numa perspectiva comunitária e intersubjetiva, mas com tônica forte de interpretação

[11] Do contrário, se estaria a concluir, como no receio de Habermas, que a "tecnicização da natureza humana" alteraria "a autocompreensão ética da espécie de tal modo que não possamos mais nos compreender como seres vivos eticamente livres e moralmente iguais" (Habermas, 2004a, p. 57).

pelo teste da universalização a partir de uma tomada de decisão desinteressada. É, por consequência, uma tendência de resgate a ideais de modernidade como contraponto à razão prática imposta pelo progresso tecnológico, justamente por reconhecer, de forma prévia, uma ameaça real às estruturas de um Estado de Direito que se pretenda estabelecido, não retoricamente, em bases democráticas.

Ao fundo, trata-se, em termos jurídicos, da mesma discussão proposta por Robert Alexy, no campo dos direitos fundamentais, em relação às restrições ponderadas acerca do exercício de liberdades no espaço público: "Quem sustenta uma teoría individualista de Estado e de sociedade, tenderá mais à teoria externa; e aquele a quem interessa a posição de integrante de uma comunidade, tenderá à teoría interna" (Alexy, 2001, p. 269). Bem compreendida a afirmação de Alexy, não se trata, aqui, unicamente de uma preocupação de caráter político-jurídico - ainda que possa permitir uma associação entre o ato de interpretar-se a possibilidade de restrições a direitos subjetivos com visões ideológicas distintas sobre questões de liberdade e justiça. A referência efetuada por Alexy é quanto à definição do universo considerado para efeito de restringir-se direitos subjetivos - seja por parte do legislador, seja por parte do intérprete para o caso. Daí porque o interesse de estudo da matéria parte de exame da extensão do conceito de restrição (*lato sensu*) aplicado pelo intérprete e da medida em que tal aplicação corresponde às exigências de uma racionalidade suficiente ao enfrentamento do tema (Cachapuz, 2018, p. 125-150). A questão é, portanto, de alcance quanto à tomada de decisão, identificando-se por qual via, a partir de pressupostos de deliberação livre da vontade, tem-se a possibilidade de promover efetiva condição de autonomia à pessoa ou se avance no sentido de uma preocupação, inclusive, com a autonomia pública dos cidadãos (Habermas, 2023, p. 49).

Dentre os desafios contemporâneos à gestão dos processos de comunicação, uma das questões centrais diz respeito à possibilidade de controle de conteúdo informativo – principalmente para o estabelecimento de freios à disseminação de informações indesejadas - por meio de uma expansão de competências em termos normativos. A ideia é de que, considerado o alcance e a velocidade de processamento dos dados e a complexidade pressuposta ao fenômeno tecnológico, a interpretação acerca do que possa, ou não, ser distribuído no espaço público seja uma atividade regrada no sentido de promoção de uma autodeterminação, individual e coletiva, justamente por se reconhecer a necessidade de compartilhamento de liberdades no espaço público. É, por consequência, um problema que afeta a intensidade de interferência restritiva a direitos fundamentais.

No primeiro caminho argumentativo, as condições fáticas a serem ponderadas exigem um consenso *a priori* em relação à partilha de liberdades no espaço público pelos partícipes do processo comunicativo, com preocupação mais estrita à promoção de uma autonomia individual no âmbito das relações de mercado. O foco, portanto, é que a pessoa receba uma proteção suficiente do ordenamento jurídico, sendo o teste da universalização da conduta reservado à perspectiva daquele sujeito num determinado conteúdo informativo, em que

desprezada – para os fins de resolução do problema - uma universalização, em termos abstratos, mais ampla. Ou seja, o universo considerado para o teste da universalização de conduta admite posições definitivas *a priori*, a partir de um consenso entre os partícipes daquela comunidade considerada, podendo ser, mais ou menos, flexível à ponderação de desafios argumentativos novos na medida em que admitir, normativamente, aberturas jurídicas, desde logo definidas, ao debate. Para o caso, identifica-se, quanto à possibilidade lógica das restrições a direitos fundamentais, uma aproximação da aplicação de uma teoria interna de restrições a direitos.

Algumas condições fáticas, tornadas definitivas desde logo, dão pistas de quando o ordenamento jurídico adota um caminho interpretativo fundado em uma teoria interna de restrição a direitos fundamentais. Assim, (I) quando tendente ao estabelecimento de um *controle comportamental da atividade comunicativa por meio de intermediários de informação*. Em que pese também nos processos de comunicação analógica existam filtros de disseminação de informação de forma corriqueira - na seleção que executam quando do acesso, da coleta, da edição, da escolha de dados, da elaboração do produto informativo, do alcance de mídia e do emprego de processos de correção -, na comunicação digital há uma potencialização desse processo comandada por uma fragmentação da participação aberta a qualquer interveniente. Se, por um lado, esse caráter plural de participação no processo de comunicação digital promove "tendências que dilatam os limites da esfera pública" (Habermas, 2023, 29), gerando uma percepção de democracia expandida a qualquer um; por outro, é justamente a abertura à participação ampla que gera a fragmentação do processo de comunicação – sem controle, sem limites, sem necessidade de maior objetividade e interesse público como norte - e autoriza uma deformação da própria ideia de esfera política, não mais representativa, mas fundada no pressuposto de liberdade irrestrita de qualquer vontade, independentemente do alcance a terceiros.

Essa fragmentação do processo comunicativo passa a exigir, por consequência, que a competência para o controle da distribuição informativa seja deslocada para quem possa fazer a gestão, por primeiro, da informação, impedindo danos incontornáveis. Há a possibilidade de restrição de comportamentos, mas o mercado trata de contribuir para efetuar um controle *a priori,* evitando maior interferência estatal que, conforme o caso, possa impedir o progresso tecnológico – com reflexos econômicos – desde logo. São exemplos de possibilidade de controle digital pelos intermediários: (a) o posicionamento e destaque em *newsfeed* das plataformas de comunicação, para estabelecimento de *ranking* e filtragem de resultados de busca; (b) a situação de predefinição de condutas ou *default*, mediante delimitação prévia de opções ao usuário para o exercício de comportamento posterior; (c) a geração de *profiling*, de forma que o usuário possa, pela identificação, ser dirigido a um ambiente seguro por identificação a outros perfis assemelhados, a partir de uma correlação de interesses, vontades, e não de mera casualidade (Hoffmann-Riem, 2022, 71). No recente Regulamento (UE) 2022/2065, que passou a disciplinar junto à Comunidade Europeia sobre um mercado único aos prestadores de serviços

digitais, algumas premissas de responsabilidade, para fins de controle, passaram a ser estimuladas no mesmo sentido de partilha de restrições às atividades de processamento de informações, a saber: (a) o desenvolvimento de sistema interno de apresentação de notificações e gestão de reclamações (arts. 16° e 20°), para além da regularidade de prestação de serviço de consumo, por armazenamento e divulgação de conteúdo impróprio ou ilegal; (b) a colaboração à resolução extrajudicial de conflitos (art. 21°); (c) o estabelecimento de sinalizadores públicos de confiança à prestação do serviço (art. 22°); (d) a identificação clara da publicidade nas plataformas em linha (art. 26°).

Também é visível, numa interpretação de restrições a direitos por posições definitivas, (II) a admissão e o estímulo à introdução de *elementos de gestão administrativa em sistemas de prestação de serviços digitais*, por meio da chamada *Legal Technology*. Ou seja, a aplicação da tecnologia da informação diretamente no controle de atividades jurídicas, de forma que o próprio processo discursivo, em termos jurídicos, condicione a forma da prestação de um serviço jurídico e, no extremo, a própria interpretação jurídica. Assim, desde a utilização prioritária de sistemas de informatização para a prestação de serviços de assessoria jurídica – armazenamento de informações, organização e gestão de processos, assessoramento *multiportas* para prestação de serviço jurídico *online* e à distância, balcão de atendimento virtual em cartórios judiciais e extrajudiciais -, até a preocupação com a forma da indexação de publicações eletrônicas, de bancos de pesquisa, de formação de jurisprudência.

No ponto, um dos campos mais complexos é o de *legal prediction*[12], pela utilização de ferramentas capazes de prever futuras decisões judiciais, condicionando a própria interpretação judicial – o que pode restar efetuado, estrategicamente, por limitações impostas tecnologicamente ao sistema (questões de nulidade, de distribuição de competência, de limitações à produção probatória). Por isso a preocupação destacada por Hoffmann-Riem (2022, p. 192), de que toda decisão judicial não seja tomada unicamente em processamento automatizado, incluindo as situações de definição de perfil do indivíduo.

Também é sinal de adoção de uma interpretação interna de restrição de direitos fundamentais (III) a construção de um *sistema de garantias centrais fortes, geralmente em termos indenizatórios, conforme a automatização de produtos e*

[12] Aqui, a preocupação tipificada no art. 22° do RGPD (Regulamento EU 679/2016) - "1. 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. 2. O n.° 1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar *os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados.*"

serviços identificados no mercado de consumo. Mesmo se reconhecendo a necessidade de construção de uma estrutura normativa potente em termos de responsabilidade civil - principalmente quando existente maior complexidade à análise de níveis altos de automatização de produtos e serviços -, o que se destaca, no tema, é um direcionamento do intérprete, quando da tipificação de condutas e da aplicação do Direito, a dar maior relevância jurídica ao prejuízo (dano) do que à causa do problema (a atividade em si). Isso é notável quando a interpretação jurídica – inclusive para efeito de estabelecimento de tipos normativos novos ou de definição curricular de novos temas, como o próprio Direito Digital - desloca-se de uma preocupação em termos de construção da hipótese do ilícito para alcançar uma ocupação no campo estrito da responsabilização civil. Trata-se de um movimento não ocasional, mas efetivamente estratégico, em que o recado é nitidamente o de não estabelecimento de freios ao avanço tecnológico – com prejuízo à própria concorrência de mercado -, mas de permanente adequação e assimilação das situações novas conforme a avaliação de risco efetuada em concreto.

De resto, também a aceitação de (IV) um *controle técnico por meio de ferramentas de design* demonstra um deslocamento nítido do exercício de restrições a direitos subjetivos a intermediários do processo de comunicação, por meio da utilização de tecnologia digital, de forma que a própria configuração de um produto ou da forma de prestação de um serviço estabeleça os parâmetros de exercício de liberdades na esfera pública. Um exemplo claro é o desenvolvimento de toda uma teoria sobre o campo da esfera privada a partir do conceito de *privacy by design* (Hoffmann-Riem, 2022, 78).

Por certo, não há qualquer problema com o uso da tecnologia para a proteção em termos de privacidade. Não é diferente a perspectiva, por exemplo, da norma prevista no art. 25º do RGPD (Regulamento EU 679/2016), no sentido de que "o responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento". A questão, como repetido, é de outra ordem. Diz respeito às condições oferecidas, em caráter definitivo e *a priori,* de onde parte o intérprete para o teste de universalidade da restrição a direitos e quais limitações se estabelecem, desde logo, de forma que a pessoa atingida, no seu exercício de uma liberdade ou de uma posição jurídica de igualdade, nem mesmo perceba que já nasce com o direito conformado a partir de um determinado projeto de mercado ou de interesse. São formas de configuração dos produtos e da prestação de serviços que estabelecem o modo de cumprimento de normas legais ou de sistemas de precaução técnica por mecanismos de controle *by design,* como nas hipóteses de (i) estabelecimento de limites de velocidade a determinados produtos; (ii) aplicação de filtros que direcionem pesquisa específica; (iii) proteção de direitos autorais por meio de bloqueio técnico de dublagem ou cópia (Hoffmann-Riem, 2022, 78).

O segundo caminho interpretativo, à base de um retorno a alguns ideais não complementados pelo projeto da modernidade, exige um desafio argumentativo mais complexo ao indivíduo e às nações e, talvez por isso,

apresente uma dificuldade de compreensão estrutural, quanto à sua manutenção, igualmente difícil. Parte, necessariamente, da compreensão de que, mesmo imperfeita, a democracia representativa não deve ser abandonada como projeto de sociedade, mas aprimorada pelo debate público, o que demanda a realização de um teste permanente de universalização das condutas no âmbito público.

Hannah Arendt apontava (1989, p. 362), ainda em meados do século XX, que a forte adesão dos movimentos totalitários entre as massas ocorreu pela ausência de percepção estatal de que o povo (i) não participava ativamente da política deliberativa e tampouco se identificava com partidos políticos específicos e (ii) sentia-se indiferente em relação à representação de interesses na esfera pública (social e política). Essa ausência de representatividade acabou por permitir a adesão da população a movimentos que trabalhassem, justamente, uma identificação direta do líder com o povo, consolidando a ideia de um Estado-nação expansionista e forte no controle das relações públicas e privadas.

Quando se identifica a possibilidade de que, na contemporaneidade, a mesma situação de reconhecimento de ausência de controle de uma esfera pública por representação deliberativa possa conduzir à representação direta por meio de um movimento do controle da opinião pública forjado por um desenho algorítmico em plataformas digitais – como identificado por Da Empoli (2022, p. 65), no exemplo italiano do Movimento 5 Estrelas -, há que se questionar em que medida é possível se depositar o controle de restrição a direitos subjetivos nas mãos dos próprios participantes do processo de comunicação digital. Na construção de uma arquitetura totalitária à base de algoritmos, o movimento representativo de massas se estrutura a partir do desconhecimento dos processos tecnológicos pela maioria – e da certeza de que qualquer controle normativo de tais processos é ineficaz -, com confiança no progresso técnico pelos avanços da ciência desde que associado ao retrocesso histórico em termos de costumes sociais e de desenvolvimento das artes. Há ainda uma ausência declarada de um programa político ou de um projeto de sociedade específico. Os algoritmos servem para captar o interesse da massa e adotá-lo de forma majoritária, a partir de uma ideia populista de governo: "É um simples algoritmo construído para interceptar o consenso graças a assuntos e tópicos 'que funcionam'. Se a imigração é um tema forte, o Movimento investe no assunto, adotando a posição mais popular" (Da Empoli, 2022, 66).

Portanto, reconhecer *a priori* a possibilidade de existência de uma gestão estratégica dos fluxos de informação é situação suficiente para exigir-se do intérprete jurídico, de forma permanente, um teste de universalização amplo em relação à adoção de práticas novas em termos tecnológicos. Isso permite que se compreenda que toda a proteção da esfera privada do indivíduo, para assegurar efetividade de tutela, demanda mais do que uma simples substituição do direito geral de liberdade negativa por uma concepção concreta de liberdade. É necessário, para o teste da universalidade, que a liberdade negativa seja uma condição necessária, mesmo que não suficiente (Alexy, 2001, p. 348), ao alcance de dignidade à pessoa humana. Algo que só é alcançável, em

termos jurídicos, quando acolhida uma teoria externa de restrição a direitos fundamentais.

Essa abertura predisposta ao intérprete jurídico só é possível se o ordenamento jurídico dispõe, ainda em tese, de uma compreensão clara quanto ao sistema de restrições a direitos fundamentais e parte de "uma associação autodeterminante de parceiros de direito livres, na qual estes, na condição de colegisladores democráticos, devem em última instância conceder a sua liberdade a si próprios pela distribuição igualitária dos direitos subjetivos segundo leis universais" (Habermas, 2023, p. 37). Para Habermas, essa é condição essencial para que se compreenda a ideia de autodeterminação coletiva, "que combina o universalismo igualitário dos direitos iguais para todos com o individualismo de cada um", reconhecendo-se democracia e Estado de Direito "em pé de igualdade" (Habermas, 2023, p. 37).

Para o teste, segundo Habermas, algumas condições fáticas e jurídicas passam a ter peso significativo para a adoção justificada de qualquer restrição a direito fundamental – por quem quer que seja o agente dessa restrição e qualquer que seja o momento dessa restrição (*input, throughput, output*) - em face da participação de um processo de fluxo de informações por um sistema que se pretenda democrático. Dentre essas condições, é central a compreensão de que só há efetivo debate político-jurídico se há consenso quanto à "disposição dos cidadãos de reconhecer reciprocamente os outros como concidadãos e colegisladores democráticos em igualdade de direitos" (Habermas, 2023, p. 47). O adversário político não é, por consequência, um inimigo, mas um oponente, cuja vontade não pode ser desprezada e apenas desafiada pela argumentação suficiente.

Da mesma forma, só se identifica uma sociedade civil plena em seu exercício de construção da esfera pública quando se possibilita que participe "de maneira espontânea e suficiente no processo democrático de formação da opinião e da vontade" (Habermas, 2023, p. 49). Isso representa afirmar que devem ser dadas condições estruturantes suficientes para que qualquer cidadão participe de forma livre do processo de representação deliberativa, sem que tenha sido instrumentalizada a informação necessária à formação de opinião pública pelo processo de comunicação digital. Ou seja, é necessário que o debate público, principalmente para efeito de representação, não parta condicionado por edições de mídia ou por informações adulteradas, que possam conduzir a uma não representação política ou a uma representação deficiente. É essencial "potencial de esclarecimento" a toda informação e "pluralismo de opinião" (Habermas, 2023, p. 41) para a construção de uma esfera pública política (Habermas, 2023, p. 39). Portanto, a ponderação que se estabeleça, desde que exercitada mediante as competências legais previstas juridicamente, é legitimada, e não constitui censura, mesmo que restrinja integralmente uma determinada liberdade.

E, por fim, como condição essencial a toda a restrição – seguindo uma compreensão muito próxima de Alexy (2001, p. 158), quando trata de um modelo de fundamentação que seja resultado de uma ponderação decorrente de um sistema de preferências condicionadas -, sustenta Habermas que todo ideal

democrático e, portanto, de preservação de autodeterminação individual e coletiva, só se configura mediante o equilíbrio de "imperativos funcionais opostos" (Habermas, 2023, p. 51).

A conexão parece decorrer, por lógica, da forma como os indivíduos se vinculam no espaço público, assumindo posições e interesses diversos, na medida em que se conectam, por titularidade, ao exercício de determinados direitos e, nessa medida, conferem-lhe determinado conteúdo. Assim, tanto a questão das restrições a direitos subjetivos, como a questão relativa ao exercício de posições jurídicas, preocupam-se como a mesma questão de fundo: para que se reconheça a manutenção de uma vontade livre, é necessário que as pessoas tenham asseguradas, no âmbito da esfera pública, tanto as suas liberdades individuais como, no âmbito coletivo e social, o direito de exigir algo frente ao Estado para que possam fazer valer a manutenção da convivência compartilhada em sociedade (Alexy, 2001, p. 189-194) – o que pode ser traduzido tanto pelo direito de não impedir ações individuais, como pelo direito à não afetação de propriedades e situações de garantias individuais ou ainda pelo direito à não eliminação de posições jurídicas na realização de direitos a ações positivas, tanto em relação a prestações fáticas, como em relação a prestações normativas.

Bauman (2017), em escrito mais tardio e à luz das questões tormentosas ligadas à migração de povos, ocupou-se da mesma preocupação quanto a conflitos individuais que toquem nas questões afetas à democracia e à pretensão de exigência de um direito a algo, em termos coletivos: "Kant previu o advento de tal situação" - o expurgo populacional - "e meditou sobre os imperativos que precisariam ser observados quando isso ocorresse – como deve ocorrer. Como conviver – viver em paz – num planeta congestionado, que está atingindo o limite de sua capacidade de ocupação?" (Bauman, 2017, 72-73). O desenvolvimento dessa tolerância, em Kant, que reforça a ideia de um projeto de sociedade voltado ao fim das hostilidades entre os povos – a sua ideia de condução normativa à paz perpétua (Kant, 2002) – é baseado, não em filantropia ou na sua tradução contemporânea de um "altruísmo eficaz" (Singer, 2020), mas na ideia de uma hospitalidade universal.

Falar em hospitalidade, num sentido universal, significa reconhecer, na mesma sequência de Habermas, algumas condições básicas morais para o exercício da tolerância entre opostos, pressupondo, obviamente, o interesse na manutenção de Estados federados e capazes de seu organizarem de forma democrática. Em tempos de novas tecnologias e de fluxo informativo digital corresponde, justamente, ao resgate exigido de teste mais amplo e *a priori* de universalização de condutas, que permita compreender a impossibilidade de redução do debate jurídico aos interesses mais estritos em discussão e que promova a ponderação em concreto em termos de conflitos individuais e coletivos.

Conclusão

Partindo-se da ideia de uma hospitalidade universal como condição ao desenvolvimento de um pressuposto de tolerância em sociedade – justamente porque o pressuposto é o de fim às hostilidades entre os povos (Kant, 2002, p. 120) -, não é difícil se deduzir que as questões pressupostas por Kant para a busca de um ideal de convivência social estão muito próximas das mesmas premissas necessárias para a promoção de uma correta autodeterminação individual e coletiva. Isto porque, tanto na esfera de relacionamento privado, como na esfera de convivência pública, a intersubjetividade encontra-se pressuposta como critério de tolerância – a ideia enfática, segundo Habermas, de que "uma pessoa só pode ser livre se todas as demais o forem igualmente" (Habermas, 2004a, p. 13).

É o que defende Habermas, em complementação, a partir da ideia de universalização pressuposta na conduta humana: "(...) assim que tomamos como ponto de partida o conceito do indivíduo essencialmente socializado e concebemos o ponto de vista moral como implícito na estrutura do reconhecimento recíproco dos sujeitos de ação comunicativa, a moral privada e a justiça pública deixam de se distinguir em princípio para passarem a diferenciar-se unicamente em grau de organização e em mediação institucional das interações" (Habermas, 1991, p. 162). Em tempos de novas tecnologias, significa compreender que, para efeito de análise do problema posto dentro das bases de um discurso jurídico - que essencialmente trabalha com categorias morais-pragmáticas -, ainda que se possa reconhecer a liberdade à pessoa em abstrato, é necessário que lhe seja possível visualizar também autonomia em potencial, porque autorizada a percepção como participante de uma comunidade moral ou "como uma comunidade formada de indivíduos livres e iguais que se sentem obrigados a tratar uns aos outros como fins em si mesmos" (Habermas, 2004a, p. 13).

Participar dessa forma de linguagem não importa, portanto, em simples verificação de pressupostos de liberdade em sociedade, pelas escolhas que são desejadas ou idealizadas de forma ampla. É preciso que se reconheça a capacidade de correção na construção de juízos pela perspectiva do outro, com quem a pessoa compartilha os espaços de liberdade no âmbito público.

Somente dessa forma é que o indivíduo aproxima-se de um estado de real desinteresse para o cumprimento de um dever ou mesmo de um desejo, ainda que possa ser praticamente utópico alcançar uma situação de completa ausência de outros móbiles ao comportamento em sociedade. Conforme Kant (2002), mesmo que a pessoa não consiga cumprir o seu dever conhecido de forma desinteressada – e não estratégica, por definição -, é o não abandono de tal ideal que mantém vivo o pressuposto de moralidade social.

Referências:

Alexy, R. (2001) Teoría de los derechos fundamentales. CEPC.

Arendt, H. (1989) Origens do totalitarismo. Companhia das Letras.

Arendt, H. (1959) Reflections on Little Rock. Dissent.

Arendt, H. (2004) Responsabilidade e julgamento. Companhia das Letras.

Bauman, Z. (2017) Estranhos à nossa porta. Zahar.

Bauman, Z. (2013) Vigilância líquida. Zahar.

Boyd, D.; Crawford, K. (2012) Critical questions for Big Data. In Information, Communication & Society. In https://people.cs.kuleuven.be/~bettina.berendt/teaching/ViennaDH15/boyd_crawford_2012.pdf.

Cachapuz, M.C. (2018) A obrigação pelo discurso jurídico. Fabris.

Da Empoli, G. (2022) Os engenheiros do caos. Vestígio.

Ferry, L. (2015) A inovação destruidora. Ensaio sobre a lógica das sociedades modernas. Objetiva.

Habermas, J. (2004a) A ética da discussão e a questão da verdade. Martins Fontes.

Habermas, J. (2004b) O futuro da natureza humana. Martins Fontes.

Habermas, J. (1984) Mudança estrutural da esfera pública. Tempo Universitário.

Habermas, J. (2023) Uma nova mudança estrutural da esfera pública e a política deliberativa. Editora Unesp.

Harari, Y.N. (2023) et alli. Pause giant AI experiments: An open letter. In http://futureoflife.org, Future of Life Institute, Narberth/PA.

Hoffmann-Riem, W. (2022) Teoria geral do Direito Digital. Forense.

Kant, I. (2002) À paz perpétua e outros opúsculos. Edições 70.

Mayer-Schonberger, V.; Cukier, K. Big Data: Como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Elsevier.

Russell, S. (2021) Inteligência artificial a nosso favor: Como manter o controle sobre a tecnologia. Companhia das Letras.

Sandel, M.J. (2013a) Contra a perfeição. Ética na era da engenharia genética. Civilização Brasileira.

Sandel, M. (2013b) Justiça: O que é fazer a coisa certa. Civilização Brasileira.

Singer, P. (2009) Ética práctica. Akal.

Singer, P. (2020) O maior bem que podemos fazer. Edições 70.

Dos ataques de ransomware na Convenção de Budapeste sobre o Crime Cibernético - um ensaio de qualificação alternativa, desde Portugal [13-14]

Manuel David Masseno[15]

Resumo

Por efeito da muito recente adesão à Convenção do Conselho da Europa sobre o Cibercrime, de 2001 (a *Convenção de Budapeste*), o Brasil terá de adequar o respetivo Direito Penal Material. Este o artigo avalia a viabilidade de enquadrar primariamente os ataques de *ransomware* no crime de "Fraude [Burla] informática", em atenção tanto aos elementos objetivos e subjetivos quanto aos bens jurídicos protegidos, os quais sempre tiveram por finalidade alargar ao máximo a criminalização de atos contra o património praticados através de meios informáticos, conforme à "Minuta do Relatório Explicativo da Convenção". São ainda objeto de estudo os concursos possíveis com outros crimes constantes da *Convenção*, como a "Violação de dados [Dano provocado nos dados]" e a "Interferência em sistema [Sabotagem informática]", com o inerente "Uso indevido de aparelhagem [Utilização indevida de dispositivos]" para a prática de ataques de *ransomware*, e ainda a "Falsificação informática" e o "Acesso ilegal [ilícito]".

Palavras-chave: Brasil, burla informática, Convenção sobre o Cibercrime, *ransomware*

---

[13] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

[14] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

[15] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Abstract

As a result of the very recent adherence to the Convention of the Council of Europe on Cybercrime, of 2001 (*the Budapest Convention*), Brazil will have to adequate its Substantive Criminal Law. This paper evaluates the viability of considering ransomware attacks within the scope of "Computer-related fraud", considering the acts and the intents of this offence as well as the legal stated protected interests, that was designed in order to include at most computer-related illegal transfers of property trough data or system manipulations, according to the "Explanatory Report to the Convention on Cybercrime". The possible cumulation with other crimes included in the *Convention*, such as "Data interference" and "System interference", along with the "Misuse of devices" intended to perform acts related with ransomware attacks, offenses, as well as "Computer-related forgery" and "Illegal access", are also comprised in the subject of study.

Kewwords: Brazil, computer-related fraud, Convention on Cybercrime, ransomware

1. Pontos de partida

Como por confessar que a efetiva razão de ser deste meu contributo passou pela necessidade de me reposicionar relativamente ao artigo escrito com Emerson Wendt, "ainda a quente", aquando dos ataques com o *WannaCry* e as questões relativas ao seu enquadramento no âmbito do Direito Penal alcançaram uma projeção global[16].

Aliás, embora redigido em poucos dias e com objetivos assumidamente humildes, sobretudo consistentes em facultar referências sólidas às Polícias e aos Ministérios Públicos de Portugal e do Brasil na investigação e perseguição criminais de tais ações, esse artigo ficou como uma referência quase obrigatória nos estudos subsequentes sobre a matéria em língua portuguesa, com múltiplas referências em livros, artigos e trabalhos académicos.

Em síntese extrema, intentámos uma caraterização material de tais ataques, em termos dinâmicos e explorando as variações em presença, e formulámos propostas de qualificação de cada um dos correspondentes passos nos Ordenamentos penais português e brasileiro, atendendo à falta de uma tipificação específica em ambos, a qual continua a se verificar quase sete anos depois. O que fizemos recorrendo ao conjunto das previsões incriminatórias, mesmo para além dos delitos informáticos em sentido próprio. A que se seguiu uma análise sumária dos concursos, tanto reais quanto aparentes, entre os tipos identificados e analisados.

Cumpre ainda acrescentar que esta perspectiva antecipou a seguida, vários anos depois, pela *Nota de Orientação* emitida a este propósito pelo *Comité da Convenção sobre o Crime Cibernético* (Comité T-CY)[17]. Embora esta proporcione sobretudo um entendimento estático, em mosaico, enquanto a nossa o fazia dinamicamente, enquanto fluxo operativo, distinguindo as possíveis variantes nas vias de ataque de *ransomware*, como já referimos[18].

---

[16] Concretamente, M.D. MASSENO & E. WENDT (2017, *passim*).

[17] Emitida em inglês como T-CY *Guidance Note #12 Aspects of ransomware covered by the Budapest Convention* (T-CY(2022)14), aprovada a 30 de novembro de 2022, a qual também abrange as matérias de Direito Processual e de Cooperação Internacional pertinente, estando disponível neste endereço: <https://www.coe.int/en/web/cybercrime/-/ransomware-new-guidance-note-by-the-t-cy>; ainda a este propósito, aproveito o ensejo para acrescentar que Portugal tem sido eleito, e sucessivamente reeleito, para este Comité desde 2006, sendo sempre representado por Pedro Verdelho, Coordenador do Gabinete Cibercrime da Procuradoria-Geral da República <https://cibercrime.ministeriopublico.pt/>.

[18] Num sentido próximo, embora centrado nas Fontes portugueses, as quais tiveram por fundo, sucessivamente, a *Recomendação n.º R (89) 9*, de 13 de setembro de 1989, relativa à criminalidade informática, do Comité de Ministros dos Estados-Membros do Conselho da Europa e a *Convenção de Budapeste*, assim como as Diretivas relevantes da União Europeia, além de facultar uma profusão de referências documentais e doutrinárias, D.R. NUNES (2019, *passim*). A *Recomendação* do Comité de Ministros está disponível em inglês, designadamente pela Organização dos Estados Americanos: <https://www.oas.org/juridico/english/89-9&final%20Report.pdf>; enquanto as versões oficiais, em inglês e francês, assim como todas oficiosas, da podem ser consultadas na correspondente página do Conselho da Europa: <https://www.coe.int/en/web/conventions/-/council-of-europe-convention-on-

Porém, cerca de um ano depois, por ocasião do *II Congresso Nacional* [brasileiro] *de Direito Digital*, organizado pela Comissão de Direito Digital da Seção de Santa Catarina da Ordem dos Advogados do Brasil, em finais de abril de 2018, a maturação resultante da continuidade do estudo da matéria conduziu-me a um novo entendimento de ordem sistemática no que se refere à qualificação dos ataques de *ransomware*, precisamente por referência à *Convenção sobre o Crime Cibernético*[19-20], a *Convenção de Budapeste*.

Entretanto, a muito recente, ainda que tardia, adesão do Brasil à *Convenção*[21-22], com a inerente necessidade de "adotar medidas legislativas e outras providências necessárias", adequando o respectivo Direito Penal

---

cybercrime-ets-no-185-translations>.

[19] Uma análise que tivera também por referência explícita a Diretiva 2013/40/UE, do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32013L0040>, M.D. MASSENO (2018a). Embora a circunstância de, ao tempo, a Decisão-quadro do Conselho, de 28 de maio de 2001, relativa ao combate à fraude e à contrafacção de meios de pagamento que não em numerário <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001F0413> ainda vigorar não tenha contribuído para um mais fácil reposicionamento da perspectiva, como porventura teria ocorrido se já tivesse saído a subsequente Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32019L0713>, sobre a qual, ainda que com a tónica na Lei n.º 79/2021, de 24 de novembro, que a transpôs para o Ordenamento português <https://diariodarepublica.pt/dr/detalhe/lei/79-2021-174824631>, é de indicar o estudo de D.R. NUNES (2022). Porém, o Direito da União Europeia não constitui o objeto deste trabalho, ainda que uma argumentação assentando nos mesmos fosse até suscetível de contribuir para um melhor esclarecimento das questões que enfrentamos.

[20] Entendimento este que tenho vindo a explorar, desde várias vertentes, no âmbito da lecionação nas disciplinas de "Direito na Segurança Informática e no Cibercrime", "Cibercriminalidade" e "Cibercrime e Prova Digital", designadamente no Mestrado em Direito e Informática da Universidade do Minho, M.D. MASSENO (2023a).

[21] Na sequência de um processo longo, formalmente desencadeado com a sinalização diplomática da sua disponibilidade para ser convidado a aderir à *Convenção*, em julho de 2019, com o convite a ser efetivado em dezembro de esse ano, embora a Presidência da República apenas tenha enviado para o Congresso a proposta de ratificação legislativa com a Mensagem nº 412, de 22 de julho de 2020, com a adesão a ser aprovada por meio do Decreto Legislativo nº 37, de 16 de dezembro de 2021, e a promulgação ocorrer através do Decreto nº 11.491, de 12 abril de 2023 <https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm>.
Embora do Decreto constar que "a República Federativa do Brasil firmou a Convenção sobre o Crime Cibernético, em Budapeste, em 23 de novembro de 2001", essa indicação apenas pode resultar de um *lapsus calami*, pois do texto resulta também que "Governo brasileiro [apenas] depositou, junto ao Secretário-Geral do Conselho da Europa, em 30 de novembro de 2022, o instrumento de ratificação à Convenção", não sendo um dos subscritores iniciais. Sobre estas vicissitudes, embora em termos muito sintéticos, M.D. Masseno (2023b).

[22] Sobre a *Convenção*, em termos gerais, embora sobretudo centrada nas suas previsíveis consequências para as Fontes legislativas portuguesas, temas as páginas introdutórias de P. VERDELHO (2003, *passim*), assim como e sobretudo as reflexões de F.P. CARVALHO, O. MORALES G. & M. ÁLVAREZ F. (2018, 48-54), além dos meus apontamentos atualizados, MASSENO (2023a).

Material[23], levaram-me a alinhar algumas reflexões, sobretudo com a finalidade de contribuir para o debate que deve anteceder a criminalização de novas condutas ou a modificação do enquadramento de condutas já antes penalizadas[24].

O que não será um exercício simplesmente académico, vazio de relevância prática, sendo a *Convenção* fragmentária, de mínimos e, consequentemente, deixar uma ampla margem de conformadora para o Poder Legislativo interno de cada uma das Partes, como mostra a *Nota de Orientação* do Comité T-CY, já referida.

2. Uma qualificação primária

Começando por recordar a caracterização dos ataques de *ransomware*, em sentido próprio, feita por mim e por E. Wendt, a qual mantenho:

> "Em extrema síntese, o mesmo pode-se resumir em quatro passos, todos eles necessários para a identificação do nosso objeto:
> (**1**) a obtenção de acesso ao sistema informático da vítima, com ou sem engano, por parte do(s) autore(s);
> (**2**) a que se segue a inserção no referido sistema de um código, o qual encripta dados, com base em um mecanismo de chaves assimétricas, gerando adicionalmente uma identificação personalizada desse mesmo sistema;
> (**3**) depois, tem lugar uma comunicação à vítima do ocorrido, assim como do montante exigido, para facultar/entregar a chave personalizada de desencriptação, enviando valores em criptomoedas (para não ser rastreável), e o endereço (carteira) para onde deve ser enviado, junto com a identificação personalizada do sistema em causa; e

---

[23] Como, aliás, procurei mostrar na minha muito recente Aula Aberta para a WB Educação, M.D. MASSENO (2023b).

[24] É de sublinhar que o Brasil optou por se afastar da terminologia e da estrutura frásica das Versões já publicadas em língua portuguesa, designadamente, da de natureza oficiosa do próprio Conselho da Europa <https://rm.coe.int/16802fa428>, assim como das oficiais de Portugal, constante da Resolução da Assembleia da República n.º 88/2009, em 10 de Julho de 2009 <https://diariodarepublica.pt/dr/detalhe/resolucao-assembleia-republica/88-2009-489698>, e de Cabo Verde, conforme à Resolução [da Assembleia Nacional] n.º 116/VIII/2014, de 19 de novembro <https://kiosk.incv.cv/V/2014/11/19/1.1.70.1929/p2107>, tendo ido diretamente à versão oficial em inglês <https://rm.coe.int/1680081561>, embora sem a seguir exatamente, inclusive ao traduzir "*Convention on Cybercrime*" por "Convenção sobre o Crime Cibernético". Ora, esta "liberdade legística" poderá ter consequências, como veremos em seguida, as quais deverão ser evitadas aquando da aprovação da lei, ou leis, de adequação do Ordenamento penal brasileiro à Convenção, sobretudo tendo em vista o conteúdo e o alcance *Princípio da tipicidade penal*, previsto no inciso XXXIX do Artigo 5º da *Constituição Federal* de 1988.

> (**4**) finalmente, uma vez, efetuado o pagamento, a vítima recebe uma chave personalizada de desencriptação que lhe permite recuperar os dados."[25]

Se nos abstrairmos de pré-entendimentos resultantes do *nomen juris* atribuído ao tipo, o qual teria sempre uma importância secundária, podemos identificar todos os traços caracterizadores de tais ataques no crime correspondente à "Fraude informática".

Aliás, é patente como o texto da *Convenção* contem uma noção muito ampla de "fraude", *rectius* de "objetivo fraudulento", nos dolos específicos facultativos dos tipos correspondentes ao "Acesso ilegal" (Artigo 2), "Interceptação ilícita" (Artigo 3) e "Falsificação informática" (Artigo 7), o usando para assinalar um desvalor de relativo à intenção de alguém se apropriar ilicitamente de bens alheios.

Adicionalmente, atendendo ao explicitado na "Minuta do Relatório Explicativo" apensa à *Convenção*, a qual acompanharemos de perto, enquanto contraponto aos enunciados normativos, a tipificação da "Fraude informática" foi concebida de modo a abranger um espectro amplo de práticas ilícitas contra o património, em ambiente informático:

> "A revolução tecnológica veio multiplicar as possibilidades de cometer infracções de carácter económico, tais como as fraudes, das quais citamos as fraudes verificadas com os cartões de crédito. Os activos representados ou administrados por sistemas informáticos (fundos eletrónicos, dinheiro de depósitos) tornam-se alvos de manipulações da mesma maneira que as tradicionais formas de propriedade. Estes crimes consistem principalmente na manipulação da entrada no sistema, em que são introduzidos dados incorretos, ou em manipulações em programas e outras interferências no tratamento de dados. [Consequentemente] **O objetivo deste artigo é o de penalizar toda e qualquer manipulação indevida durante o tratamento de dados, cuja intenção seja a de efectuar uma transferência indevida de propriedade** [negrito meu]"[26].

---

[25] Sobre estes, inclusive identificando variantes, são de assinalar os desenvolvimentos de D.R. NUNES (2019, 61-68) e as considerações muito recentes, embora breves, de J.C. PINTO (2023).

[26] Assim, no Ponto 36 da *Minuta*, a qual está também acessível em língua portuguesa, embora seguindo a norma europeia anterior ao *Acordo Ortográfico* de 1990 <https://rm.coe.int/16802fa429>. Do mesmo modo e ainda mais claramente, estes objetivos constam do Ponto II.2.a do *Relatório* do Comité Europeu de Problemas Criminais do Conselho da Europa, apenso à *Recomendação n.º R (89) 9*, já referido e que teve uma importância fundamental nos trabalhos preparatórios da *Convenção*, como é assumido tanto na *Minuta de qua* quanto no *Preâmbulo* da própria *Convenção*.

Portanto, podemos ter por assente que o preceito foi concebido e redigido cuma grande abertura, de modo a abranger as novas realidades sociais e tecnológicas suscetíveis de alcançar os resultados indesejados, embora sempre de natureza essencialmente patrimonial, o que nos permite enquadrar ações ainda desconhecidas ou inviáveis à época por razões de ordem tecnológica. Assim, da Convenção consta o tipo relativo à:

> "Artigo 8 - **Fraude informática** [negrito meu]
> Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, a conduta de quem causar, de forma dolosa e não autorizada, prejuízo patrimonial a outrem por meio de:
> a. qualquer inserção, alteração, apagamento ou supressão de dados de computador;
> b. qualquer interferência no funcionamento de um computador ou de um sistema de computadores, realizada com a intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita."[27-28]

---

[27] Esta redação segue de perto a constante do *Relatório* apenso à *Recomendação n.º R (89)* 9, de 13 de setembro de 1989, em cujos termos a "Computer related fraud" [aliás, a primeira das condutas a serem criminalizadas] consiste em: "The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for oneself or for another person (alternative draft: with the intent to unlawfully deprive that person of his property)". A *Recomendação* do Comité de Ministros, incluindo o *Relatório*, por esta recebido, estão disponíveis em inglês, designadamente pela Organização dos Estados Americanos: <https://www.oas.org/juridico/english/89-9&final%20Report.pdf>.

[28] Efetivamente, esta conceptualização corresponde ao estado dos debates a propósito de estas questões, designadamente quanto à inserção do § 263a "Computerbetrug" [Fraude informática] no *Strafgesetzbuch* (StGB) [*Código Penal*, alemão] através da "Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität" [a Segunda Lei para Combater a Criminalidade Económica], de 15 de maio de 1986, a qual dispõe, quanto ao nosso objeto de estudo, que "1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.". Por sua vez, a *Recomendação* esteve na base da *Primeira Geração* de Leis europeias sobre a matéria, como ocorreu em Itália com a inclusão do art. 640 ter "Frode informática" no *Codice Penale*, pela "Legge 23 dicembre 1993 n. 547", pela qual "Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto com qualsiasi modalita' su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a se' o ad altri un ingiusto profitto con altrui danno, e' punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni.", assim como em Portugal, aproveitando a reforma profundada do *Código Penal*, operada pelo Decreto-Lei n.º 48/95, de 15 de março, ao inserir o Art.º 221.º "Burla informática", "1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo

Passando a uma análise do tipo, sempre na perspectiva dos ataques de *ransomware*, no referente ao seu elemento objetivo, temos enquanto objetos necessários e alternativos da ação ou os "dados de computador", entendidos como "qualquer representação de fatos, informações ou conceitos numa forma adequada para o processamento num sistema de computador que inclua um programa capaz de fazer o sistema realizar uma tarefa;" (Artigo 1 b.) ou o "sistema de computador" [o qual] designa qualquer aparelho ou um conjunto de aparelhos interconectados ou relacionados entre si que asseguram, isoladamente ou em conjunto, pela execução de um programa, o processamento eletrônico de dados;" (Artigo 1 a.).

A este propósito, é necessário entender que o "programa" é abrangido pela noção de "dados de computador" e por "aparelho" deve ser considerado não apenas um esquipamento físico (*hardware*), mas também os programas de computador que permitem o respectivo funcionamento (*software*), como resulta explicitamente do texto da Convenção, a propósito da criminalização de atos preparatórios, ao incluir o "programa de computador" na noção de "aparelho" (Artigo 6º parágrafo 1, letra a i)[29].

Por sua vez, no que se refere à caracterização do conteúdo da ação típica, temos dois elementos de natureza objetiva, em alternativa e de forma relativamente vinculada, consistentes em "qualquer inserção, alteração, apagamento ou supressão de dados de computador" ou em "qualquer interferência no funcionamento de um computador ou de um sistema de computadores", incluindo o próprio *hardware*. O que nos ataques de *ransomware* é efetivado por meio da encriptação ou cifragem de dados ou programas, o Passo 2) no procedimento descrito.

Quanto ao elemento subjetivo do tipo, temos um dolo genérico correspondente a "causar, de forma dolosa e não autorizada, prejuízo patrimonial a outrem", ao qual acresce o dolo específico que subjaz à "intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita". Correspondendo aos objetivos essenciais dos ataques, consistentes na obtenção

---

patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.", a propósito deste preceito, embora em termos contextualizados com a *Recomendação* e também com a posterior *Convenção*, têm interesse as reflexões de C.G. PEDRA (2019, 15-19), assim como de C. RODRIGUES (2019, 44-45), D.S. PALMA (2019, 77-82 e 84-86) e de P.L.R. MOTA (2019, 171-173).

[29] Neste ponto, é indispensável ter em atenção que, como resulta explicitamente do Ponto 22 da *Minuta*, "Foi considerado pelos autores do projeto que, ao abrigo da presente Convenção, as Partes não ficariam obrigadas a copiar textualmente, para as suas legislações nacionais, os quatro conceitos definidos no Artigo 1º, desde que tais conceitos se encontrem abrangidos nas referidas legislações de uma forma coerente com os princípios da *Convenção* e proporcionem uma estrutura equivalente para a sua implementação.". Ora, no Ponto 22, a propósito do "sistema de computador" consta que este "é um equipamento composto por *hardware* e *software* desenvolvidos para o tratamento automático de dados digitais [enquanto] a expressão "tratamento de dados" significa que os dados no sistema informático são operados através da execução de um programa de computador.".

de um pagamento por parte da vítima, a qual procura assim recuperar o controle dos dados e ou do sistema, os Passos 3) e 4).

Ainda a propósito do alcance do dolo específico indicado, apesar de uma interpretação apenas enunciativa apontar para o inverso, é indispensável acrescentar que o mesmo releva para as duas condutas típicas e não apenas em caso de "interferência no funcionamento de um computador ou de um sistema de computadores". Como nos mostra uma leitura comparativa entre as versões oficiais e vinculantes, em inglês[30] e em francês[31], assim como as outras versões em língua portuguesa, a oficiosa do Conselho da Europa[32] e as correspondentes às aprovações para ratificação de Portugal e de Cabo Verde[33], as quais coincidem, *verbatim*.

Nestes termos, estamos perante um crime de dano, a ser consumado com o prejuízo patrimonial efetivo da vítima, para tal não bastando à "inserção, alteração, apagamento ou supressão de dados de computador" ou a "interferência no funcionamento de um computador ou de um sistema de computadores". Embora destas ações, em si mesmo consideradas possam também resultar danos de natureza patrimonial, inclusive de carácter permanente se não for facultada à vítima a chave de desencriptação, possibilitando a recuperação por esta do controle dos dados ou do sistema, o Passo 5). Ainda a este propósito, cabe acentuar que o objetivo de obter "para si

---

[30] "Article 8 – **Computer-related fraud**
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
a any input, alteration, deletion or suppression of computer data,
b any interference with the functioning of a computer system,
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person".

[31] "Article 8 – **Fraude informatique**
Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:
a par toute introduction, altération, effacement ou suppression de données informatiques;
b par toute forme d'atteinte au fonctionnement d'un système informatique,
dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.".

[32] "Artigo 8º – **Burla informática**
Cada Parte adoptará as medidas legislativas e outras que se revelem necessária para estabelecer como infracção penal, em conformidade com o seu direito interno, o acto intencional e ilegítimo, que origine a perda de bens a terceiros através:
a) Da introdução, da alteração, da eliminação ou da supressão de dados informáticos;
b) De qualquer intervenção no funcionamento de um sistema informático,
com a intenção de obter um benefício económico ilegítimo para si ou para terceiros.".

[33] "Artigo 8.º – **Burla informática**
Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu direito interno, quando praticado intencional e ilicitamente, o prejuízo patrimonial causado a outra pessoa por meio de:
a) Qualquer introdução, alteração, apagamento ou supressão de dados informáticos;
b) Qualquer interferência no funcionamento de um sistema informático;
com intenção de obter para si ou para outra pessoa um benefício económico ilegítimo."

ou para outrem, vantagem econômica ilícita" integra apenas o elemento subjetivo do tipo.

No que respeita ao bem jurídico penalmente protegido, a própria redação do preceito aponta, em termos inequívocos, para o património da vítima. Aliás, no mesmo sentido, como antecipámos, da *Minuta* consta, explicitamente, que o "objetivo deste artigo é o de penalizar toda e qualquer manipulação indevida durante o tratamento de dados, cuja intenção seja a de efectuar uma transferência indevida de propriedade." (Ponto 36).

O que deverá ser entendido para além de uma consideração estática dos bens em propriedade, incluindo também todas as situações jurídicas de natureza patrimonial, além dos poderes de livre disposição das mesmas através de atos de natureza negocial. Consequentemente, a confiança dos operadores económicos dos mercados na integridade e fiabilidade nos sistemas e redes de computadores é também protegida, ainda que reflexamente.

Por outro lado, a referência a uma ação "não autorizada", pelo próprio titular do sistema ou pela lei, incluindo quem tivesse autorizado acesso ao sistema, embora não para a prática de tais ações, resultando na manipulação dos dados ou do sistema, obriga a considerar o controlo exclusivo destes também no âmbito dos bens jurídicos protegidos pelo crime de "Fraude informática".

Cabe ainda acrescentar que a tentativa, iniciada com o começo das ações mencionadas na previsão típica, será tendencialmente punível[34]. O mesmo não ocorrendo com os atos preparatórios[35].

3. Os concursos pensáveis

Como veremos em seguida, os vários Passos correspondentes aos ataques de ramsonware são suscetíveis de preencherem as previsões típicas de outros crimes constantes da *Convenção* para além da "Fraude informática", o que suscita necessariamente a questão dos concursos, embora não apenas com o tipo que identificámos como primário.

Todavia, para um tal exercício, apenas poderemos contar com os textos das previsões normativas e, sobretudo, com a consideração dos bens jurídicos protegidos, na falta de referências quanto às medidas das penas ou da atribuição das iniciativas processuais aos lesados e ou ao Ministério Público, cuja determinação caberá às Partes ao adequarem as respectivas leis à *Convenção*.[36]

---

[34] Nos termos do previsto no Artigo 11 parágrafo 2, embora as Partes possam reservar-se o direito de não o fazer, conforme a parágrafo 3.

[35] Pois o crime correspondente ao "Uso indevido de aparelhagem" (Artigo 6) apenas prevê a obrigatoriedade para as Partes no que se refere aos tipos "Crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador" e não aos "Crimes informáticos", como ocorre com a "Fraude informática" ou a "Falsificação informática", o mesmo valendo para os "Crimes relacionados ao conteúdo da informação" ou a "Violação de direitos autorais e de direitos correlatos".

[36] Sobre estas questões, tem um particular interesse o estudo, no contexto da *Convenção de Budapeste*, de P.D. VENÂNCIO (2013, 99-105), assim como, no âmbito do Direito português, embora desde perspectivas várias, mas quase sempre tendo por referência subjacente a *Convenção*, de D.R. NUNES (2017, 41-48), D.R. (2019, 69-82), assim como os

a) com a "Violação de dados" (Artigo 4) **e** com a "Interferência em sistema" (Artigo 5) Antes de mais, temos dois tipos cujos objetos e conteúdos das respetivas ações coincidem com os da "Fraude informática", pelo que os trataremos conjuntamente. Assim, no que se refere à "Violação de dados"[37], resulta que:

> "1. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a danificação, a eliminação, a deterioração, a alteração ou a supressão dolosas e não autorizadas de dados de computador.
> 2. Qualquer Parte pode reservar-se o direito de exigir que da conduta descrita no parágrafo 1 resulte sério dano para a vítima."

A este propósito, quanto a uma questão de especial pertinência para o nosso objeto de estudo, ao corresponder ao Passo 1) dos ataques de ransomware, a Minuta esclarece que: "A introdução de códigos dolosos, tais como vírus e rotinas tais como os chamados "cavalos de Tróia", encontra-se pois abrangida por este parágrafo da mesma maneira que a modificação dos dados resultante deste acto." (Ponto 61)
Por sua vez, a propósito da "Interferência em sistemas", temos que:

> "Cada Parte adotará medidas legislativas semelhantes e outras providências necessárias para tipificar como crime, em sua legislação interna, qualquer grave obstrução ou impedimento, dolosos e não autorizados, do funcionamento de um sistema de computador por meio da inserção, transmissão, danificação, apagamento, deterioração, alteração ou supressão de dados de computador."

Sempre seguindo a *Minuta*, se na "Violação de dados" "[…] os interesses jurídicos protegidos são a integridade e o adequado funcionamento ou a correcta utilização dos dados ou programas informáticos armazenados." (Ponto 60), na "Interferência em sistemas", o mesmo "reside no interesse de operadores

---

contributos sintéticos, tendo por referência o crime de "Burla informática", de C.G. PEDRA (2019, 25-29), de C. RODRIGUES (2019, 54-60), de D.S. PALMA (2019, 86-89) e de P.L.R. MOTA (2019, 178-180).

[37] Manifestamente, esta terminologia não é feliz por coincidir com a usualmente usada, também no Brasil, para referir os incidentes de segurança conduzindo a violações de segurança de dados pessoais, os "vazamentos de dados", conforme ao Artigo 48 da Lei n. 13.709, de 14 de agosto de 2018, a *Lei Geral de Proteção de Dados Pessoais*, sobre estas questões, por todos, M.D. MASSENO, G.M. MARTINS & J.L. FALEIROS Jr. (2020). Aliás, neste caso, a versão brasileira não apenas se afasta da oficiosa, a qual prefere a designação "Interferência nos dados", como da portuguesa e cabo-verdiana, "Dano provocado nos dados", sendo esta também objeto de críticas ao indiciar um mimetismo excessivo com o crime de "Dano", como também das oficiais "Data interference" e "Atteinte à l'intégrité des données".

e utilizadores de sistemas informáticos e de telecomunicações em que os mesmos apresentem um funcionamento adequado." (Ponto 65).

Nestas bases, embora a consumação de cada um de estes crimes seja suscetível de afetar o património das vítimas, o mesmo não surge em primeira linha. Aliás, sobretudo no que se refere à "Interferência em sistemas", poderão estar em causa interesses sociais gerais, muito para além dos enunciados na Minuta. Sendo certo estarmos perante dois crimes de resultado e de dano, pois a respectiva consumação constitui um dano para o bem jurídico protegido.

Do mesmo modo, na respeitante ao elemento subjetivo de ambos os tipos, não está prevista qualquer intenção de natureza patrimonial, quer em prejuízo da vítima, quer em proveito próprio.

O que afastará a viabilidade de estarmos perante um concurso aparente, por consumpção, de estes tipos relativamente à "Fraude informática" no caso dos ataques de ransomware, embora seja pensável relativamente a outras condutas enquadráveis na previsão típica, como as transferências bancárias ilícitas[38].

Sem esquecer que as consequências dos ataques alcançam frequentemente bens jurídicos que extravasam acentuadamente o património das vítimas, mesmo quando os valores dos pagamentos exigidos são muito menores que os resultantes das interferências, muitas vezes atingindo a sociedade no seu conjunto. O que suscita ou a previsão legal de formas qualificadas de estes tipos ou o recurso a outros já presentes nos Ordenamentos penais, desde que passíveis de também aplicarem em meios digitais.

O que também permite ampliar a criminalização ao que seriam atos preparatórios dos ataques, por força do disposto a propósito do "Uso indevido de aparelhagem" (Artigo 6), não previsto para a "Fraude informática", como verificámos. Precisamente,

> "1. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, as seguintes condutas, quando dolosas e não autorizadas:
> a. a produção, venda, aquisição para uso, importação, distribuição ou a disponibilização por qualquer meio de:
> i. aparelho, incluindo um programa de computador, desenvolvido ou adaptado principalmente para o cometimento de quaisquer dos crimes estabelecidos de acordo com os artigos de 2 a 5;
> ii. uma senha de computador, código de acesso, ou dados similares por meio dos quais se possa acessar um sistema de computador ou qualquer parte dele, com a intenção de usá-lo para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5; e

[38] Sobre o *modus operandi* de estas, C.F. BARREIRA (2015), embora desde uma perspectiva diferente.

> b. a posse de qualquer dos instrumentos referidos nos parágrafos a.i ou ii, com a intenção de usá-los para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5. Qualquer Parte pode exigir, por lei, a posse de um número mínimo de tais instrumentos, para que a responsabilidade criminal se materialize" […] [39]

b) com a "Falsificação informática" (Artigo 7)

Neste caso, também coincidem os objetos e os conteúdos das ações com os da "Fraude informática", embora restritamente aos dados, nos seguintes termos:

> "Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a inserção, alteração, apagamento ou supressão, dolosos e não autorizados, de dados de computador, de que resultem dados inautênticos, com o fim de que sejam tidos como legais, ou tenham esse efeito, como se autênticos fossem, independentemente de os dados serem ou não diretamente legíveis e inteligíveis. Qualquer Parte pode exigir, para a tipificação do crime, o seu cometimento com intenção de defraudar ou com outro objetivo fraudulento."[40]

Porém, diferem o não terem de ser dados alheios e o resultado consistente na obtenção de "dados inautênticos, com o fim de que sejam tidos como legais, ou tenham esse efeito, como se autênticos fossem". O que configura um crime de perigo, ao não ser exigida a efetivação do dano.

Adicionalmente, a *Minuta* assume que: "Neste caso, o interesse jurídico protegido será o da segurança e da credibilidade dos dados eletrónicos que poderão ter consequências ao nível das relações jurídicas." (Ponto 81, in fine).

O que extravasa também o âmbito patrimonial, alcançando o interesse geral relativo à segurança jurídica e a fiabilidade das transações eletrónicas, mesmo sem incidência económica.

---

[39] O preceito acrescenta ainda que "[…]
2. Este Artigo não deve ser interpretado para estabelecer responsabilidade criminal quando a produção, venda, aquisição para uso, importação, distribuição ou disponibilização por qualquer meio ou a posse referidos no parágrafo 1 deste Artigo não se destine à prática de qualquer dos crimes tipificados de acordo com os artigos 2 a 5 desta Convenção, como para, por exemplo, a realização de testes autorizados ou a proteção de um sistema de computador.
3. Cada Parte pode reservar-se o direito de não aplicar o parágrafo 1 deste Artigo, desde que a reserva não se refira à venda, distribuição ou a disponibilização por qualquer meio, dos itens ou instrumentos referidos no parágrafo 1 a.ii deste Artigo.".

[40] Sobre a configuração de este tipo, também com referências à *Convenção*, embora essencialmente centrado nas fontes portuguesas, é de indicar o estudo de D.R. NUNES (2017).

Sempre no contexto dos ataques de ransomware, esta previsão abrangerá as condutas orientadas à produção de mensagens falsas de correio eletrónico, criadas com o objetivo de induzir as vítimas a ativarem programas que encriptarão dados, incluindo programas (Phishing e Spear Phishing), ou de páginas simuladas, de modo a obterem as identificações e as palavras-passe das vítimas (Pharming), embora esta seja uma prática muito menos comum neste contexto[41].

Consequentemente, estaremos perante um concurso efetivo com a "Fraude informática", correspondendo a uma das vias para o Passo 1) dos ataques.

c) e ainda com o "Acesso ilegal" (Artigo 2)

Em cujos termos,

> "Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, o acesso doloso e não autorizado à totalidade de um sistema de computador ou a parte dele. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento mediante a violação de medidas de segurança; com o fim de obter dados de computador ou com outro objetivo fraudulento; ou contra um sistema de computador que esteja conectado a outro sistema de computador". [42]

Quanto ao bem jurídico protegido, ainda segundo a Minuta, está em causa "A necessidade de protecção reflecte os interesses de organizações e indivíduos em gerir, operar e controlar os seus sistemas de forma livre e tranquila." (Ponto 44) Por outras palavras, é procurada a segurança dos sistemas de computadores, de modo a manter a confiança dos particulares e das empresas, assim como dos mercados e da sociedade em geral, na respectiva segurança, confidencialidade e integridade, incluindo os dados presentes nos mesmos.

Em extrema síntese, será este um crime de perigo abstrato, não relevando qualquer dano ou dolo específico, designadamente de índole patrimonial.

---

[41] Para uma caraterização de ambas práticas, têm bastante interesse a exposição detalhada de C.F. BARREIRA (2015, 25-30), assim como as referências de D.R. NUNES (2019, 69-70).

[42] A propósito deste tipo, analisando as mudanças a resultarem da Convenção para *a Lei da Criminalidade Informática* então vigente em Portugal, a Lei n.º 109/91, de 17 de agosto <https://diariodarepublica.pt/dr/detalhe/lei/109-1991-674438>, têm muito interesse as considerações de R. BRAVO (2003), enquanto eu me ocupei da respetiva comparação com o previsto na Diretiva 2013/40/UE, do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa *a ataques contra os sistemas de informação* e que substitui a Decisão-Quadro 2005/222/JAI do Conselho <https://eur-lex.europa.eu/eli/dir/2013/40/oj?locale=pt> e com a *Lei Carolina Dieckmann*, Lei nº 12.737, de 30 de novembro de 2012*, dispõe sobre a tipificação criminal de delitos informáticos*; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> , M.D. MASSENO (2018b).

Consequentemente, na perspectiva da "Fraude informática" em geral, apenas estaremos perante um concurso real se o acesso for obtido diretamente por meios técnicos (Hacking) ou através de Pharming, nos termos antes mencionados. Sendo ideal sempre que os ataques de ransomware se processem através de uma injeção de código malicioso, assim como nos casos de "inserção, alteração, apagamento ou supressão de dados de computador" ou de a "interferência no funcionamento de um computador ou de um sistema de computador" ser operada por quem estiver autorizado a aceder ao sistema, mas não a operar as referidas ações, sendo esta última via muito pouco comum.

4. Algumas, brevíssimas, considerações conclusivas

Nos próximos meses, cumprindo o previsto, o Congresso Nacional deverá adequar o brasileiro a este novo enquadramento. O que implicará uma reforma legislativa ampla e sistemática, inclusive reformulando intervenções recentes, como as introduzidas pela Lei nº 14.155, de 27 de maio de 2021, tendo por objeto realidades suscetíveis de caírem no âmbito da "Fraude informática" como a mesma está concebida na Convenção, com a tipificação da "Fraude eletrônica" e do "Furto mediante fraude"[43].

Em suma, embora o interesse expresso do Brasil estivesse sobretudo na Cooperação Internacional com as demais Partes da Convenção, surge agora uma oportunidade para atualizar também o seu Direito Penal Material. Espero ter dado um pequeno contributo para esse desiderato.

[43] Precisamente, esta Lei *altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato* <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm>, sobre a mesma e suas dissonâncias com a Convenção, embora brevemente, M.D. MASSENO (2023b).

Referências bibliográficas:

BARREIRA, C.F. (2015). "Home banking: A Repartição dos prejuízos decorrentes de fraude informática". RED – Revista Eletrónica de Direito, 3. Disponível em: <https://bit.ly/4bbAD7h>.

BRAVO, R. (2003). "O Crime de Acesso Ilegítimo na Lei da Criminalidade Informática e na CiberConvenção". Direito n@ Rede, 3. Disponível em: <https://bit.ly/3tY2OWk>.

CARVALHO, F.P., MORALES G., O. & ÁLVAREZ F., M. (2018). "Regulamentação supranacional sobre Criminalidade Informática e Técnicas de Transposição. O Direito Penal Português e Espanhol como Paradigmas". Actualidad Jurídica Uría Menéndez, 48, 48-64. Disponível em: <https://www.uria.com/documentos/publicaciones/5801/documento/art04.pdf>.

MASSENO, M.D. (2018a). Os ataques de "Ransomware" na "Convenção de Budapeste" e no Direito Penal da União Europeia. II Congresso Nacional de Direito Digital. Comissão de Direito Digital da Seção de Santa Catarina da Ordem dos Advogados do Brasil, Florianópolis. Disponível em: <https://bit.ly/48Ukuku>.

MASSENO, M.D. (2018b). "Da criminalização do "acesso ilícito" (hacking) nos Ordenamentos do Brasil e de Portugal". CALHEIROS, C. et al. (Eds.), Direito na lusofonia : direito e novas tecnologias. Braga: Escola de Direito da Universidade do Minho, 279-288. Disponível em: <https://bit.ly/3SfnC3L>.

MASSENO, M.D. (2023a). Das Fontes Internacionais e Europeias da Cibercriminalidade. Aula ao XII Curso de Mestrado em Direito e Informática da Escola de Direito da Universidade do Minho, Braga. Disponível em: <https://bit.ly/3U3XtYk>.

MASSENO, M.D. (2023b). Os Tipos Penais Brasileiros perante a Convenção de Budapeste sobre o Cibercrime, principais problemas de adequação. Porto Alegre: WB Educação. Disponível em: <https://bit.ly/46cuLXM>.

MASSENO, M.D., MARTINS, G.M. & FALEIROS Jr. (2020). "A Segurança na Proteção de Dados: Entre o RGPD Europeu e a LGPD Brasileira". Revista do CEJUR/TJSC: Prestação Jurisdicional, 8(1), e346. Disponível em: <https://revistadocejur.tjsc.jus.br/cejur/article/view/346>.

MASSENO, M.D. & WENDT, E. (2017). "O Ransomware na Lei: Apontamentos Breves de Direito Português e Brasileiro". Revista Eletrônica Direito & TI, 1(8). Disponível em: <https://direitoeti.com.br/direitoeti/article/view/80>.

MOTA, P.L.R. (2019). "Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual". PEREIRA, L. M. C. S. et al. (Eds.), O Crime de Abuso de Cartão de Garantia e Crédito e o Crime de Burla Informática (Trabalhos do 2.º Ciclo do Curso de Formação – Ministério Público). Lisboa: Centro de Estudos Judiciários, 167-192. Disponível em: <https://bit.ly/4aV3soa>.

NUNES, D.R. (2017). "O crime de falsidade informática". JULGAR Online. Disponível em: <https://julgar.pt/o-crime-de-falsidade-informatica/>.

NUNES, D.R. (2019). "O fenómeno do Ransomware e o seu enquadramento jurídico-penal". Cyberlaw by CIJIC, 8, 58-82. Disponível em: <https://www.iuris.edu.pt/xms/files/Cyberlaw-by-CIJIC_8.pdf >.

NUNES, D.R. (2019). "Reflexões sobre as alterações às disposições penais materiais da Lei do Cibercrime". Privacy and Data Protection Magazine - Revista Científica na Área Jurídica, 5, 11-50. Disponível em: <https://www.europeia.pt/resources/media/documents/Revista_Privacy_Data_Protection_Magazine_N5.pdf>.

PALMA, D.S. (2019). "Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual". PEREIRA, L. M. C. S. et al. (Eds.), O Crime de Abuso de Cartão de Garantia e Crédito e o Crime de Burla Informática (Trabalhos do 2.º Ciclo do Curso de Formação – Ministério Público). Lisboa: Centro de Estudos Judiciários, 73-105. Disponível em: <https://bit.ly/4aV3soa>.

PEDRA, C.G. (2019). "Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual". PEREIRA, L. M. C. S. et al. (Eds.), O Crime de Abuso de Cartão de Garantia e Crédito e o Crime de Burla Informática (Trabalhos do 2.º Ciclo do Curso de Formação – Ministério Público). Lisboa: Centro de Estudos Judiciários, 11-38. Disponível em: <https://bit.ly/4aV3soa>.

PINTO, J.C. (2023). Ransomware - Ameaça Crescente às Empresas. Lisboa: Instituto Superior de Economia e Gestão da Universidade de Lisboa. Disponível em: <https://bit.ly/48PPrGC>.

RODRIGUES, C. (2019). "Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual". PEREIRA, L. M. C. S. et al. (Eds.), O Crime de Abuso de Cartão de Garantia e Crédito e o Crime de Burla Informática (Trabalhos do 2.º Ciclo do Curso de Formação – Ministério Público). Lisboa: Centro de Estudos Judiciários, 39-71. Disponível em: <https://bit.ly/4aV3soa>.

VENÂNCIO, P.D. (2013). "Similarity and Competition Between Cybercrimes Related to Computer Data in the Council of Europe's Convention on Cybercrime". Masaryk University Journal of Law and Technology, 7(1), 97-105. Disponível em: <https://journals.muni.cz/mujlt/article/view/2629>. Acesso em 30/01/2024.

VERDELHO, P. (2003). "A Convenção sobre Cibercrime do Conselho da Europa – Comentário". VERDELHO, P. et al. (Eds.): Leis do Cibercrime, I. Centro Atlântico: Vila Nova de Famalicão, 10-23. Disponível em: <https://bit.ly/3TUEM9r>.
Nota: todas as hiperligações foram verificadas no dia 30 de janeiro de 2024.

Inteligência Artificial e Arbitragem: Um Breve Estudo Sobre a Instrumentalização da Tecnologia em Procedimentos Arbitrais

Daniel Becker[44]

Ludmilla Campos[45]

Resumo

O artigo analisa a integração da Inteligência Artificial (IA) na arbitragem e suas implicações procedimentais e materiais. A IA aprimora a eficiência e reduz vieses cognitivos ao otimizar processos como gestão documental e predição jurisprudencial. No entanto, sua adoção traz desafios, como opacidade algorítmica (black boxes), assimetria tecnológica e a necessidade de equilibrar inovação e garantias processuais. Embora a regulamentação da IA na arbitragem seja necessária, regras excessivamente rígidas podem inibir inovação e investimentos. O debate deve reconhecer os altos padrões de transparência, ética e imparcialidade da arbitragem sem aplicá-los automaticamente à regulação geral da IA. O artigo propõe regulamentação risk-based, transparência algorítmica e governança auditável para alinhar avanços tecnológicos a princípios como contraditório, confidencialidade e igualdade processual.

Palavras-chave: Inteligência Artificial; Arbitragem; Processo Arbitral; Transparência Algorítmica; Regulamentação de IA; Disputas Tecnológicas.

[44] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

[45] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Abstract
The article examines the integration of Artificial Intelligence (AI) in arbitration and its procedural and substantive implications. AI enhances efficiency and reduces cognitive biases by optimizing processes such as document management and jurisprudential pattern prediction. However, challenges remain, including algorithmic opacity (black boxes), technological asymmetry, and the need to balance innovation with procedural safeguards. While AI regulation in arbitration is necessary, overly rigid rules may hinder innovation and investment. The debate must recognize arbitration's high standards of transparency, ethics, and impartiality without automatically extending its guidelines to broader AI regulation. The article proposes risk-based regulation, algorithmic transparency, and auditable governance to align technological advancements with fundamental principles such as due process, confidentiality, and procedural equality.

Kewwords: Artificial Intelligence; Arbitration; Arbitral Proceedings; Algorithmic Transparency; AI Regulation; Technological Disputes.

1. Inteligência Artificial e Arbitragem – Contexto e Perspectivas

A inteligência artificial (IA) transcendeu a esfera do futurismo especulativo para se consolidar como uma realidade disruptiva em múltiplos setores econômicos. Sua capacidade de otimizar processos produtivos, acelerar análises massivas de dados e redesenhar estruturas decisórias não poupou o universo jurídico. Na arbitragem, contudo, essa revolução assume contornos singulares: a natureza consensual e flexível desse método de resolução de disputas converte-o em um laboratório privilegiado para a experimentação tecnológica. Não se trata, porém, de mera adoção instrumental de ferramentas digitais, mas de uma reconfiguração estrutural que desafia paradigmas tradicionais — desde a condução processual até a epistemologia da decisão arbitral.

O avanço de sistemas baseados em *machine learning* e processamento de linguagem natural (PLN) oferece aos tribunais arbitrais ganhos tangíveis: eficiência procedimental (triagem automatizada de documentos, predição de padrões jurisprudenciais) e redução de vieses cognitivos (como a tendência humana à superconfiança em heurísticas). Entretanto, a euforia inovadora não pode obscurecer dilemas críticos. A arbitragem, alicerçada em princípios como confidencialidade e autonomia da vontade, enfrenta um paradoxo: como harmonizar a opacidade inerente a certos algoritmos (as chamadas "*black boxes*") com a exigência de transparência e previsibilidade que legitimam o sistema? A resposta, sugere-se, não reside na regulamentação prévia da tecnologia em si, mas na regulação *risk-based* de seus *usos concretos*.

A interação entre IA e arbitragem opera em duas esferas complementares. Na esfera procedimental, a tecnologia otimiza a gestão de provas e a construção de argumentos: ferramentas como *LEX MACHINA* utilizam algoritmos preditivos para mapear padrões em milhares de precedentes, acelerando a identificação de inconsistências e conexões relevantes. Na esfera material, surgem novas categorias de disputas, como aquelas envolvendo a interpretação de cláusulas em contratos automatizados ou a responsabilidade por decisões tomadas por sistemas autônomos. Esses casos exigem dos árbitros não apenas expertise jurídica, mas também compreensão técnica para dialogar com cientistas de dados e decifrar a lógica operacional de algoritmos complexos — um horizonte que redefine as fronteiras tradicionais da prática arbitral.

Críticos argumentam que a automação de etapas processuais poderia coisificar a arbitragem, transformando-a em um mero exercício algorítmico (SUSSKIND, 2019). Tal visão, contudo, subestima o papel humano na interpretação de cláusulas ambíguas ou na ponderação de princípios concorrentes. A IA, nesse contexto, atua menos como substituta e mais como amplificadora cognitiva: ao liberar profissionais de tarefas repetitivas (análise de milhares de documentos), permite que concentrem esforços em estratégias de litígio sofisticadas e na construção de argumentos jurídicos criativos.

O cerne do debate, portanto, não é se a IA será integrada à arbitragem, mas como fazê-lo da melhor forma. Questões como a imparcialidade algorítmica, que exige mecanismos de auditoria para evitar discriminação indireta em sistemas de recomendação utilizados por árbitros, a necessidade de

assegurar o contraditório em ambientes opacos, garantindo que as partes possam entender e contestar decisões baseadas em algoritmos preditivos, e a validação técnica, que levanta a discussão sobre a exigência de certificação independente para ferramentas de IA empregadas em procedimentos arbitrais, permanecem centrais nesse cenário.

A experiência do Silicon Valley Arbitration & Mediation Center (SVAMC), pioneiro na criação de diretrizes para uso de inteligência artificial em arbitragem com foco em inovação e padrões éticos, reforça a tese de que modelos setoriais flexíveis podem superar regulamentações estatais excessivamente prescritivas, desde que fundamentados em critérios claros de transparência algorítmica e governança auditável. O caminho à frente, assim, exige equilíbrio: aproveitar o potencial transformador da IA (análise em tempo real de jurisprudência global, mitigação de assimetrias informacionais) enquanto se blindam valores essenciais do devido processo arbitral. A alternativa não é estagnação, mas inovação responsável — onde tecnologia e garantias jurídicas coexistem em simbiose crítica.

2. Inteligência Artificial como Ferramenta Prática no Procedimento Arbitral – Um Estudo Procedimental

A integração da inteligência artificial nos procedimentos arbitrais, deve-se dizer, não se resume a uma mera modernização tecnológica: trata-se de uma reengenharia pragmática de práticas consolidadas, capaz de redefinir desde a gestão de casos até a epistemologia da decisão final. Longe de ser um recurso meramente acessório, a IA emerge como uma parceira estratégica em todas as fases do processo, oferecendo soluções que otimizam a eficiência sem, contudo, esvaziar o papel decisório humano. Essa simbiose entre algoritmo e expertise jurídica revela-se não apenas viável, mas indispensável em um cenário global marcado pela complexidade crescente de disputas transnacionais e pela explosão de dados jurídicos digitais.

A adoção da IA na arbitragem opera em múltiplas camadas, adaptando-se às necessidades específicas de cada ator envolvido. Para árbitros, transforma-se em um *assistente cognitivo*, capaz de identificar padrões em milhares de precedentes; para tribunais, converte-se em um *gestor procedural*, automatizando prazos e garantindo compliance; para advogados, atua como um *estrategista preditivo*, antevendo movimentos da contraparte; e para as partes, funciona como um *mediador informacional*, reduzindo assimetrias por meio da democratização de análises jurídicas complexas.

Este capítulo desvenda essa atuação multifacetada, analisando criticamente como a IA é operacionalizada em cada esfera do procedimento arbitral. O foco recairá não apenas nos benefícios tangíveis (velocidade, redução de custos, precisão), mas também nos desafios operacionais e éticos inerentes a essa transformação – como a preservação do contraditório em ambientes algorítmicos e o risco de superconfiança em outputs tecnológicos. Ao mapear casos concretos e tendências setoriais, busca-se demonstrar que a IA,

quando calibrada com precisão jurídica, não é incompatível com a arbitragem nem se propõe a substituí-la.

2.1. Uso de IA pelos Árbitros

A integração de sistemas de inteligência artificial na atuação dos árbitros representa uma evolução inevitável diante da complexidade crescente das disputas comerciais globais. A capacidade da IA de processar grandes volumes de dados, identificar padrões em jurisprudência e automatizar tarefas repetitivas tem sido amplamente reconhecida como um avanço para a eficiência arbitral. No entanto, essa incorporação não ocorre sem tensões, especialmente quando envolve atividades tradicionalmente dependentes do discernimento humano, como a ponderação de provas e a interpretação de cláusulas contratuais ambíguas.

Já em 2018, a ICCA divulgou uma série de estudos aprofundados que analisam a integração de tecnologias digitais no âmbito da arbitragem internacional. Dentre esses trabalhos, destaca-se o relatório elaborado pela Força-Tarefa ICCA-Queen Mary sobre Financiamento por Terceiros (ICCA, 2018), o qual explora como a automação de procedimentos arbitrais pode gerar ganhos operacionais significativos.

Contudo, a aplicação da IA em atividades de maior subjetividade jurídica permanece controversa. Sistemas de análise preditiva de resultados, como o Lex Machina (usado para prever tendências em litígios), suscitam debates sobre a padronização excessiva do direito. Críticos argumentam que tais ferramentas podem incentivar uma abordagem formulista da arbitragem, na qual argumentos são moldados para se adequar a padrões algorítmicos, em vez de refletirem as nuances específicas do caso.

A **assimetria tecnológica** entre as partes também emerge como uma preocupação relevante. Em arbitragens envolvendo empresas de países com acesso desigual a tecnologias avançadas, a utilização de ferramentas preditivas por um único litigante pode distorcer o equilíbrio processual. Relatórios recentes alertam que a disparidade tecnológica na arbitragem pode violar o princípio da igualdade processual, especialmente quando uma parte não tem recursos para auditar ou contestar ferramentas algorítmicas utilizadas contra si. A Câmara de Comércio Internacional (ICC), em seu Guia sobre Inteligência Artificial na Arbitragem (ICC, 2022), alerta que o acesso desigual a tecnologias preditivas pode distorcer o equilíbrio entre as partes, privilegiando aquelas com maior capacidade financeira (cf. seção 4.2 do relatório). Para mitigar esse risco, instituições como a Câmara de Comércio Internacional recomendam a divulgação prévia do uso de IA e a disponibilização de versões simplificadas dos sistemas para a contraparte.

No plano regulatório, iniciativas como as Diretrizes emitidas pela CIArb (**CIArb, s.d.)** buscam equilibrar inovação e segurança jurídica. Entre suas recomendações, destacam-se: ***(i)*** auditorias independentes para detectar vieses em algoritmos; ***(ii)*** obrigação de árbitros declararem o uso de ferramentas preditivas em suas decisões; e ***(iii)*** proibição de sistemas que substituam a

avaliação humana de questões como credibilidade de testemunhas ou aplicação de princípios de equidade.

O **futuro da IA na arbitragem** dependerá da capacidade de instituições e profissionais em estabelecer protocolos claros de governança. O letramento digital dos árbitros – de todas as demais partes envolvidas – será crucial: cursos sobre funcionamento básico de algoritmos e identificação de vieses já são oferecidos por entidades como a Universidade de Harvard e o Chartered Institute of Arbitrators. Paralelamente, o desenvolvimento de algoritmos *explicáveis* (*XAI*), que permitem rastrear a lógica decisória, surge como uma frente promissora para conciliar tecnologia e transparência.

Sem dúvidas, a IA não substitui a essência humana da arbitragem, mas redefine suas fronteiras operacionais. Cabe aos árbitros, como garantidores da legitimidade do processo, assegurar que a tecnologia sirva para aprimorar, e não para corroer, os pilares do sistema arbitral: celeridade, especialidade e justiça consensual. A regulamentação, neste contexto, deve focar em mitigar riscos concretos (como vieses e assimetrias), evitando restrições prévias que obstruam o potencial transformador da inovação.

2.2. Uso de IA pelas Partes e pelos Advogados

A integração de sistemas de inteligência artificial por advogados e partes em procedimentos arbitrais reflete uma evolução inevitável e desejável na advocacia contemporânea. Em um cenário de disputas cada vez mais complexas e transnacionais, a IA surge não como substituta, mas como parceira estratégica, ampliando a capacidade humana de análise, predição e gestão processual. Seu potencial transformador, no entanto, demanda uma governança pragmática, que mitigue riscos sem engessar a inovação — um equilíbrio que já começa a se consolidar na prática arbitral global.

Na gestão documental, ferramentas como Relativity e DISCO revolucionaram a fase de e-discovery, automatizando a triagem de milhões de e-mails e contratos. Em casos de grande escala, algoritmos de NLP podem ser empregados para identificar padrões em comunicações internas, acelerando a fase probatória. Contudo, a eficácia desses sistemas depende da qualidade dos dados e da supervisão humana, pois erros na filtragem automatizada podem excluir documentos críticos, reforçando a necessidade de revisão cuidadosa.

A redação assistida por IA também ganha espaço, com ferramentas como Casetext, gerando rascunhos atualizados. No entanto, episódios como o caso Mata v. Avianca (EUA, 2023), onde advogados usaram ChatGPT e citaram precedentes fictícios, destacam a importância de diretrizes claras. A ICC recomenda a supervisão humana de ferramentas de IA em seu Relatório sobre Arbitragem e Inteligência Artificial (2021), alinhando-se a precedentes como Mata v. Avianca, que exigem verificação humana dos outputs tecnológicos.

Os riscos éticos, como vazamentos em plataformas de nuvem, são reais, mas gerenciáveis. No caso Schrems II (CJUE, 2020), tribunais exigiram transparência em ferramentas de transferência de dados, estabelecendo precedentes para auditorias técnicas.

O futuro da advocacia arbitral reside na integração responsável de humanos e máquinas. Como resume Professor Richard Susskind (Oxford, 2023), *'a IA não substitui advogados, mas redefine suas competências*. A regulação deve ser habilitadora: protocolos como a ABA Resolution 112 (American Bar Association, 2019) exigem transparência no uso de IA, enquanto cláusulas adaptativas preveem auditorias, como no contrato-modelo da UNCITRAL.

2.3. Uso de IA pelas Instituições Arbitrais

Ao automatizar tarefas repetitivas e oferecer *insights* estratégicos, a IA permite que Mais do que uma ferramenta, a IA representa um paradigma operacional — uma reengenharia silenciosa de processos que permite às instituições manterem-se ágeis diante de litígios cada vez mais técnicos e multifacetados. Seu valor reside na capacidade de transformar gargalos históricos (como gestão manual de cronogramas ou análise morosa de precedentes) em oportunidades para reforçar a confiabilidade e acessibilidade do sistema arbitral, garantindo que princípios como celeridade e especialização não sejam comprometidos pelo aumento da escala ou da complexidade.

A **seleção de árbitros** exemplifica como a IA pode aprimorar processos sem substituir o discernimento humano. Algoritmos são capazes de analisar milhares de perfis em segundos, identificando profissionais com expertise específica em disputas de energia, tecnologia ou comércio internacional. Imagine um sistema que, além de considerar experiência e formação, cruze dados sobre taxas de aceitação de teses jurídicas em casos semelhantes, sugerindo árbitros cujo perfil decisório alinha-se às complexidades do litígio. Contudo, a verdadeira inovação está em programar critérios éticos como diversidade geográfica e equilíbrio de gênero. Em vez de replicar vieses históricos — como a predominância de árbitros de economias desenvolvidas —, a IA pode ser calibrada para priorizar representatividade. Um exemplo hipotético: uma instituição que, após recalibrar seu algoritmo, aumentou em 35% a indicação de árbitros mulheres e de países em desenvolvimento para disputas de investimento, corrigindo distorções históricas. A IA, aqui, não é fim, mas meio para uma arbitragem mais inclusiva.

Na **gestão administrativa,** a automação é uma aliada inquestionável. Calcular custos, distribuir documentos e monitorar prazos são tarefas que consomem recursos humanos valiosos — recursos estes que poderiam ser realocados para análise estratégica de casos complexos.

A crítica de que a automação engessa procedimentos ignora um ponto crucial: a IA não define regras, apenas as executa conforme estabelecido pelas instituições. Cabe, então, aos usuários desses sistemas – ou seja, nós, humanos – garantirem que sistemas sejam configurados para permitir exceções quando a justiça assim exigir.

A **análise preditiva**, por sua vez, não deve ser temida como um oráculo determinista, mas celebrada como um mapa de tendências. Identificar padrões em decisões passadas não substitui o julgamento, mas o informa. Se um algoritmo

revela que cláusulas de *force majeure*[46] são interpretadas de forma distinta em disputas pós-pandemia, caberá ao árbitro, e não à máquina, decidir como aplicar esse *insight* ao caso concreto.

Os riscos existem, mas são geríveis mediante governança proativa. A transparência algorítmica, por exemplo, não exige a divulgação de segredos comerciais, mas a clareza sobre critérios usados em sistemas de seleção de árbitros ou cálculo de custos. Instituições como a London Court of International Arbitration (LCIA) têm adotado políticas para incorporar tecnologias emergentes, como algoritmos de inteligência artificial, em seus processos de arbitragem. Essas políticas visam garantir transparência e equidade, especialmente em relação a critérios como experiência, diversidade e custos. Embora a LCIA não divulgue publicamente os detalhes de seus algoritmos, enfatiza a importância de auditorias independentes para evitar vieses e discriminações. A International Chamber of Commerce (ICC, s.d.) também tem demonstrado compromisso com a diversidade e a imparcialidade em arbitragens, revisando periodicamente seus critérios de seleção de árbitros para garantir que não haja favorecimento inadvertido de grupos específicos.

A cibersegurança é outro pilar fundamental no uso de tecnologias em arbitragens, especialmente em disputas que envolvem patentes ou segredos industriais. A American Arbitration Association (AAA) tem implementado medidas robustas de proteção de dados, incluindo o uso de criptografia avançada em plataformas de armazenamento em nuvem. Além disso, tecnologias como zero-knowledge proofs[47] – protocolos criptográficos que permitem a um proponente demonstrar a veracidade de uma afirmação a um verificador sem revelar qualquer informação adicional além da própria veracidade da afirmação – têm sido adotadas para verificar a integridade de documentos sem expor seu conteúdo, garantindo confidencialidade e segurança. Essa tecnologia já é utilizada em arbitragens de propriedade intelectual na Europa, como

---

[46] No contexto da arbitragem, o conceito de força maior pode impactar a execução de obrigações contratuais e o cumprimento de prazos processuais. A aplicação desse instituto em arbitragens internacionais geralmente segue padrões estabelecidos por convenções e regras institucionais, como as Regras da Câmara de Comércio Internacional (ICC) e a Convenção das Nações Unidas sobre Contratos de Compra e Venda Internacional de Mercadorias (CISG, Art. 79). Em decisões arbitrais, a caracterização da força maior requer prova de que o evento era imprevisível, inevitável e tornou impossível o cumprimento da obrigação. Para uma análise aprofundada sobre o tema, ver Gaillard, E., & Savage, J. (1999). *Fouchard, Gaillard, Goldman on international commercial arbitration*. Kluwer Law International.

[47] Zero-Knowledge Proofs (ZKPs) são protocolos criptográficos que permitem a um proponente demonstrar a veracidade de uma afirmação a um verificador sem revelar qualquer informação adicional além da própria veracidade da afirmação. Esses protocolos garantem três propriedades fundamentais: (i) completude, onde um proponente honesto sempre convencerá um verificador honesto; (ii) solidez, impedindo que um proponente desonesto engane o verificador com alta probabilidade; e (iii) zero conhecimento, garantindo que nenhuma informação extra seja divulgada. ZKPs são amplamente utilizados em aplicações que exigem privacidade e segurança, como autenticação sem senha, transações financeiras anônimas em blockchain e sistemas de identidade digital descentralizados. Para um aprofundamento teórico, ver: Goldwasser, S., Micali, S., & Rackoff, **C.** (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on Computing, 18*(1), 186–208. https://doi.org/10.1137/0218012

demonstrado em estudos recentes sobre aplicações de blockchain e criptografia em disputas legais.

2.4. IA na Mediação e na Resolução Alternativa de Disputas

A digitalização dos métodos de resolução de disputas tem catalisado modelos inovadores, como Online Dispute Resolution (ODR), Crowdjury, Independent Legal Oracles (ILOs) e Smart Arbitration, que redefinem a interação entre tecnologia e justiça. Essas abordagens prometem eficiência e acesso democratizado, mas suscitam debates críticos sobre transparência, legitimidade e preservação de garantias processuais. Enquanto a inteligência artificial otimiza processos e reduz custos, sua aplicação em contextos decisórios exige uma reflexão aprofundada sobre os limites éticos da automação e os riscos de reducionismo jurídico.

O Online Dispute Resolution (ODR) tem se destacado como ferramenta eficiente e acessível para a resolução de disputas. Plataformas como Modria, desenvolvida por ex-colaboradores do eBay, utilizam algoritmos para mediar conflitos consumeristas, analisando padrões de casos anteriores para sugerir soluções.

O Crowdjury, modelo que envolve a participação coletiva de cidadãos leigos assistida por IA, tem sido testado em alguns países. A plataforma CrowdJury, por exemplo, permite que indivíduos contribuam financeiramente e opinem sobre casos legais, promovendo um maior engajamento público na justiça.

Os **Independent Legal Oracles (ILOs)** buscam conciliar blockchain e IA para emitir pareceres automatizados em disputas contratuais. Em ambientes de *DeFi* (finanças descentralizadas), plataformas como *Kleros* analisam cláusulas codificadas para resolver conflitos objetivos, como atrasos em pagamentos via criptomoedas.

A Smart Arbitration, integrada a contratos inteligentes, automatiza a execução de decisões quando condições pré-programadas são atendidas. Plataformas como Lex Machina utilizam IoT (Internet das Coisas) para monitorar cláusulas contratuais em tempo real, como atrasos em entregas, e executar penalidades automaticamente.

A ascensão desses modelos traz desafios e oportunidades. A transparência é essencial: como garantir explicabilidade sem sufocar a inovação? Em sistemas como o Crowdjury, onde decisões emergem da interação complexa entre humanos e algoritmos, a chave é construir modelos auditáveis sem impor burocracias desnecessárias. A responsabilidade também exige novas abordagens: em plataformas de resolução de disputas baseadas em IA, o foco deve estar na mitigação de riscos reais, e não na atribuição difusa de culpa. Quanto à segurança, o setor precisa priorizar arquiteturas resilientes, aprendendo com incidentes passados para fortalecer protocolos e prevenir vulnerabilidades exploráveis.

Diretrizes que equilibram inovação e segurança são essenciais. Em vez de regulamentos engessados, *frameworks* flexíveis, como os desenvolvidos por organismos internacionais, orientam boas práticas sem frear avanços. Auditorias

algorítmicas independentes são importantes, mas devem ser escaláveis e proporcionais ao impacto real dos sistemas. Em contratos inteligentes, mecanismos de intervenção humana são recomendáveis para exceções, mas sem comprometer a eficiência da automação. Por fim, a portabilidade de dados entre plataformas deve ser incentivada para evitar monopólios tecnológicos e ampliar a competitividade.

3. Acervo de Diretrizes e Regulamentações da IA nos Tribunais Arbitrais

A integração da inteligência artificial em tribunais arbitrais não ocorre em um vácuo normativo. Instituições arbitrais ao redor do globo, conscientes dos riscos e oportunidades, têm desenvolvido diretrizes específicas para regular o uso dessas tecnologias, garantindo que inovação e ética caminhem em paralelo. Essas regras, embora influenciadas por contextos legais regionais, compartilham um traço comum: o equilíbrio entre eficiência tecnológica e preservação de garantias fundamentais, como transparência, contraditório, sigilo e igualdade processual.

Nos Estados Unidos, a American Arbitration Association (AAA) e o Judicial Arbitration and Mediation Services (JAMS) têm publicado protocolos recomendando a divulgação prévia do uso de IA por partes e árbitros, além de orientações para garantir a auditabilidade de algoritmos empregados na análise de provas ou predição de resultados. Paralelamente, estados como Illinois e Califórnia avançaram em normas que restringem o uso de sistemas enviesados em processos decisórios, influenciando indiretamente a conduta de tribunais arbitrais sediados em seus territórios. Essa fragmentação reflete a tensão entre a autonomia das partes na arbitragem e a necessidade de padrões mínimos para evitar abusos tecnológicos.

O Silicon Valley Arbitration & Mediation Center, por exemplo, lançou um conjunto de Diretrizes sobre o Uso de IA na Arbitragem Internacional (SVAMC, 2024), estabelecendo princípios fundamentais para a adoção dessas tecnologias nos tribunais arbitrais. O documento enfatiza a importância da transparência na utilização de ferramentas de IA, a necessidade de divulgação do uso de algoritmos nos procedimentos e a preservação da independência dos árbitros na tomada de decisões assistidas por tecnologia.

As diretrizes do SVAMC também abordam preocupações específicas relacionadas à explicabilidade dos sistemas de IA na arbitragem. A falta de clareza sobre como determinados algoritmos chegam a suas conclusões pode comprometer a previsibilidade e a confiança nos procedimentos arbitrais. Para mitigar esse problema, o SVAMC recomenda a aplicação de mecanismos de auditoria e governança que permitam supervisão adequada do uso da IA, garantindo que seu impacto nos processos decisórios seja compreendido e controlado.

Na Ásia, destaca-se o pragmatismo de centros arbitrais como Singapura e Hong Kong, que combinam regulação estatal com iniciativas setoriais. Singapura exige que o processamento de dados por IA respeite finalidades específicas e

consentimento informado, princípios incorporados pelas regras do Singapore International Arbitration Centre (SIAC).

Organizações internacionais também contribuem para esse acervo normativo. A Câmara de Comércio Internacional (ICC), por meio de sua Comissão de Arbitragem e Alternative Dispute Resolution, publicou em 2022 o relatório Leveraging Technology for Fair, Effective and Efficient International Arbitration Proceedings (ICC, 2022), que inclui diretrizes sobre ética digital. O documento recomenda, por exemplo, que, caso as partes desejem utilizar IA generativa — por exemplo, para traduzir materiais —, seja obtida a concordância da parte adversa, sob risco de comprometer a integridade do processo.

Já a Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL), em seu Grupo de Trabalho III, debateu a modernização das Regras Modelo de Arbitragem para abordar desafios tecnológicos.

Além disso, os Princípios da Comissão Europeia para a Eficiência da Justiça (CEPEJ) sobre IA e Justiça estabelecem diretrizes para o uso responsável da inteligência artificial nos sistemas judiciais, servindo de referência para o contexto arbitral. O documento reforça a necessidade de supervisão humana sobre decisões assistidas por IA e de garantir que qualquer tecnologia empregada respeite os princípios fundamentais do devido processo legal e da imparcialidade.

Essas iniciativas demonstram que, apesar das incertezas regulatórias, há um movimento global voltado à padronização do uso da inteligência artificial nos métodos alternativos de resolução de disputas. Contudo, a coexistência de múltiplos marcos regulatórios gera complexidade em arbitragens cross-border, nas quais partes de diferentes jurisdições podem ter expectativas dissonantes quanto ao uso de IA. Por exemplo, enquanto a Europa prioriza a proteção de dados, tribunais sob influência asiática podem valorizar a eficiência operacional, e instituições norte-americanas tenderem à autorregulação setorial. Essa disparidade exige que árbitros e advogados cultivem competência técnica para navegar conflitos normativos e garantir que a escolha de ferramentas digitais não comprometa a validade do laudo ou a igualdade processual.

O futuro desse acervo regulatório dependerá da convergência entre inovação responsável e legitimidade processual. Espera-se que padrões internacionais de soft law ganhem tração, servindo como referência para reformas legislativas e cláusulas contratuais.

Conclusão

A arbitragem contemporânea está diante de uma transformação inevitável: a inteligência artificial não é mais uma promessa distante, mas uma realidade que redefine práticas e expectativas. Seu êxito, contudo, dependerá menos da tecnologia em si e mais das escolhas feitas por seus operadores. A IA pode ser um vetor de eficiência, acessibilidade e qualidade decisória, desde que utilizada de forma criteriosa, potencializando a deliberação humana, sem substituí-la.

O desafio, portanto, não está na simples incorporação de novas ferramentas, mas na construção de um ecossistema que equilibre inovação e responsabilidade. Isso exige que árbitros desenvolvam novas competências, que instituições arbitrais estabeleçam diretrizes de transparência e que desenvolvedores de IA compreendam o impacto jurídico de seus sistemas. Mais do que um campo de experimentação tecnológica, a arbitragem pode se tornar um modelo para o uso responsável da IA no direito.

Muito se encoraja a regulamentação clara do uso de IA em procedimentos arbitrais, mas, para evitar exigências inviáveis e interpretações excessivamente amplas, é crucial delimitar seu escopo. Regras rígidas sobre transparência e explicabilidade, quando aplicadas indistintamente ao setor, podem frear a pesquisa, desencorajar investimentos e comprometer a inovação. No entanto, no contexto da arbitragem, a exigência de padrões elevados se justifica, pois o procedimento arbitral pressupõe um rigoroso dever de ética, transparência inquestionável e imparcialidade absoluta. Assim, o debate regulatório sobre IA deve reconhecer que as diretrizes específicas da arbitragem não podem ser automaticamente transpostas para o panorama regulatório mais amplo da tecnologia.

As orientações aqui propostas servem, então, como um guia valioso para a harmonização entre IA e arbitragem. Contudo, qualquer regulamentação futura — seja o Projeto de Lei de IA no Brasil, o AI Act europeu ou outros marcos normativos — precisará compreender a natureza singular da arbitragem e a necessidade de preservar seus princípios fundamentais. Estimular o uso da inteligência artificial na resolução de disputas é necessário e louvável, mas seu impacto só será positivo se acompanhado de diretrizes claras sobre seus limites, sua aplicação em cada fase do procedimento e os mecanismos para auditar sua influência nos resultados.

O devido processo legal, portanto, não pode ser um entrave à tecnologia, mas deve ser atualizado para acomodá-la sem comprometer os pilares da justiça arbitral. O futuro da arbitragem não será decidido por uma escolha binária entre tradição e disrupção, mas pela capacidade de equilibrar inovação e governança. Cabe à arbitragem, mais uma vez, liderar esse movimento, assegurando que a IA seja não um fim em si mesma, mas um instrumento a serviço da justiça, da eficiência e da confiança no procedimento arbitral.

Referências Bibliográficas

Susskind, R. (2019). *Online courts and the future of justice*. Oxford University Press.

Silicon Valley Arbitration and Mediation Center. (2024, 30 de abril). *Guidelines on the use of artificial intelligence in international arbitration*. Recuperado de https://svamc.org/svamc-publishes-guidelines-on-the-use-of-artificial-intelligence-in-arbitration/

Brasil. (2018). *Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018*. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

International Council for Commercial Arbitration (ICCA). (2018). *Report of the ICCA-Queen Mary Task Force on Third-Party Funding in International Arbitration*. Recuperado de https://cdn.arbitration-icca.org/s3fs-public/document/media_document/Third-Party-Funding-Report.pdf

International Chamber of Commerce (ICC). (2022). *Leveraging technology for fair, effective and efficient international arbitration proceedings*. Recuperado de https://iccwbo.org/news-publications/arbitration-adr-rules-and-tools/icc-arbitration-and-adr-commission-report-on-leveraging-technology-for-fair-effective-and-efficient-international-arbitration-proceedings/

Chartered Institute of Arbitrators (CIArb). (s.d.). *Professional Practice Guidelines*. Recuperado de https://www.ciarb.org/resources/professional-practice-guidelines/

Mata v. Avianca, Inc. (2023). *United States District Court for the Southern District of New York*, 678 F. Supp. 3d 443. Recuperado de https://casetext.com/case/mata-v-avianca-inc-3

Mildebrath, H. (2020). *The CJEU judgment in the Schrems II case*. European Parliamentary Research Service. Recuperado de https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

American Bar Association. (2019). *Resolution 112: Urging courts and lawyers to address ethical and legal issues related to artificial intelligence*. Recuperado de https://www.americanbar.org/content/dam/aba/directories/policy/annual-2019/112-annual-2019.pdf

United Nations Commission on International Trade Law (UNCITRAL). (1996). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998*. Recuperado de https://uncitral.un.org/en/texts/ecommerce/modellaw

International Chamber of Commerce (ICC). (s.d.). *Arbitration*. Recuperado de https://iccwbo.org/dispute-resolution/dispute-resolution-services/arbitration/

Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on Computing, 18*(1), 186–208. https://doi.org/10.1137/0218012

Martins, D. R. M., Butori, C., & Rezende, N. S. (2019). *Resolução de conflitos online e o case do Modria*. Recuperado de https://www.camesbrasil.com.br/resolucao-conflitos-online-case-modria/

Illinois General Assembly. (s.d.). *Artificial Intelligence Video Interview Act, 820 ILCS 42*. Recuperado de https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68

Gaillard, E., & Savage, J. (1999). *Fouchard, Gaillard, Goldman on international commercial arbitration*. Kluwer Law International.

Serrato, J. K., Mastromonaco, C., Arora, S. B., Caplan, A., Choo, E., Rendar, M., Watson, L., Voigts, A. M., Rivaux, S., Purcell, J., & Ajanaku, D. F. (2025, 7 de fevereiro). *California's AI laws are here—Is your business ready?* Pillsbury Law. Recuperado de https://www.pillsburylaw.com/en/news-and-insights/california-ai-laws.html

Personal Data Protection Commission (PDPC). (2024, 1 de março). *Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems.* Recuperado de https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-the-use-of-personal-data-in-ai-recommendation-and-decision-systems.pdf

International Chamber of Commerce (ICC). (2022). *Leveraging technology for fair, effective and efficient international arbitration proceedings.* Recuperado de https://iccwbo.org/wp-content/uploads/sites/3/2022/02/icc-arbitration-and-adr-commission-report-on-leveraging-technology-for-fair-effective-and-efficient-international-arbitration-proceedings.pdf

Miami International Arbitration Society (MIAS). (2024, 10 de fevereiro). *Report of the MIAS Task Force on "Technology-Related Dispute Resolution and Adjudication: Model Clauses and Guidance Texts"*. Recuperado de https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/comments_of_mias_february_2024.pdf

European Commission for the Efficiency of Justice (CEPEJ). (2018). *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment.* Recuperado de https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%

20-%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf

A conservação e utilização probatória de metadados após a Lei n.º 18/2024, de 5 de fevereiro

Duarte Rodrigues Nunes[48]

Resumo

O presente artigo analisa criticamente o atual regime jurídico da conservação e do acesso a dados de tráfego, de localização e de base (metadados) que tenham sido alvo de conservação prévia. Analisa-se igualmente a jurisprudência do TJUE em matéria de metadados posterior ao Acórdão Digital Rights e a jurisprudência do TEDH com relevância em matéria de admissibilidade da conservação para fins de investigação criminal e do acesso das autoridades competentes para a investigação criminal a metadados previamente conservados (apontando-se os riscos de o seguimento da jurisprudência do TJUE poder acarretar condenações por violação da CEDH). Por fim, também é analisada a questão de saber se o Tribunal Constitucional estava, ou não, obrigado a acolher a jurisprudência do TJUE em matéria de admissibilidade da conservação para fins de investigação criminal e do acesso das autoridades competentes para a investigação criminal a metadados previamente conservados.

Palavras-chave: metadados, conservação de dados, investigação criminal,Tribunal Constitucional, Tribunal de Justiça da União Europeia.

[48] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Abstract
This article critically analyses the current legal regime for of traffic, location and user data (metadata) retention and for access to metadata that have been subject to previous retention. The case-law of the CJEU on metadata subsequent to the Digital Rights Judgement and the case-law of the ECHR relevant to the admissibility of data retention for criminal investigation purposes and access by the competent authorities for criminal investigation to previously preserved metadata are also analysed (pointing out that following the case-law of the CJEU can lead to convictions for violation of the ECHR).
Finally, the issue of whether or not the Constitutional Court was obliged to follow the case-law of the CJEU on data retention for criminal investigation purposes and access by the competent authorities for criminal investigation to previously preserved metadata is also analysed.

Kewwords: metadada, data retention, criminal investigation, Constitutional Court, Court of Justice of the European Union.

1. Preliminares

No rescaldo dos terroristas de Madrid (11 de março de 2004) e de Londres (7 de julho de 2005), em que foi a reconstituição das comunicações eletrónicas entre os vários intervenientes das redes terroristas em causa e a determinação da localização dos seus telemóveis que permitiu às autoridades perceberem as relações existentes entre eles, o Parlamento Europeu e o Conselho adotaram a Diretiva 2006/24/CE, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, mas excluindo expressamente do seu âmbito de aplicação a conservação de dados de conteúdo de comunicações.

A Diretiva 2006/24/CE, que visou harmonizar as disposições dos Estados-Membros relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de dados de tráfego, dados de localização relativos pessoas singulares e/ou a pessoas coletivas e dados conexos necessários para identificar o assinante ou o utilizador registado por eles gerados ou tratados (correntemente designados como metadados[49]) para fins de investigação, deteção e repressão de crimes graves, tal como definidos no Direito nacional de cada Estado-Membro, veio impor aos Estados-Membros a adoção de medidas destinadas a garantir a conservação dos dados necessários para:

a) encontrar e identificar a fonte e/ou o destino de uma comunicação;

b) identificar a data, a hora e a duração de uma comunicação;

c) identificar o tipo de comunicação;

d) identificar o equipamento de telecomunicações dos utilizadores ou o que se considera ser o seu equipamento; e

e) identificar a localização do equipamento de comunicação móvel (incluindo no caso de chamadas telefónicas falhadas), quando gerados ou tratados e armazenados (no caso de dados telefónicos) ou registados (no caso de dados da Internet) por fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações que estejam sob a jurisdição do Estado-Membro em questão, no contexto da oferta de serviços de comunicação.

Tal Diretiva excluía expressamente do seu âmbito de aplicação a conservação de dados de conteúdo de comunicações (cfr. arts. 1.º, n.º 2, e 5.º, n.º 2).

---

* Professor Associado da Universidade Europeia e da Universidade Lusíada – Angola. Doutor em Direito pela Faculdade de Direito de Lisboa. Investigador integrado do Centro de Investigação de Direito Penal e Ciências Criminais e não integrado do Centro de Investigação Jurídica do Ciberespaço, ambos da Faculdade de Direito da Universidade de Lisboa. Jurisconsulto. Conferencista. Juiz de Direito (atualmente em situação de licença sem retribuição).

[49] Sem prejuízo do escasso rigor dessa designação.

A Diretiva 2006/24/CE foi transposta para a nossa ordem jurídica através da Lei n.º 32/2008, de 17 de julho.

Todavia, a Diretiva 2006/24/CE foi declarada inválida pelo TJUE no seu Acórdão Digital Rights Ireland Ltd e Kärntner Landesregierung, de 8 de abril de 2014[50].

Nesse aresto, o TJUE entendeu que a conservação e a utilização de metadados para fins de investigação criminal tal como estavam previstos na Diretiva restringiam, de forma intensa (embora sem afetar o seu conteúdo essencial), os direitos tutelados pelos arts. 7.º e 8.º da CDFUE, sendo que, nos termos do artigo 52.º, n.º 1, da Carta, qualquer restrição ao exercício dos direitos e liberdades garantidos pela CDFUE deve estar prevista na Lei e respeitar o conteúdo essencial desses direitos e liberdades e, por força dos ditames do princípio da proporcionalidade, só podem ser introduzidas restrições a esses direitos e liberdades se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União Europeia ou à necessidade de proteção dos direitos e liberdades de terceiros.

O TJUE considerou que, apesar de não ocorrer qualquer restrição do conteúdo essencial dos referidos direitos fundamentais e de estar em causa a prossecução de fins legítimos (a resposta à criminalidade grave e, em última análise, a salvaguarda da segurança pública), a Diretiva 2006/24/CE restringia, de forma desproporcionada, os mencionados direitos fundamentais, uma vez que:

a) abrangia, de uma forma indiscriminada, todas as pessoas que utilizassem serviços de comunicações eletrónicas, inclusivamente pessoas em relação às quais não existiam indícios de que o seu comportamento pudesse ter um nexo, ainda que indireto ou longínquo, com infrações graves e sem prever qualquer exceção quanto a comunicações abrangidas pela proteção do segredo profissional;

b) não exigia nenhuma relação entre os dados conservados e uma ameaça para a segurança pública nem limitava a conservação a dados relativos a um período de tempo, a uma zona geográfica determinada e/ou a um círculo de pessoas determinadas que possam estar implicadas, de alguma forma, numa infração grave nem a dados relativos a pessoas cuja conservação pudesse contribuir para a prevenção, a deteção ou a repressão de infrações graves;

c) não estabelecia critérios objetivos que permitissem delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior à prevenção, deteção ou punição de infrações graves;

d) não limitava o acesso e a utilização posterior dos dados conservados à prevenção e à deteção de crimes graves nem estabelecia critérios objetivos que permitam limitar o número de pessoas com autorização de acesso e de utilização posterior dos dados conservados ao estritamente necessário tendo em conta o objetivo prosseguido;

e) não exigia que o acesso aos dados conservados dependesse de um pedido fundamentado no âmbito de procedimentos de prevenção ou de

[50] Usualmente designado Acórdão Digital Rights.

deteção de crimes ou de uma ação penal e fosse objeto de controlo prévio por um órgão jurisdicional ou entidade administrativa independente e também não obrigava os Estados-Membros a preverem esses requisitos no seu Direito interno;

f) no que respeita à duração da conservação dos dados, que impunha que fosse fixada entre 6 e 24 meses, não procedia a qualquer distinção entre as categorias de dados em função da sua eventual utilidade relativamente ao objetivo prosseguido ou em função das pessoas em causa nem impunha que a determinação do período de conservação deveria basear-se em critérios objetivos, a fim de garantir que se limitava ao estritamente necessário; e

g) quanto à segurança e à proteção dos dados conservados pelos fornecedores de serviços de comunicações eletrónicas, (1) não obrigava os Estados-Membros a estabelecerem regras específicas e adaptadas à grande quantidade de dados cuja conservação era imposta, ao caráter sensível desses dados e ao risco de acesso ilícito aos mesmos, (2) não garantia a aplicação, pelos referidos fornecedores, de um nível particularmente elevado de proteção, (3) não impunha a destruição definitiva dos dados no termo do período de conservação dos mesmos e (4) não impunha a obrigação de os metadados serem conservados no território da União Europeia (pelo que não se poderia considerar que estivesse plenamente garantida a fiscalização do respeito das exigências de proteção e de segurança por uma entidade independente, tal exigido pelo art. 8.º, n.º 3, da CDFUE).

Na sequência do Acórdão Digital Rights, passou a discutir-se se a compatibilidade, ou não, da Lei n.º 32/2008 com o Direito da União Europeia e se, consequentemente, a conservação de dados à luz dessa Lei era, ou não, admissível à luz da CRP e da CDFUE[51].

Do mesmo modo, agindo como se de um Tribunal se tratasse, a CNPD decidiu "desaplicar" a Lei n.º 32/2008 (por considerar que violava a CDFUE e o art. 18.º, n.º 2, da CRP), deixando de cumprir as funções de fiscalização a que estava (e está) adstrita nos termos da Lei n.º 32/2008[52].

Contudo, a principal consequência, entre nós, do Acórdão Digital Rights foi o Acórdão do TC n.º 268/2022, em que o TC, embora com um voto de vencido, declarou inconstitucionais, com força obrigatória geral:

a) a norma constante do art. 4.º da Lei n.º 32/2008, conjugada com o art. 6.º da mesma Lei, por violação do disposto nos arts. 35.º, n.ºs 1 e 4, e 26.º, n.º 1, em conjugação com o art. 18.º, n.º 2, todos da CRP; e

b) a norma constante do art. 9.º da Lei n.º 32/2008 (na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida

---

[51] *Vide* a este respeito, com maiores desenvolvimentos, DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, pp. 22-23.

[52] Cfr. Deliberação n.º 1008/2017

ou integridade física de terceiros), por violação do disposto nos arts. 35.º, n.º 1, e 20.º, n.º 1, em conjugação com o art. 18.º, n.º 2, todos da CRP[53].

c) Esta declaração da inconstitucionalidade veio suscitar a questão da admissibilidade, ou não, da obtenção e valoração, nos processos em curso, de metadados que tenham sido conservados pelos respetivos operadores e das provas obtidas através desses metadados. E, ainda mais grave, o aresto do TC abriu a possibilidade de serem interpostos recursos de revisão ao abrigo do art. 449.º, n.º 1, als. e) e f), do CPP, que, caso fossem julgados procedentes, poderiam conduzir à anulação de condenações transitadas em julgado em processos em que, tendo sido salvaguardadas todas as garantias do arguido, ficara provado, para além da dúvida razoável, o cometimento do crime ou dos crimes pelos quais os arguidos foram condenados[54].

2. A jurisprudência do TJUE posterior ao Acórdão Digital Rights

Após ter anulado a Diretiva 2006/24/CE, o TJUE passou a apreciar a questão da conservação e utilização de metadados previamente conservados na investigação criminal com base no art. 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho, conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, interpretado à luz dos arts. 7.º, 8.º e 52.º, n.º 1, da CDFUE, nos Acórdãos:

a) Tele2 Sverige AB;
b) Ministerio Fiscal;
c) Privacy International;
d) La Quadrature du Net;
e) Prokuratuur;
f) G. D. e Commissioner of An Garda Síochána;
g) Acórdão SpaceNet e Telekom Deutschland[55]; e
h) Acórdão Procura della Repubblica presso il Tribunale di Bolzano.

De acordo com esta jurisprudência do TJUE – que, salvo no caso do Acórdão Procura della Repubblica presso il Tribunale di Bolzano, foi estritamente acolhida pelo TC no seu Acórdão n.º 800/2023 –, a CDFUE impõe que os dados sejam

---

[53] Note-se, porém, que o TC (tal como o TJUE, embora relativamente à CDFUE), em momento algum considerou inconstitucional a utilização probatória de metadados nem a obtenção de metadados em tempo real (no mesmo sentido, RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", *in* RMP, n.º 172, pp. 35 e ss.).

[54] No entanto, tais recursos têm sido julgados improcedentes pelo STJ (cfr., entre outros, Acórdãos do STJ de 21/09/2022, 10/11/2022, 19/01/2023, 01/02/2023, 11/05/2023, 21/06/2023, 29/06/2023, 31/01/2024 e 15/05/2024), com fundamento no disposto no art. 282.º, n.º 3, 2.ª parte, da CRP, porquanto o TC, no Acórdão n.º 268/2022 não afastou a ressalva dos casos julgados, entendimento cuja bondade não cumpre analisar no âmbito do presente artigo, atento o respetivo objeto.

[55] Sobre os arestos referidos nas als. a) a g), com maior detalhe, DUARTE RODRIGUES NUNES, "O Day After do Acórdão do Tribunal Constitucional n.º 268/2022", *in* Privacidade e Proteção de Dados do Município de Lisboa, pp. 176 e ss.

conservados no território da União Europeia e proíbe a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, a título preventivo, para efeitos de luta contra a criminalidade grave e de prevenção de ameaças graves contra a segurança pública, mas permite:

1. A conservação generalizada e indiferenciada de dados de tráfego e de dados de localização para salvaguarda da segurança nacional, quando o Estado-Membro em causa enfrente uma ameaça grave, real e atual ou previsível, desde que essa conservação apenas ocorra durante um período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça, contanto que a decisão que determina a conservação seja fiscalizada por um Tribunal ou entidade administrativa independente, cuja decisão seja vinculativa;
2. A conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, desde que delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;
3. A conservação generalizada e indiferenciada, por um período temporalmente limitado ao estritamente necessário, dos endereços IP, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional; e
4. A conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública.

E, relativamente ao acesso aos metadados conservados, a CDFUE apenas permite o acesso aos dados conservados para efeitos de luta contra a criminalidade grave e desde que esse acesso esteja sujeito a controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente (que não pode ser o MP, pois é o titular da ação penal). A este respeito, no Acórdão Procura della Repubblica presso il Tribunale di Bolzano, o TJUE considerou que o acesso a dados de tráfego e de localização para investigação de infrações penais puníveis com uma pena máxima de prisão igual ou superior a 3 anos autorizado pelo Juiz é conforme à CDFUE desde que existam indícios suficientes da prática de tais infrações e esses dados sejam relevantes para o apuramento dos factos.

Finalmente, no Acórdão A. G. e Lietuvos Respublikos generalinė prokuratūra, o TJUE analisou uma questão diversa: saber se é admissível, à luz da CDFUE, a utilização, em investigações relativas a ilícitos disciplinares concernentes a atos de corrupção, de metadados que haviam sido conservados pelos prestadores de serviços de comunicações eletrónicas, tendo concluído pela não admissibilidade.

1. A jurisprudência dos tribunais comuns na sequência do Acórdão do Tribunal Constitucional n.º 268/2022

No seguimento do Acórdão do TC n.º 268/2022, surgiram, na jurisprudência dos tribunais comuns, dois entendimentos em matéria de obtenção e/ou valoração de metadados conservados[56].

Para um primeiro entendimento, por força da declaração de inconstitucionalidade com força obrigatória geral dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008, não é admissível obter e a valorar, em processos penais, metadados conservados à luz da Lei n.º 41/2004 e obtidos à luz do art. 189.º, n.º 2, do CPP ou da Lei n.º 109/2009[57].

Diversamente, para um segundo entendimento, a declaração de inconstitucionalidade com força obrigatória geral dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008 não impede a obtenção e a valoração, em processos penais, com base nos arts. 187.º a 189.º do CPP e na Lei n.º 109/2009, de metadados conservados à luz da Lei n.º 41/2004, pois essas normas não foram declaradas inconstitucionais[58].

3. O Tratado da União Europeia e a Carta dos Direitos Fundamentais da União Europeia *vs.* a Convenção Europeia dos Direitos Humanos e a Constituição da República Portuguesa

Tanto o Acórdão Digital Rights do TJUE como o Acórdão do TC n.º 268/2002 consideraram apenas os direitos fundamentais consagrados nos arts. 7.º e 8.º da CDFUE e 20.º, n.º 1, 26.º, n.º 1, e 35.º, n.ºs 1 e 4, da CRP.

Todavia, existem outros direitos fundamentais protegidos pela CDFUE[59] que foram, pura e simplesmente, ignorados pelo TJUE, sendo certo que a ponderação de interesses à luz do princípio da proporcionalidade tem de considerar *todos* os interesses contrapostos, precisamente porque essa ponderação visa obter uma concordância prática entre esses mesmos interesses. Além disso, o princípio da

---

[56] Sobre esta questão, com maiores desenvolvimentos, DUARTE RODRIGUES NUNES, "O Day After do Acórdão do Tribunal Constitucional n.º 268/2022", *in* Privacidade e Proteção de Dados do Município de Lisboa, pp. 182 e ss.

[57] Acolhido nos Acórdãos da RL de 25/10/2022, da RP de 07/09/2022, 07/12/2022 e 24/05/2023, da RC de 12/10/2022 e da RE de 25/10/2022, 28/02/2023, 09/05/2023 e 12/09/2023.

[58] Acolhido nos Acórdãos do STJ de 21/06/2023, da RL de 26/01/2023 e 22/02/2023, da RP de 29/03/2023, da RC de 21/06/2023 e 27/09/2023, da RE de 28/06/2023 e da RG de 02/05/2023.

[59] De facto, a CDFUE também garante, no seu art. 6.º, os direitos à liberdade e à segurança, bem como, noutros preceitos, diversos direitos fundamentais que constituem o referente constitucional de bens jurídicos tutelados por diversos tipos de crime particularmente graves e cuja prevenção e repressão são essenciais num Estado de Direito, como, por exemplo, os direitos à vida (art. 2.º), à integridade pessoal (art. 3.º), a não ser escravizado nem alvo de redução à servidão ou sujeito a tráfico de seres humanos (art. 5.º), à propriedade (art. 17.º), à saúde (art. 35.º), ao ambiente (art. 37.º), a uma boa Administração (art. 41.º), à ação e a um Tribunal imparcial (art. 47.º), etc., que, na nossa ótica, não foram tidos em conta pelo TJUE. E o mesmo sucede, inclusivamente, com os direitos ao respeito pela vida privada e familiar (art. 7.º) e à proteção de dados pessoais (art. 8.º), que também podem ser lesados por via da prática de crimes, pelo que não podem ser considerados apenas para justificar a limitação da utilização de medidas de investigação criminal.

proporcionalidade foi considerado apenas na sua vertente de proibição do excesso, desconsiderando-se totalmente a vertente de proibição de insuficiência desse mesmo princípio[60], sobretudo quando está em causa, entre outras finalidades, a luta contra a criminalidade grave[61].

E o TC incorreu na mesma falha, ao também não considerar minimamente (ou se o considerou, tal não resulta do texto do Acórdão n.º 268/2022) os interesses (obviamente legítimos) prosseguidos por via da administração da Justiça penal (onde se inclui a investigação criminal e mesmo a prevenção criminal *ante delictum*), que visam a proteção dos direitos fundamentais dos cidadãos[62] contra o crime e não o engrandecimento do Estado[63]. E, como sabemos, para que a criminalização de uma conduta seja admissível, terá de estar em causa a proteção de um bem jurídico essencial à convivência comunitária e ao livre desenvolvimento da pessoa, que terá de estar relacionado com um direito fundamental ou com um interesse constitucionalmente protegido, sendo os bens jurídico-penais concretizações dos valores constitucionais expressa ou implicitamente ligados aos direitos e deveres fundamentais e à ordenação social, política e económica[64]; deste modo, no caso dos crimes que integram o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008, está em causa a proteção de alguns dos bens mais relevantes à luz da ordem de valores jurídico-constitucional[65].

Apesar de tanto o TJUE, na jurisprudência posterior ao Acórdão Digital Rights que referimos, como o TC, no Acórdão n.º 800/2023, referirem que levaram

---

[60] Acerca do princípio da proporcionalidade na vertente de proibição de insuficiência e da sua aplicação no âmbito do Direito penal e processual penal, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 311 e ss.

[61] A que podemos subsumir a criminalidade organizada, o terrorismo, a criminalidade económico-financeira, a criminalidade violenta e outras formas de criminalidade, como os crimes sexuais (mesmo quando não impliquem o uso de violência e não sejam cometidos para obtenção financiamento do terrorismo e/ou de lucro para grupos criminosos organizados) ou mesmo os crimes puníveis com pena de prisão cujo limite máximo seja superior a 5 anos.

[62] De resto, o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008, inclui crimes gravíssimos, como sejam: homicídio doloso, ofensa à integridade física grave, mutilação genital feminina, ofensa à integridade física agravada pelo resultado, violência doméstica, violação, coação sexual, abuso sexual de menores, roubo, extorsão, associação criminosa, tráfico de órgãos, tráfico de pessoas, tráfico de armas, tráfico de droga, corrupção, tráfico de influência, participação económica em negócio, branqueamento de capitais, grupo terrorista, terrorismo, financiamento do terrorismo, rapto, sequestro agravado, tomada de reféns, escravidão, tortura, etc. De todo o modo, afigura-se-nos que este catálogo é excessivamente restritivo, não se percebendo, o porquê de ser mais restritivo do que o catálogo dos arts. 187.º, n.º 1, do CP e 18.º, n.º 1, da Lei n.º 109/2009, que regulam meios de obtenção de prova que restringem direitos fundamentais de um forma muito mais intensa.

[63] Cfr. DUARTE RODRIGUES NUNES, Curso de Direito Processual Penal, 1, p. 147.

[64] Cfr. FIGUEIREDO DIAS, Direito Penal, Parte Geral, Tomo I, 3.ª Edição, pp. 136 e ss., e DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, 2.ª Edição, p. 88.

[65] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 33.

a cabo uma ponderação de interesses, as suas decisões acabaram por traduzir-se na criação de sérias dificuldades ao nível da investigação de crimes e/ou de formas de criminalidade extremamente graves, de que poderá resultar uma proteção insuficiente – tanto à luz da CDFUE como à luz da CRP – de direitos fundamentais[66] e, desse modo, violações graves do princípio da proporcionalidade na vertente de proibição de insuficiência.

Ainda no que tange à CDFUE, há que ter em conta o disposto no seu art. 53.º, nos termos do qual, «*Nenhuma disposição da presente Carta deve ser interpretada no sentido de restringir ou lesar os direitos do Homem e as liberdades fundamentais reconhecidos, nos respetivos âmbitos de aplicação, pelo direito da União, o direito internacional e as Convenções internacionais em que são Partes a União ou todos os Estados-Membros, nomeadamente a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, bem como pelas Constituições dos Estados-Membros*».

Daqui resulta que a aplicação da CDFUE não pode conduzir a uma menor proteção de direitos fundamentais do que a proteção proporcionada por outros instrumentos de Direito internacional (como a CEDH) ou das Constituições dos Estados-Membros, sendo que a prevenção e a repressão de crimes graves são justificadas e mesmo impostas, no plano jurídico-constitucional, enquanto mecanismos de proteção dos bens jurídico-penais e, consequentemente, de direitos fundamentais[67].

No caso da CRP, cumpre considerar o art. 8.º, n.º 4, nos termos do qual, as normas do Direito da União Europeia são aplicáveis na ordem jurídica portuguesa nos termos definidos pelo Direito da União Europeia (incluindo a sua interpretação pelo TJUE), *mas sempre com respeito pelos princípios fundamentais do Estado de Direito Democrático*, sendo que esta reserva constitucional prevista na parte final do n.º 4 do art 8.º da CRP, nas palavras de GOMES CANOTILHO/VITAL MOREIRA[68], «*poderá considerar-se como uma norma de colisão explícita, pois ela torna claro que o princípio do primado do direito da União está limitado por núcleo essencial da Constituição – princípios fundamentais do Estado de direito democrático – que funcionarão como uma espécie de «reserva de ordem pública constitucional» («teoria dos contratualistas») contra eventuais preceitos ou disposições do direito da União aniquiladores da estadualidade (Estado), juridicidade (Estado de direito), democraticidade (Estado de direito constitucional) e fundamentalidade de direitos básicos (Estado de direitos fundamentais)*».

No fundo, esta reserva constitucional do art. 8.º, n.º 4, *in fine*, da CRP corresponde *grosso modo* à ressalva contida no art. 53.º da CDFUE.

---

[66] Desde logo, no caso do Direito português, os direitos fundamentais a que se reconduzem os bens jurídicos tutelados pelos crimes elencados no art. 2.º, n.º 1, al. g), da Lei n.º 32/2008.

[67] Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 334 e ss. (sobretudo na p. 336), e voto de vencido do Juiz Schluckebier na Sentença do BVerfG de 02/03/2010.

[68] GOMES CANOTILHO/VITAL MOREIRA, Constituição Anotada, I, 4.ª Edição, p. 267.

Ainda no que concerne ao Direito da União Europeia, nos termos do art. 6.º, n.º 2 e 3, do TUE (na versão *oficial* portuguesa):

«*2. A União adere à Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. Essa adesão não altera as competências da União, tal como definidas nos Tratados.*

3. Do direito da União fazem parte, enquanto princípios gerais, os direitos fundamentais tal como os garante a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais e tal como resultam das tradições constitucionais comuns aos Estados-Membros».

Ainda que, formalmente, a UE não tenha aderido à CEDH e, pelo menos, as versões inglesa e espanhola refiram que a UE "aderirá" e que os direitos fundamentais garantidos pela CEDH "farão parte" do Direito da União Europeia enquanto princípios gerais de direito, pelo menos nas versões portuguesa, italiana, alemã e francesa, refere-se que a UE "adere" e que os direitos fundamentais garantidos pela CEDH "fazem parte" do Direito da União Europeia enquanto princípios gerais de direito. Por isso, do ponto de vista material, tendo em conta, não apenas o art. 6.º, n.ºs 2 e 3, do TUE, mas sobretudo o art. 53.º da CDFUE, a UE, do ponto de vista material, está vinculada à CEDH e os direitos fundamentais garantidos pela CEDH tal como interpretados pelo TEDH integram o Direito da União Europeia. E não podemos olvidar que os Estados-Membros da UE são igualmente Estados-Membros do Conselho da Europa, estando, por isso, sujeitos à CEDH e à jurisprudência do TEDH.

Deste modo, a CEDH, tal como interpretada pelo TEDH, prevalece sobre a CDFUE e a jurisprudência do TJUE[69], que cedem igualmente perante a CRP nos casos em que esta conceda uma melhor proteção dos direitos fundamentais[70], sendo que, como referimos, a prevenção e a repressão de crimes graves são justificadas e mesmo impostas, no plano jurídico-constitucional, enquanto mecanismos de proteção dos bens jurídico-penais e, consequentemente, de direitos fundamentais[71].

E, como veremos já a seguir, o TEDH considera que a proteção dos direitos fundamentais inclui o dever de as autoridades levarem a cabo uma investigação efetiva e eficaz (o que inclui a obrigação de utilizar os meios de investigação que, não violando o disposto na CEDH, se mostrem necessários no caso concreto) dos crimes que lesem ou ponham em perigo algum dos direitos fundamentais garantidos pela CEDH. De resto, não faltam casos de condenação de Estados por ineficácia da investigação criminal em virtude do não uso de meios

---

[69] Como resulta dos arts. 6.º, n.ºs 2 e 3, do TUE e 53.º da CDFUE.

[70] Cfr. arts. 53.º da CDFUE e 8.º, n.º 4, *in fine*, da CRP.

[71] Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 334 e ss. (sobretudo na p. 336), e voto de vencido do Juiz Schluckebier na Sentença do BVerfG de 02/03/2010.

E, como referimos, os crimes que integram o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 protegem alguns dos bens mais relevantes à luz da ordem de valores jurídico-constitucional (cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 33).

investigatórios que se mostravam necessários para investigar os crimes em causa no caso concreto.

4. A jurisprudência do Tribunal Europeu dos Direitos Humanos

Nos Acórdãos Big Brother Watch e Outros c. Reino Unido e Centrum för rättvisa c. Suécia, em que estava em causa a apreciação da compatibilidade da interceção massiva (e, como tal, generalizada e indiferenciada) de informáticos relativos a dados de conteúdo de comunicações e de dados de tráfego (*bulk interception*) com o art. 8.º da CEDH, o TEDH considerou que esta interceção massiva não viola o art. 8.º da CEDH, desde que se verifiquem as seguintes condições mínimas:

- O Direito interno prever, de forma clara, os pressupostos da interceção massiva de dados de conteúdo e de dados de tráfego, a duração da execução da medida, o procedimento relativo ao exame, utilização e conservação dos dados recolhidos, as precauções a observar na transmissão dos dados a outras entidades e em que circunstâncias os dados deverão ser destruídos;
- Haver, em todas as fases de implementação da medida um controlo efetivo (por uma entidade independente do poder executivo, que não tem de ser um Juiz);
- O Direito interno prever mecanismos que permitam às pessoas que suspeitem de que os seus dados foram alvo de interceção em massa contestar a legalidade da medida e/ou a compatibilidade do regime da interceção em massa com a CEDH, sem dependência de qualquer notificação de que os seus dados foram alvo da medida; e
- A entidade competente para apreciar a impugnação (que não tem de ser um Tribunal) terá de ser independente do poder executivo e a sua decisão terá de ser juridicamente vinculativa para o poder executivo.

O TEDH também tem entendido que a proteção dos direitos fundamentais inclui o dever de as autoridades levarem a cabo uma investigação efetiva e eficaz dos crimes que atentem contra algum dos direitos fundamentais garantidos pela CEDH (desde logo, no caso de homicídios, tendo em conta o disposto no art. 2.º da CEDH[72]), o que inclui a obrigação de serem utilizados os meios de investigação que se mostrem necessários para a descoberta da verdade material e para a recolha de provas no caso concreto.

No que concerne à obtenção de metadados em investigações criminais, o TEDH tem considerado que a não obtenção de metadados cuja obtenção se mostre necessária para a investigação de crimes cometidos através da Internet ou com utilização da Internet é incompatível com o art. 8.º da CEDH (que também inclui um dever positivo de as autoridades levarem a cabo uma investigação efetiva e eficaz relativamente a crimes que lesem os direitos

[72] Cfr. Acórdãos McCann e Outros c. Reino Unido, Mahmut Kaya c. Turquia, Hugh Jordan c. Reino Unido, Paul e Audrey Edwards c. Reino Unido, Nachova e Outros c. Bulgária, Kaya e Outros c. Turquia, Ramsahai e Outros c. Países Baixos, Angelova e Iliev c. Bulgária, Opuz c. Turquia, Kolevi c. Bulgária, Al-Skeini e Outros c. Reino Unido, Vasîlka c. Moldávia, Jaloud c. Países Baixos, Mustafa Tunç e Fecire Tunç c. Turquia e Armani da Silva c. Reino Unido.

fundamentais tutelados por esse preceito da CEDH) nos casos em que tal puser em causa a eficácia da investigação[73].

De resto, no Acórdão K.U. c. Finlândia é particularmente evidente a censura do TEDH à excessiva importância que foi atribuída pelas autoridades finlandesas à confidencialidade dos dados de tráfego dos internautas na investigação de uma situação em que um determinado indivíduo publicou um anúncio na Internet, o que levou a que um menor fosse alvo de abordagens de pedófilos; dado que a Lei finlandesa em vigor, que visava proteger a liberdade de expressão e o direito à expressão anónima e protegia os autores de mensagens anónimas na Internet, impedia as autoridades de ordenarem ao fornecedor de serviços que lhes disponibilizasse metadados que, muito provavelmente, poderiam ter permitido a identificação do agente da infração, as autoridades não haviam lançado mão desse meio de obtenção de prova, o que votara a investigação ao insucesso.

Finalmente, no Acórdão Breyer c. Alemanha, o TEDH considerou que a Lei alemã em matéria de conservação de metadados não viola o art. 8.º da CEDH, cumprindo todos os requisitos do n.º 2 desse preceito. No entanto, à luz da Lei alemã, apenas é possível a conservação de dados reconduzíveis à categoria dos dados de base.

5. O regime da conservação e da obtenção de metadados atualmente em vigor

Na sequência da declaração de inconstitucionalidade com força obrigatória geral dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008[74], a Assembleia da República aprovou alterações aos arts. 4.º, 6.º e 9.º (bem como a outros preceitos) da Lei n.º 32/2008.

Remetido o decreto para promulgação, o Presidente da República solicitou a fiscalização preventiva da constitucionalidade das normas constantes desse decreto.

Em sede de fiscalização preventiva da constitucionalidade, o TC proferiu o Acórdão n.º 800/2023, que voltou a pronunciar-se no sentido da inconstitucionalidade da conservação generalizada e indiferenciada de dados de localização e de dados de tráfego, embora com três votos de vencido, dois dos quais, de juízas que haviam votado o Acórdão n.º 268/2022.

Comparando o Acórdão n.º 800/2023 com o Acórdão n.º 268/2022, denota-se que, ao passo que, no Acórdão n.º 268/2022, o TC seguiu estritamente o Acórdão Digital Rights, no Acórdão n.º 800/2023 seguiu estritamente a jurisprudência posterior do TJUE, passando a admitir a conservação de metadados em determinadas situações e a sua utilização probatória exatamente nos mesmos termos em que são admitidos pelo TJUE[75].

---

[73] Cfr. Acórdãos K.U. c. Finlândia, Khadija Ismayilova c. Azerbaijão e Volodina c. Rússia (n.º 2).

[74] Cfr. Acórdão do TC n.º 268/2022.

[75] *Vide* a nossa crítica aos Acórdãos do TC n.ºs 268/2022 e 800/2023 e à jurisprudência do TJUE em que aqueles acórdãos de basearam em DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, pp. 9

Os fundamentos da declaração de inconstitucionalidade constante do Acórdão n.º 800/2023 poderão sintetizar-se nos seguintes termos:

a) Os dados de localização tanto podem ser subsumidos à categoria dos dados de base (quando identificam a posição geográfica do aparelho, independentemente de qualquer comunicação) como à categoria dos dados de tráfego (quando a identificação da posição geográfica do aparelho está associada a uma comunicação ou tentativa de comunicação), sendo que, na maioria das situações, são subsumíveis à categoria dos dados de tráfego[76] – e, com isto, o TC logra reconduzir os dados de localização aos dados de tráfego e, assim, abrangê-los na declaração de inconstitucionalidade;

b) A conservação dos dados de tráfego e de localização restringe os direitos à intimidade/privacidade e à autodeterminação informacional de uma forma mais intensa do que no caso dos dados de base, sendo que essa restrição é também desproporcionada, atenta a sua especial danosidade para tais direitos fundamentais;

c) A conservação dos dados de tráfego e de localização só será admissível se for levada a cabo de uma forma seletiva, para que não sejam conservados dados de cidadãos que não são suspeitos de qualquer atividade criminosa atual nem futura;

d) As modificações introduzidas nos arts. 4.º e 6.º da Lei n.º 32/2008 em matéria de dados de tráfego e de localização tiveram apenas a ver com os prazos de conservação e, por isso, o juízo de inconstitucionalidade formulado no Acórdão n.º 268/2022 não foi superado.

Na sequência da declaração de inconstitucionalidade parcial do decreto da Assembleia da República que aprovara as alterações à Lei n.º 32/2008, o Presidente da República acabou por vetar esse decreto na sua totalidade.

Após a Assembleia da República yer aprovado um novo decreto, o Presidente da República promulgou o novo decreto, que veio a entrar em vigor como Lei n.º 18/2024, de 5 de fevereiro.

Tendo em conta as questões que motivaram as declarações de inconstitucionalidade, limitar-nos-emos às alterações introduzidas nos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008, sem prejuízo de uma referência ao art. 11.º da mesma Lei,

---

e ss., e também em "O Day After do Acórdão do Tribunal Constitucional n.º 268/2022", *in* Privacidade e Proteção de Dados do Município de Lisboa, pp. 171 e ss., "Audição da Associação D3 – Defesa dos Direitos Digitais e de Duarte Rodrigues Nunes", Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República – Grupo de trabalho metadados e "A utilização probatória de metadados das telecomunicações após o Acórdão do Tribunal Constitucional n.º 268/2022", Centro de Estudos Judiciários, Formação Contínua de Magistrados.

[76] O que tende a nem sequer corresponder à realidade, pois, pelo menos, na esmagadora maioria das situações, os dados de localização respeitam apenas à localização do dispositivo e, ainda que o utilizador tenha realizado alguma comunicação, se forem solicitados ao operador os dados de localização daquele dispositivo, o operador fornecerá apenas os dados de localização às autoridades e não também dados de tráfego "acoplados" aos dados de localização. Ademais, contrariamente ao que é referido no Acórdão n.º 800/2023, os dados de localização são uma tipologia de dados autónoma face aos dados de tráfego e aos dados de base (e também face aos dados de conteúdo).

relativo à destruição dos metadados que tenham sido transmitidos para o processo.

Começando pelo art. 4.º da Lei n.º 32/2008, cumpre referir a introdução da exigência de que a conservação dos metadados ocorra em Portugal ou no território de outro Estado-Membro da União Europeia no n.º 1 desse preceito, sendo, desse modo, dado cumprimento às exigências do TC e do TJUE e sem que daí resulte qualquer prejuízo para a investigação criminal. Quanto ao mais, o texto do art. 4.º da Lei n.º 32/2008 mantém-se idêntico ao texto que vigorava anteriormente ao Acórdão do TC n.º 268/2022.

Passando ao art. 6.º da Lei n.º 32/2008, esta norma prevê dois regimes de conservação: um para os dados de base e outro para os dados de tráfego e para os dados de localização.

Assim, quanto aos dados de base, nos termos do art. 6.º, n.º 1, da Lei n.º 32/2008, «*Para efeitos da finalidade prevista no n.º 1 do artigo 3.º, as entidades referidas no n.º 1 do artigo 4.º devem conservar, pelo período de um ano a contar da data da conclusão da comunicação, os seguintes dados:*

a) *Os dados relativos à identificação civil dos assinantes ou utilizadores de serviços de comunicações publicamente disponíveis ou de uma rede pública de comunicações;*

b) *Os demais dados de base;*

c) *Os endereços de protocolo IP atribuídos à fonte de uma ligação*».

Deste modo, no caso dos dados de base, a conservação é automática, não dependendo de qualquer decisão judicial nesse sentido, sendo os dados conservados durante 1 ano a contar da data da conclusão da comunicação. Contudo, fica sem se perceber qual será essa data, uma vez que não se trata de dados relativos a qualquer comunicação em concreto.

Relativamente aos dados de tráfego e de localização, que, por sinal, são aqueles que, tendencialmente mais relevam para a investigação, rege o disposto restantes números do art. 6.º da Lei n.º 32/2008.

Assim, nos termos do art. 6.º, n.ºs 2 e 7, da Lei n.º 32/2008, a conservação de dados de tráfego e de localização terá de ser autorizada por três Juízes do STJ (!), o que não se percebe, pois, no caso do inquérito, a sua instauração pressupõe a obtenção da notícia de um crime e, por isso, a conservação dos metadados será tendencialmente irrelevante, salvo no caso de crimes que sejam cometidos no decurso da investigação.

Além disso, fica sem se saber qual será a utilidade do art. 6.º, n.º 2, da Lei n.º 32/2008 face ao que já consta do art. 12.º da Lei n.º 109/2009 (preservação expedita de dados informáticos); de facto, ainda que o limite máximo da preservação expedita de dados informáticos seja de 3 meses, poderá ser sempre alvo de prorrogações até ao limite máximo de 1 ano, sendo que, não fixando o art. 6.º da Lei 32/2008 qualquer prazo máximo, o MP (ou mesmo o OPC, mediante ratificação do MP), desde que a conservação não deva estender-se por mais de 1 ano, nem precisa de solicitar qualquer autorização nos termos do art. 6.º da Lei n.º 32/2008, limitando-se a ordenar a preservação e a sua prorrogação nos termos do art. 12.º da Lei n.º 109/2009.

De todo o modo, na parte final do n.º 2 do art. 6.º da Lei n.º 32/2008, o legislador também prevê a utilizabilidade dos metadados conservados pelos operadores nos termos da Lei n.º 41/2004 (ou de outro diploma que venha a vigorar).

No caso dos metadados conservados pelos operadores nos termos da Lei n.º 41/2004 não será necessária qualquer autorização judicial para a conservação, sendo apenas necessária para o acesso, nos termos do art. 9.º da Lei n.º 32/2008. Admitindo-se, embora com reservas, que a conservação de metadados mediante a autorização prevista nos n.ºs 2, 3 e 7 do art. 6.º da Lei n.º 32/2008 possa ter alguma aplicabilidade/utilidade prática, o pedido de autorização judicial para conservação de dados de tráfego e de localização tem caráter urgente e deve ser decidido no prazo máximo de 72 horas, podendo o MP, para evitar a perda dos metadados que, entretanto, forem produzidos e que possam ser necessários para a investigação, comunicar aos operadores que requereu a sua conservação, o que impede a destruição dos dados até à decisão final sobre a conservação[77]. Também aqui é evidente a tendencial inutilidade do art. 6.º, n.ºs 2 a 4, da Lei 32/2008 face ao que já estava previsto no art. 12.º da Lei n.º 109/2009, em que o próprio OPC pode ordenar a preservação, embora com sujeição a ratificação do MP.

Quanto à necessidade de a autorização para a conservação ser concedida por três Juízes do STJ[78] não nos parece que exista qualquer justificação para a atribuição da competência a um coletivo de Juízes do STJ, uma vez que um Tribunal de Comarca pode condenar em penas de 25 anos de prisão e um único Juiz de 1.ª Instância pode determinar a prisão preventiva ou autorizar o recurso a meios de obtenção de prova muito mais restritivos de direitos fundamentais do que a conservação de metadados.

E ainda se percebe menos o porquê de ser necessário um coletivo de Juízes do STJ para autorizar a conservação (que não restringe direitos fundamentais[79]), mas depois bastar a autorização de um único Juiz de um

---

[77] Cfr. art. 6.º, n.ºs 3 e 4, da Lei n.º 32/2008.

[78] Cfr. art. 6.º, n.º 7, da Lei n.º 32/2008.

[79] Como referimos em DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, pp. 28 e ss., a conservação de metadados não restringe qualquer direito fundamental.

Na verdade, nos termos dos arts. 3.º, n.º 3, e 7.º, n.º 2, da Lei n.º 32/2008, os metadados terão de ser guardados em ficheiros (*que têm de estar obrigatoriamente separados de quaisquer outros ficheiros para outros fins*) e *encriptados* e, nos termos dos arts. 3.º, n.ºs 1 e 2, 8.º e 9.º, n.º 1, esses ficheiros só podem ser desencriptados e acedidos para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes e mediante despacho judicial fundamentado. Além disso, os ficheiros terão de observar todas as regras de segurança previstas na Lei n.º 32/2008.

Ou seja, na fase de conservação, os metadados são, apenas e só, inseridos em ficheiros encriptados, os quais ficam intocados até à sua destruição, a menos que seja autorizada a transmissão de determinados metadados para o processo, sendo que apenas poderão ser transmitidos metadados relativos ao arguido, ao suspeito, ao intermediário ou, mediante consentimento, à vítima e não todos os metadados que estejam naquele ou naqueles ficheiros encriptados.

qualquer Tribunal criminal para autorizar o acesso (em que já ocorre uma restrição de direitos fundamentais).

Apesar de o n.º 3 não o prever, resulta do n.º 5 do art. 6.º da Lei n.º 32/2008 que o prazo de conservação inicialmente fixado pode ser prorrogado.

O art. 6.º, n.º 5, da Lei n.º 32/2008 (que só se aplica aos dados de tráfego e/ou de localização que tenham sido conservados nos termos do n.º 2 desse preceito[80], não se aplicando aos que tenham sido conservados à luz da Lei n.º 41/2004) não fixa qualquer prazo de conservação[81], apenas determinando que o prazo de conservação inicialmente fixado e as suas prorrogações devem limitar-se ao estritamente necessário.

Por fim, no que concerne ao art. 9.º da Lei n.º 32/2008 (que, no caso dos dados de tráfego e de localização, inclui a obtenção dos dados cuja conservação tenha sido ordenada nos termos do art. 6.º, n.º 2, e dos dados conservados pelos operadores nos termos da Lei n.º 41/2004), sempre entendemos[82] que, apesar do disposto no art. 11.º, n.º 2, da Lei n.º 109/2009, o art. 9.º da Lei n.º 32/2008 fora revogado pelos arts. 12.º e ss. da Lei n.º 109/2009.

No entanto, tendo em conta que, com a declaração com força obrigatória geral, o art. 9.º da Lei n.º 32/2008 foi suprimido da nossa ordem jurídica, o novo art. 9.º da Lei n.º 32/2008 constitui *lex posterior* face às normas da Lei n.º 109/2009 e, por isso, quando se tratar da utilização de metadados que tenham sido alvo de conservação, aplica-se o atual art. 9.º da Lei n.º 32/2008, por força do princípio *lex posterior derogat legi priori*.

Assim, nos termos do art. 9.º, n.ºs 1 e 2, da Lei n.º 32/2008, a utilização de metadados que tenham sido objeto de conservação depende de autorização do JIC, a requerimento do MP, contanto que existam razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil e desde que se trate da investigação de algum dos crimes elencados no art. 2.º, n.º 1, al. g), da Lei n.º 32/2008, ou seja, crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou de títulos equiparados a moeda, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento

---

[80] Sem prejuízo do que referimos supra quanto à utilidade da conservação de dados de tráfego ou de localização à luz do art. 6.º, n.ºs 2 e ss., da Lei n.º 32/2008.

[81] Diversamente, no caso dos metadados conservados à luz da Lei n.º 41/2004, os prestadores de serviços de comunicações eletrónicas podem conservar esses metadados durante 6 meses (que é o período durante o qual a fatura pode ser legalmente contestada e em que o respetivo pagamento pode ser exigido) para fins de faturação dos serviços prestados (cfr. arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004, de 18 de agosto, e 9.º, n.º 2 e 10.º. n.º 1, da Lei n.º 23/96 de 26 de julho).

[82] Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 563-564, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 65 e ss., com maiores desenvolvimentos e referências bibliográficas.

contrafeitos, atos preparatórios da contrafação e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima.

Ademais, nos termos do art. 9.º, n.º 4, da Lei n.º 32/2008, a decisão judicial que autorize a utilização de metadados conservados deve respeitar os princípios da adequação, necessidade e proporcionalidade, designadamente no que se refere à definição das categorias de dados em causa e das autoridades competentes com acesso aos dados e à proteção do segredo profissional, nos termos legalmente previstos.

Deste o modo, o legislador acaba por introduzir incongruências na nossa ordem jurídica, porquanto cria dois regimes diversos para a obtenção dos mesmos tipos de dados, sendo o regime aplicável à obtenção de dados previamente conservados inexplicavelmente muito mais restritivo do que o regime aplicável à obtenção de dados em tempo real.

De acordo com o conceito de dados previsto no art. 2.º, n.º 1, al. a), da Lei n.º 32/2008, incluem-se aí os dados de tráfego, os dados de base e os dados de localização, mas não os dados de conteúdo, que, não podem ser alvo de conservação[83] e, por isso, o art. 9.º da Lei n.º 32/2008 não é aplicável à obtenção de dados de conteúdo, que atento o elevado grau de restrição de direitos fundamentais que a sua obtenção acarreta, estão submetidos ao regime particularmente restritivo dos arts. 187.º e 189.º do CPP, 6.º da Lei n.º 5/2002 e 18.º da Lei n.º 109/2009 (autorização judicial prévia, catálogo de crimes, catálogo de alvos, grau de necessidade exigente, etc.).

É inegável que a obtenção de dados de tráfego constitui uma restrição de direitos fundamentais, designadamente daqueles que são também restringidos pela intervenção nas comunicações eletrónicas (com exceção dos direitos à palavra e à liberdade de expressão)[84], mas trata-se de uma restrição muitíssimo menos intensa[85].

No entanto, apesar de a sua obtenção não acarretar uma restrição tão intensa de direitos fundamentais como no caso dos dados de conteúdo e de não se tratar de uma restrição qualificável como intensa, o legislador, no exercício da sua liberdade de conformação, submeteu a obtenção de dados de tráfego a um regime similar ao da obtenção de dados de conteúdo (cfr. arts. 189.º, n.º 2, do CPP e 18.º da Lei n.º 109/2009).

Só que, apesar de já ter consagrado um regime extremamente restritivo no que tange à obtenção de dados de tráfego em tempo real, o legislador consagrou um regime ainda mais restritivo para os casos em que os dados de tráfego tenham sido alvo de conservação, uma vez que o catálogo de crimes do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 é muito mais restritivo do que o catálogo de crimes dos arts. 187.º, n.ºs 1 e 2, do CP e 18.º, n.º 1, da Lei n.º 109/2009.

E, de facto, não vemos razão para a coexistência de dois regimes diversos, consoante a obtenção ocorra em tempo real ou incida sobre dados

---

[83] Cfr. art. 1.º, n.º 2, da Lei n.º 32/2008.

[84] Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 565 e ss.

[85] Cfr. DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, p. 68.

conservados, sendo que o facto de os dados terem sido conservados em nada aumenta a danosidade da sua utilização para fins de investigação criminal, resultando dessa diferenciação mais uma incongruência legislativa, pois, relativamente a crimes que qualifica como graves (os crimes elencados no art. 2.º, n.º 1, al. g), da Lei n.º 32/2008), o legislador consagra um regime muito mais restritivo e garantístico do que no caso de crimes menos graves (que os catálogos dos arts. 187.º, n.º 1, do CPP e 18.º da Lei n.º 109/2009 também incluem).

Mas, a situação é ainda mais grave no caso dos dados de localização e de base, em que o legislador também cria dois regimes diversos para a obtenção dos mesmos tipos de dados, sendo o regime aplicável à obtenção de dados previamente conservados muito mais restritivo do que o regime aplicável à obtenção de dados obtidos em tempo real, uma vez que tais dados, quando obtidos em tempo real, estão sujeitos ao regime do art. 14.º da Lei n.º 109/2009, que, diversamente do que sucede no caso da obtenção de dados de tráfego, não contém qualquer elenco de crimes ou de alvos, não exige autorização judicial prévia na fase de inquérito e, em termos de grau de necessidade, basta a necessidade da obtenção informações em causa para a investigação.

Ora, em primeiro lugar, também aqui não vemos em que medida o facto de os dados terem sido conservados aumenta a lesividade da sua transmissão, para fins de investigação criminal, às autoridades que justifique uma tal diferenciação, da qual resulta igualmente que, relativamente a crimes que qualifica como graves, o legislador consagra um regime muito mais restritivo e garantístico do que no caso de crimes menos graves, sendo que o "afrouxamento" garantístico de medidas que restringem direitos fundamentais só será admissível quando se trate de criminalidade grave (como sucede na Lei n.º 32/2008) e nunca de pequena ou média criminalidade (que a Lei n.º 109/2009 também inclui).

E, em segundo lugar, meios de obtenção de prova que possuem um grau de lesividade muitíssimo menor do que os meios de obtenção de prova que incidem sobre o conteúdo de comunicações acabam por estar sujeitos a um regime bastante mais restritivo do que estes.

De todo o modo, afigura-se-nos que não existe qualquer necessidade de recorrer ao art. 9.º da Lei n.º 32/2008 relativamente aos dados de base, uma vez que se trata de dados que não são verdadeiramente alvo de conservação (como os dados de tráfego ou de localização), sendo antes dados relativos ao contrato de prestação de serviços de comunicações eletrónicas, tal como sucede com os dados dos clientes de uma qualquer empresa. Daí que, tratando-se de dados informáticos, poderão sempre ser obtidos por via da injunção para apresentação ou concessão do acesso a dados prevista no art. 14.º da Lei n.º 109/2009.

No que tange ao n.º 2 do art. 9.º da Lei n.º 32/2008, tendo em conta o critério previsto nos arts. 268.º, n.º 2, e 269.º, n.º 2, do CPP, consideramos que deveria prever-se, também aqui, a possibilidade de, em casos de perigo na demora, o pedido de acesso ser apresentado ao Juiz diretamente pela autoridade de polícia criminal ou mesmo a possibilidade de a autorização ser concedida pelo MP, embora com sujeição a ulterior ratificação *expressa* do Juiz

(o que não contradiz a jurisprudência do TC e do TJUE, pois existe uma intervenção, ainda que *a posteriori*, do Juiz). Por isso, ao determinar que só o MP poderá requerer ao Juiz a transmissão de metadados que tenham sido alvo de conservação, o legislador cria mais uma incongruência na nossa ordem jurídica, sendo certo que a possibilidade prevista nos arts. 268.º, n.º 2, e 269.º, n.º 2, do CPP inclui o recurso a meios de obtenção de prova muito mais restritivos de direitos fundamentais do que a obtenção de metadados que tenham sido alvo de conservação, bem como a obtenção de dados de localização e/ou de tráfego em tempo real.

Parece-nos, pois, que o legislador poderia e deveria ter aproveitado a oportunidade oferecida pela Lei n.º 18/2024 para passar a subsumir a utilização probatória dos metadados previamente conservados ao regime da obtenção de dados da mesma natureza em tempo real vigente.

O art. 9.º da Lei n.º 32/2008 não regula a obtenção de dados sobre a localização celular para afastar perigo para a vida ou de ofensa à integridade física grave, que são obtidos nos termos do artigo 252.º-A do CPP[86].

Nos termos do art. 9.º, n.ºs 7 e 8, da Lei n.º 32/2008, o despacho que autoriza o acesso aos metadados é notificado ao titular dos dados no prazo máximo de 10 dias a contar da sua prolação, sem prejuízo de o MP, caso considere que essa notificação é passível de pôr em causa a investigação, dificultar a descoberta da verdade ou criar perigo para a vida, para a integridade física ou psíquica ou para a liberdade dos participantes processuais, das vítimas do crime ou de outras pessoas devidamente identificadas, pode solicitar ao JIC que protele a notificação, que será realizada logo que a razão do protelamento deixar de existir ou, o mais tardar, no prazo máximo de 10 dias a contar da data em que for proferido despacho de encerramento do inquérito.

Parece-nos que a Lei deveria prever também o protelamento nos casos em que a notificação possa pôr em causa as investigações no âmbito de outros processos.

De todo o modo, a inobservância do disposto no art. 9.º, n.ºs 7 e 8, da Lei n.º 32/2008 não acarreta quaisquer consequências quanto à validade e à utilizabilidade das provas obtidas.

De acordo com o art. 9.º, n.º 9, da Lei n.º 32/2008, a transmissão dos metadados a autoridades de outros Estados só pode ocorrer no âmbito da cooperação judiciária internacional em matéria penal, de acordo com as regras fixadas na respetiva Lei e desde que esses Estados garantam o mesmo nível de proteção de dados pessoais vigente no território da União Europeia.

Por último, no que tange à destruição dos metadados, nos termos do art. 11.º da Lei n.º 32/2008, o Juiz deve determinar, oficiosamente ou a requerimento de qualquer interessado, a destruição dos metadados que estejam na posse das autoridades competentes, bem como dos metadados preservados pelas entidades referidas no n.º 1 do art. 4.º dessa Lei, logo que os mesmos deixem de ser estritamente necessários para os fins a que se destinam, considerando-se que tal sucederá logo que ocorra alguma das seguintes circunstâncias:

---

[86] Cfr. art. 9.º, n.º 5, da Lei n.º 32/2008.

a) Arquivamento definitivo do processo penal;
b) Absolvição, transitada em julgado;
c) Condenação, transitada em julgado;
d) Prescrição do procedimento penal;
e) Amnistia.

Pese embora o disposto no art. 11.º da Lei n.º 32/2008, consideramos que haverá que aplicar analogicamente o disposto no art. 188.º, n.º 13, do CPP, por necessidade de salvaguardar a eventual instauração de recurso de revisão da decisão que tenha posto fim ao processo[87].

[87] Sobre as decisões que são passíveis de ser objeto de recurso de revisão, DUARTE RODRIGUES NUNES, Curso de Direito Processual Penal, 2, pp. 369-370, 433-434 e 675.

Bibliografia

Canotilho, José Joaquim Gomes/Moreira, Vital – Constituição da República Portuguesa Anotada, Volume I, 4.ª Edição, Coimbra Editora, Coimbra, 2007.

Cardoso, Rui – "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", *in* Revista do Ministério Público, n.º 172, pp. 9 e ss., Lisboa, 2022.

Dias, Jorge de Figueiredo – Direito Penal, Parte Geral, Tomo I, Questões fundamentais, A doutrina geral do crime, 3.ª Edição, Coimbra Editora, Coimbra, 2019.

Nunes, Duarte Rodrigues – O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, Gestlegal, Coimbra, 2019.
Nunes, Duarte Rodrigues – Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, Gestlegal, Coimbra, 2021.

Nunes, Duarte Rodrigues – "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* Revista do Ministério Público n.º 170, pp. 9 e ss., Sindicato dos Magistrados do Ministério Público, Lisboa, 2022.

Nunes, Duarte Rodrigues – Curso de Direito Penal, Parte Geral, Tomo I, Questões fundamentais, Teoria geral do crime, 2.ª Edição, Gestlegal, Coimbra, 2023.

Nunes, Duarte Rodrigues – Curso de Direito Processual Penal, 1, Noções gerais, Elementos do processo penal, Universidade Católica Editora, Lisboa, 2023.

Nunes, Duarte Rodrigues – Curso de Direito Processual Penal, 2, Elementos do processo penal (continuação), O procedimento criminal, Universidade Católica Editora, Lisboa, 2023.

Nunes, Duarte Rodrigues – "O Day After do Acórdão do Tribunal Constitucional n.º 268/2022", *in* Privacidade e Proteção de Dados do Município de Lisboa, pp. 171 e ss., Câmara Municipal de Lisboa, Lisboa, 2024.

Conferências e intervenções em formato digital

"Audição da Associação D3 – Defesa dos Direitos Digitais e de Duarte Rodrigues Nunes", Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República – Grupo de trabalho metadados, *in https://canal.parlamento.pt/?cid=7363&title=audicao-da-associacao-d3-defesa-dos-direitos-digitais-e-de-duarte-ro* (acedido em 04/11/2024).

Duarte Rodrigues Nunes, "A utilização probatória de metadados das telecomunicações após o Acórdão do Tribunal Constitucional n.º 268/2022", Centro de Estudos Judiciários, Formação Contínua de Magistrados, *in https://educast.fccn.pt/vod/clips/12qirigyde/streaming.html?locale=pt* (acedido em 04/11/2024).

Jurisprudência - Tribunal Europeu dos Direitos Humanos

Acórdão McCann e Outros c. Reino Unido (de 27 de setembro de 1995), *in https://hudoc.echr.coe.int/*.

Acórdão Mahmut Kaya c. Turquia (de 28 de março de 2000), *in https://hudoc.echr.coe.int/*.

Acórdão Hugh Jordan c. Reino Unido (de 4 de maio de 2001), *in https://hudoc.echr.coe.int/*.

Acórdão Paul e Audrey Edwards c. Reino Unido (de 14 de março de 2002), *in https://hudoc.echr.coe.int/*.

Acórdão Nachova e Outros c. Bulgária (de 6 de julho de 2005), *in https://hudoc.echr.coe.int/*.

Acórdão Kaya e Outros c. Turquia (de 24 de outubro de 2006), *in https://hudoc.echr.coe.int/*.

Acórdão Ramsahai e Outros c. Países Baixos (de 15 de maio de 2007), *in https://hudoc.echr.coe.int/*.

Acórdão Angelova e Iliev c. Bulgária (de 26 de julho de 2007), *in https://hudoc.echr.coe.int/*.

Acórdão K.U. c. Finlândia (de 2 de dezembro de 2008), *in https://hudoc.echr.coe.int/*.

Acórdão Opuz c. Turquia (de 9 de junho de 2009), *in https://hudoc.echr.coe.int/*.

Acórdão Kolevi c. Bulgária (de 5 de novembro de 2009), *in https://hudoc.echr.coe.int/*.

Acórdão Al-Skeini e Outros c. Reino Unido (de 7 de julho de 2011), *in https://hudoc.echr.coe.int/*.

Acórdão Vasîlka c. Moldávia (de 11 de fevereiro de 2014), *in https://hudoc.echr.coe.int/*.

Acórdão Jaloud c. Países Baixos (de 20 de novembro de 2014), *in https://hudoc.echr.coe.int/*.

Acórdão Mustafa Tunç e Fecire Tunç c. Turquia (de 14 de abril de 2015), *in https://hudoc.echr.coe.int/*.

Acórdão Armani da Silva c. Reino Unido (de 30 de março de 2016), *in https://hudoc.echr.coe.int/*.
Acórdão Khadija Ismayilova c. Azerbaijão (de 10 de janeiro de 2019), *in https://hudoc.echr.coe.int/*.
Acórdão Breyer c. Alemanha (de 30 de janeiro de 2020), *in https://hudoc.echr.coe.int/*.
Acórdão Big Brother Watch e Outros c. Reino Unido (de 25 de maio de 2021), *in https://hudoc.echr.coe.int/*.
Acórdão Centrum för rättvisa c. Suécia (de 25 de maio de 2021), *in https://hudoc.echr.coe.int/*.
Acórdão Volodina c. Rússia (n.º 2) (de 14 de setembro de 2021), *in https://hudoc.echr.coe.int/*.

Tribunal de Justiça da União Europeia

Acórdão Digital Rights Ireland Ltd e Kärntner Landesregierung e Outros (de 8 de abril de 2014, Processos C-293/12 e C-594/12), *in http://curia.europa.eu*.
Acórdão Tele2 Sverige AB e Secretary of State for the Home Department (de 21 de dezembro de 2016, Processos C-203/15 e C-698/15), *in http://curia.europa.eu*.
Acórdão Ministerio Fiscal (de 2 de outubro de 2018, Processo C-207/16), *in http://curia.europa.eu*.
Acórdão Privacy International (de 6 de outubro de 2020, Processo C-623/17), *in http://curia.europa.eu*.
Acórdão La Quadrature du Net e Outros (de 6 de outubro de 2020, Processos C-511/18, C-512/18 e C-520/18), *in http://curia.europa.eu*.
Acórdão Prokuratuur (de 2 de março de 2021, Processo C-746/18), *in http://curia.europa.eu*
Acórdão G. D. e Commissioner of An Garda Síochána (de 5 de abril de 2022, Processo C-140/20), *in http://curia.europa.eu*.
Acórdão SpaceNet e Telekom Deutschland (de 20 de setembro de 2022, Processos C-793/19 e C-794/19), *in http://curia.europa.eu*.
Acórdão A. G. e Lietuvos Respublikos generalinė prokuratūra (de 7 de setembro de 2023, Processo C-162/22), *in http://curia.europa.eu*.
Acórdão Procura della Repubblica presso il Tribunale di Bolzano (de 30 de abril de 2024, Processo C-178/22), *in http://curia.europa.eu*.

Portugal Tribunal Constitucional

Acórdão n.º 268/2022, *in www.tribunalconstitucional.pt*.
Acórdão n.º 800/2023, *in www.tribunalconstitucional.pt*.

Supremo Tribunal de Justiça

Acórdão de 21 de setembro de 2022 (Processo 79/13.5JBLSB-C.S1), *in www.dgsi.pt*.
Acórdão de 10 de novembro de 2022 (Processo 120/17.2TELSB-B.S1), *in www.dgsi.pt*.
Acórdão de 19 de janeiro de 2023 (Processo 33/15.2JAPRT-B.S1), *in www.dgsi.pt*.

Acórdão de 1 de fevereiro de 2023 (Processo 35/17.4GACHV-A.S1), *in www.dgsi.pt*.
Acórdão de 11 de maio de 2023 (Processo 21/11.8PEPRT-M.S1), *in www.dgsi.pt*.
Acórdão de 21 de junho de 2023 (Processo 1229/19.3TELSB-A.S1), *in www.dgsi.pt*.
Acórdão de 29 de junho de 2023 (Processo 42/10.8PBVCD-B.S1), *in www.dgsi.pt*.
Acórdão de 31 de janeiro de 2024 (Processo 170/11.2TAOLH-E.S1), *in www.dgsi.pt*.
Acórdão de 15 de maio de 2024 (Processo 88/20.8SMLSB-C.S1), *in www.dgsi.pt*.
Tribunal da Relação de Coimbra

Acórdão de 12 de outubro de 2022 (Processo 538/22.9JALRA.C1), *in www.dgsi.pt*.
Acórdão de 21 de junho de 2023 (Processo 302/21.2JACBR.C1), inédito.
Acórdão de 27 de setembro de 2023 (Processo 13/20.6PEVIS.C1), *in www.dgsi.pt*.

Tribunal da Relação de Évora

Acórdão de 25 de outubro de 2022 (Processo 52/18.7GBSLV.E1), *in www.dgsi.pt*.
Acórdão de 28 de fevereiro de 2023 (Processo 661/17.1TELSB.E1), *in www.dgsi.pt*.
Acórdão de 9 de maio de 2023 (Processo 275/22.4GCSTB-A.E1), *in www.dgsi.pt*.
Acórdão de 28 de junho de 2023 (Processo 2010/21.5JFLSB-A.E1), *in www.dgsi.pt*.
Acórdão de 12 de setembro de 2023 (Processo 950/10.6PCSTB.E2), *in www.dgsi.pt*.

Tribunal da Relação de Guimarães

Acórdão de 2 de maio de 2023 (Processo 12/23.6 PBGMR-A.G1), *in www.dgsi.pt*.

Tribunal da Relação de Lisboa

Acórdão de 25 de outubro de 2022 (Processo 50/22.6JBLSB-A.L1-5), *in www.dgsi.pt*.
Acórdão de 26 de janeiro de 2023 (Processo 849/20.8PBCSC.L1-9), *in www.dgsi.pt*.
Acórdão de 22 de fevereiro de 2023 (Processo 495/22.1JAFUN-A.L1-5), *in www.dgsi.pt*.

Tribunal da Relação do Porto

Acórdão de 7 de setembro de 2022 (Processo 877/22.9JAPRT-A.P1), *in www.dgsi.pt*.
Acórdão de 7 de dezembro de 2022 (Processo 5011/22.2JAPRT-A.P1), *in www.dgsi.pt*.
Acórdão de 29 de março de 2023 (Processo 47/22.6PEPRT-Z.P1), *in www.dgsi.pt*.
Acórdão de 24 de maio de 2023 (Processo 747/20.5JGLSB.P1), *in www.dgsi.pt*.

Alemanha *Bundesverfassungsgericht*
Sentença de 2 de março de 2010 (1 BvR 256/08; 1 BvR 263/08; 1 BvR 586/08), *in* https://www.bundesverfassungsgericht.de.

Decisões administrativas

Comissão Nacional de Proteção de Dados – Deliberação n.º 1008/2017, *in* www.cnpd.pt.

Desafios de Privacidade e Segurança no Setor Bancário: Uma Abordagem de Proteção de Dados

Lurdes Dias Alves [88]

Resumo

O setor bancário, um dos pilares essenciais da economia global, tem experimentado uma transformação significativa com o avanço da digitalização. O aumento da utilização de plataformas *online*, serviços bancários móveis e soluções financeiras digitais tem facilitado o acesso e a conveniência para consumidores e empresas. Contudo, essa revolução digital trouxe consigo desafios substanciais no que diz respeito à privacidade e à segurança dos dados. A crescente dependência de tecnologias digitais, a utilização de dados em larga escala e a transição para operações computadas em nuvem e inteligência artificial elevaram os riscos associados a ataques cibernéticos, fraudes e outras ameaças à segurança da informação. A proteção dos dados bancários é crucial, já que as instituições lidam com informações sensíveis, e qualquer falha pode resultar em danos financeiros, prejuízos à reputação e violação da privacidade. A confiança do consumidor, essencial para o setor, depende diretamente da segurança dos dados. Legislações como o Regulamento Geral sobre a Proteção de Dados (RGPD) e entidades reguladoras, como a Comissão Nacional de Proteção de Dados (CNPD) e o Banco de Portugal (BdP), têm um papel fundamental na criação de um ambiente seguro e na supervisão da conformidade.

Palavras-chave: Proteção de dados; setor bancário; privacidade e segurança dos dados.

[88] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Abstract

The banking sector, one of the essential pillars of the global economy, has experienced a significant transformation with the advancement of digitalization. The increased use of online platforms, mobile banking services and digital financial solutions has facilitated access and convenience for consumers and businesses. However, this digital revolution has brought with it substantial challenges when it comes to privacy and data security. The growing dependence on digital technologies, the use of large-scale data and the transition to cloud computing operations and artificial intelligence have increased the risks associated with cyber-attacks, fraud and other threats to information security. The protection of banking data is crucial, as institutions deal with sensitive information, and any failure can result in financial damage, reputational damage and privacy violations. Consumer trust, essential for the sector, directly depends on data security. Legislation such as the General Data Protection Regulation (GDPR) and regulatory entities, such as the National Data Protection Commission (CNPD) and the Bank of Portugal (BdP), play a fundamental role in creating a safe environment and supervising of compliance.

Kewwords: Data protection; banking sector; privacy and data security.

Introdução

O setor bancário tem evoluído rapidamente nas últimas décadas, impulsionado pelo desenvolvimento da tecnologia e pela crescente digitalização dos seus serviços. As inovações tecnológicas, como a implementação de soluções financeiras digitais, a utilização de plataformas *online* para transações e o aumento dos serviços móveis, transformaram profundamente o modo como as instituições financeiras operam e como os consumidores interagem com os seus serviços bancários. O aumento da utilização de tecnologias digitais trouxe inúmeros benefícios, incluindo maior conveniência, acessibilidade e eficiência para os consumidores – clientes bancários. No entanto, esta transição também apresenta desafios significativos, particularmente no que diz respeito à proteção da privacidade e à segurança dos dados financeiros. Num ambiente cada vez mais digital, os dados bancários tornam-se alvo de inúmeras ameaças, como ataques cibernéticos, roubo de identidade e fraudes financeiras, que exigem soluções robustas de segurança e conformidade regulatória.

A proteção dos dados pessoais e financeiros dos consumidores no setor bancário tornou-se uma questão fundamental, dada a natureza sensível dessas informações. O uso de plataformas digitais e a recolha massiva de dados aumentaram o risco de vulnerabilidades nas infraestruturas bancárias, tornando a privacidade e a segurança da informação tópicos centrais nas discussões sobre a digitalização financeira. O tratamento indevido de dados bancários pode resultar em consequências prejudiciais, tanto para as instituições financeiras como para os próprios consumidores, podendo afetar a confiança pública nas instituições e, por conseguinte, comprometer a estabilidade do sistema financeiro. Nesse contexto, a necessidade de estabelecer práticas eficazes de proteção de dados e de garantir a conformidade com as legislações vigentes é urgente. Em particular, o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia surge como uma das ferramentas mais importantes para regular e assegurar o tratamento ético e seguro dos dados no setor financeiro, impondo requisitos rigorosos sobre como os dados devem ser protegidos e tratados.

1. O Setor Bancário no Contexto Digital

O setor bancário tem experimentado uma transformação sem precedentes nas últimas décadas, impulsionada principalmente pela digitalização. A adoção de novas tecnologias, como plataformas *online*, serviços bancários móveis e a utilização crescente de soluções financeiras baseadas em inteligência artificial, tem alterado profundamente a forma como as instituições financeiras operam e interagem com os seus clientes. Em Portugal, tal como em muitos outros países, a

digitalização tem permitido a democratização dos serviços bancários, proporcionando maior acessibilidade e conveniência aos consumidores, além de reduzir custos operacionais para os bancos. Esta evolução, no entanto, traz consigo uma série de desafios, especialmente no que diz respeito à privacidade e segurança dos dados bancários.

A digitalização do setor bancário implica um maior volume de dados pessoais e financeiros sendo processados e armazenados de forma eletrónica, muitas vezes em ambientes de computação em nuvem. O aumento das transações *online* e o uso de sistemas de pagamento digitais têm gerado um ambiente fértil para a inovação, mas também para a exploração de vulnerabilidades. A cibersegurança tornou-se, assim, um tema central, com ataques de hackers e violações de dados a tornar-se uma ameaça constante para a estabilidade e confiança do setor bancário. A transição para uma economia cada vez mais digital exige que os bancos e outras instituições financeiras adotem soluções eficazes para proteger os dados dos clientes e garantir a conformidade com as normas de proteção de dados vigentes, como o Regulamento Geral sobre a Proteção de Dados (RGPD)[89].

1.1 Importância da Proteção de Dados no Setor Bancário

No setor bancário, a proteção dos dados é de extrema importância, uma vez que as instituições lidam com informações altamente sensíveis, como dados pessoais, históricos financeiros e transações de clientes. A segurança dos dados financeiros não se resume a proteger as informações contra perdas ou danos; trata-se de garantir a privacidade dos indivíduos, prevenindo o uso indevido ou não autorizado dos seus dados. Qualquer falha na proteção desses dados pode resultar em consequências graves, como roubo de identidade, fraude financeira e prejuízos económicos significativos para os clientes, além de danos à reputação das instituições bancárias.

Além disso, a confiança do consumidor é um dos pilares do setor bancário. Num ambiente cada vez mais digitalizado, onde as transações bancárias podem ser realizadas a qualquer momento e em qualquer lugar, os consumidores exigem um elevado nível de segurança no tratamento dos seus dados. A quebra dessa confiança pode levar à perda de clientes, além de consequências legais e financeiras para as instituições bancárias. A implementação de medidas de proteção de dados adequadas não só protege as informações dos consumidores, mas também contribui para a competitividade e a sustentabilidade das instituições financeiras a longo prazo.

A conformidade com as legislações nacionais e internacionais, como o RGPD, é fundamental para garantir que os dados dos clientes sejam tratados de

[89] REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2961&tabela=leis Regulamento Geral sobre a Proteção de Dados (RGPD).

acordo com os princípios de transparência[90], integridade e confidencialidade[91]. As instituições financeiras têm a responsabilidade de assegurar que todos os dados pessoais sejam tratados de forma ética, segura e em conformidade com as normas legais, evitando riscos de multas e sanções regulatórias.

1.2 Objetivos do Artigo

O objetivo deste artigo é analisar os principais desafios que o setor bancário enfrenta em termos de privacidade e segurança dos dados, com foco nas questões relacionadas com a proteção dos dados pessoais dos clientes. O artigo irá explorar as ameaças emergentes no contexto digital, como ataques cibernéticos, fraudes e a utilização indevida de dados bancários, e as medidas de segurança que as instituições financeiras têm implementado para mitigar esses riscos. A análise incluirá o impacto da regulamentação, com especial destaque para o RGPD, e o papel das entidades reguladoras, como a Comissão Nacional de Proteção de Dados (CNPD) e o Banco de Portugal (BdP), na supervisão e na imposição de políticas de segurança.

Através deste estudo, pretende-se compreender a importância da proteção de dados no setor bancário, analisar as melhores práticas adotadas pelos bancos e outras instituições financeiras, e destacar os desafios relacionados com a inovação tecnológica, a segurança da informação e a conformidade regulatória. O artigo também discutirá as perspetivas futuras para o setor, à medida que a tecnologia continua a evoluir e novos riscos surgem. Em última análise, este estudo visa contribuir para uma maior compreensão da complexidade envolvida na proteção dos dados bancários, oferecendo recomendações para fortalecer a segurança e melhorar a confiança no setor bancário digital.

2. A Regulação e Conformidade na Proteção de Dados Bancários

A regulação e a conformidade com as normas legais de proteção de dados no setor bancário são fundamentais para garantir a segurança e a privacidade das informações dos consumidores. No contexto atual, marcado por uma crescente digitalização dos serviços financeiros, as instituições bancárias estão sujeitas a um vasto quadro legal que regula como os dados dos clientes devem ser tratados, armazenados e protegidos[92].

---

[90] "Os dados pessoais são objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»)", (alínea a) do n.º 1, do art.º 5.º do RGPD).

[91] "Os dados pessoais são 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 («integridade e confidencialidade»)", (alínea f) do n.º 1 do art.º 5.º do RGPD).

[92] Como é o caso da *Instrução n.º 7/2021*, de 15 de abril, do Banco de Portugal (BdP). [Em linha]. Instrução que acolhe na ordem jurídica interna o Portal do Sistema de Gestão de Informação do BCE e altera a declaração para cumprimento do dever de informação relativamente ao tratamento de dados pessoais [Consultado em 9 nov. 2024]. Disponível em: https://www.bportugal.pt/sites/default/files/anexos/instrucoes/449350810_1.docx.pdf

2.1 O Regulamento Geral sobre a Proteção de Dados (RGPD)

O Regulamento Geral sobre a Proteção de Dados (RGPD), implementado pela União Europeia em 2018, é um dos pilares fundamentais da regulação da proteção de dados pessoais no espaço europeu, e tem um impacto direto sobre o setor bancário. O RGPD visa garantir a privacidade dos dados pessoais dos cidadãos da UE, estabelecendo exigências rigorosas sobre como as organizações, incluindo as instituições financeiras, devem tratar essas informações.

No setor bancário, o RGPD é particularmente relevante, visto que os bancos lidam com um volume significativo de dados pessoais e sensíveis dos clientes, incluindo dados financeiros e históricos de transações. Entre as principais obrigações impostas pelo RGPD estão a transparência no tratamento de dados[93], a segurança da informação[94], a minimização dos dados recolhidos[95], e a responsabilidade das instituições financeiras na gestão desses dados[96]. Além disso, a consentimento explícito dos clientes é necessário para o tratamento dos seus dados pessoais, salvo em algumas exceções que envolvem, por exemplo, a execução de contratos ou obrigações legais.

A conformidade com o RGPD é essencial para as instituições bancárias, não apenas para evitar pesadas multas que podem atingir até 4% do volume de negócios anual do banco, mas também para garantir a confiança dos consumidores. Num setor altamente competitivo e em que a confiança do cliente é fundamental, a conformidade com a proteção de dados é um diferencial estratégico.

2.2 Legislação e Normas Nacionais e Internacionais

Além do RGPD, as instituições bancárias devem estar atentas a um conjunto de outras legislações e normas que regem a proteção de dados, tanto a nível nacional como internacional.

Em Portugal, a Lei n.º 58/2019, de 8 de agosto[97], complementa o RGPD e regula a sua execução no direito interno. A legislação portuguesa adapta os requisitos do RGPD às especificidades do contexto nacional, estabelecendo, entre outras coisas, as competências da Comissão Nacional de Proteção de Dados (CNPD), a qual é a autoridade de controlo responsável pela fiscalização da implementação do RGPD em Portugal. A CNPD pode realizar investigações, aplicar sanções e fornecer orientações às instituições financeiras sobre como cumprir as suas obrigações.

---

[93] Princípio da licitude, lealdade e transparência (alínea a) do n.º 1, do art.º 5.º, do RGPD).
[94] Princípio da integridade e confidencialidade (alínea f) do n.º 1, do art.º 5.º, do RGPD).
[95] Princípio da minimização dos dados (alínea c) do n.º 1, do art.º 5.º, do RGPD).
[96] Princípio da responsabilidade (n.º 2, do art.º 5.º, do RGPD).
[97] Lei n.º 58/2019, de 8 de agosto. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3118A0002&nid=3118&tabela=leis&ficha=1&nversao= - LEI DA PROTEÇÃO DE DADOS PESSOAIS -

Além disso, as normas internacionais também desempenham um papel crucial na conformidade das instituições bancárias. Em países fora da União Europeia, como os Estados Unidos, *v.g.*, a *Gramm-Leach-Bliley Act (GLBA)*[98] e o *California Consumer Privacy Act (CCPA)*[99], que abordam a proteção de dados pessoais no setor financeiro, impõem exigências semelhantes de segurança e privacidade. A GLBA, por exemplo, obriga as instituições financeiras a protegerem as informações pessoais dos consumidores, garantindo a implementação de medidas de segurança adequadas, e o CCPA concede aos consumidores da Califórnia direitos semelhantes aos do RGPD, como o direito de acesso, eliminação e exclusão de dados pessoais.

No plano internacional, as normas ISO/IEC 27001[100] e a ISO/IEC 27018[101], que fornecem diretrizes para a implementação de sistemas de gestão de segurança da informação, também são frequentemente adotadas por instituições bancárias como complemento às exigências legais, especialmente no que se refere à proteção de dados no ambiente digital.

2.3 O Papel das Entidades Reguladoras

[98] *Gramm-Leach-Bliley Act (GLBA)*. [Em linha]. 12 de novembro de 1999. [Consultado em 9 nov. 2024]. Disponível em: https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act e https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

[99] *California Consumer Privacy Act (CCPA)*. [Em linha]. [Consultado em 9 nov. 2024]. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 e https://oag.ca.gov/privacy/ccpa

[100] A norma ISO 27001 é o padrão e a referência Internacional para a gestão da Segurança da informação, assim como a ISO 9001 é a referência Internacional para a certificação de gestão em Qualidade. A norma ISO 27001 tem vindo, de forma continuada, a ser melhorada ao longo dos anos e deriva de um conjunto anterior de normas, nomeadamente a ISO 27001 e a BS 7799 (British Standards). A sua origem remota na realidade a um documento publicado em 1992 por um departamento do governo Britânico que estabelecia um código de práticas relativas à gestão da Segurança da Informação. Ao longo dos anos, milhares de profissionais contribuíram com o seu *know-how* e experiência para o estabelecimento de um Standard estável e maduro, mas que certamente continuará a evoluir ao longo dos tempos. A norma tem como princípio geral a adoção pela organização de um conjunto de requisitos, processos e controlos com o objetivo de mitigarem e gerirem adequadamente o risco da organização.

[101] A ISO/IEC 27018:2014 estabelece objetivos de controle, controles e diretrizes comumente aceitos para implementar medidas para proteger Informações de Identificação Pessoal (PII) de acordo com os princípios de privacidade da ISO/IEC 29100 para o ambiente de computação em nuvem pública. Em particular, a ISO/IEC 27018:2014 especifica diretrizes baseadas na ISO/IEC 27002, levando em consideração os requisitos regulatórios para a proteção de PII que podem ser aplicáveis dentro do contexto dos ambientes de risco de segurança da informação de um provedor de serviços de nuvem pública. A ISO/IEC 27018:2014 é aplicável a todos os tipos e tamanhos de organizações, incluindo empresas públicas e privadas, entidades governamentais e organizações sem fins lucrativos, que fornecem serviços de processamento de informações como processadores de PII por meio de computação em nuvem sob contrato com outras organizações. As diretrizes na ISO/IEC 27018:2014 também podem ser relevantes para organizações que atuam como controladores de PII; no entanto, os controladores de PII podem estar sujeitos a legislação, regulamentações e obrigações adicionais de proteção de PII, não se aplicando a processadores de PII. A ISO/IEC 27018:2014 não se destina a cobrir tais obrigações adicionais.

O papel das entidades reguladoras é fundamental para garantir que as instituições bancárias cumpram as normas e exigências relativas à proteção de dados. As entidades reguladoras asseguram que as instituições financeiras implementem as melhores práticas de segurança e protejam adequadamente os dados dos clientes.

A CNPD tem a autoridade para investigar alegadas violações das normas de proteção de dados, emitir recomendações, orientar as organizações e aplicar sanções, incluindo multas substanciais. A CNPD desempenha também um papel consultivo, ajudando as instituições bancárias a entenderem e a implementarem as exigências do RGPD e da legislação nacional.

O Banco de Portugal (BdP), embora com um foco primário na supervisão da estabilidade financeira e na regulamentação prudencial, também exerce um papel importante na proteção de dados bancários. Através das suas diretrizes, o BdP assegura que as instituições financeiras implementem práticas adequadas de segurança e que os riscos associados à gestão de dados sejam mitigados. O BdP estabelece, ainda, as políticas de segurança no setor bancário, tendo em conta a crescente digitalização e o aumento das ameaças cibernéticas[102].

[102] Cfr. Brenner, Susan W. - *Cyber Threats: The Emerging Fault Lines of the Nation State*. [Em linha]. New York, 2009. [Consultado em 23 nov. 2024]. Disponível em: https://doi.org/10.1093/acprof:oso/9780195385014.001.0001: "À medida que as novas tecnologias se desenvolvem, os grupos terroristas desenvolvem novos métodos de ataque utilizando a Internet e, ao utilizarem o ciberespaço como campo de batalha, torna-se cada vez mais difícil descobrir a identidade dos atacantes e levá-los à justiça. As fronteiras aparentemente ilimitadas do ciberespaço permitiram que praticamente qualquer pessoa lançasse um ataque a partir de um local remoto e anónimo. Mas uma vez que esses ataques ocorrem, surgem várias questões importantes. Quem deve responder e como? Como devem os Estados-nação lidar eficazmente com um ataque cibernético? Serão os Estados Unidos e outros Estados-nação capazes de sobreviver num mundo onde as fronteiras virtuais são ilimitadas?" Tradução nossa de: "As new technologies develop, terrorist groups are developing new methods of attack by using the Internet, and by using cyberspace as a battlefield, it has become increasingly difficult to discover the identity of attackers and bring them to justice. The seemingly limitless boundaries of cyberspace have allowed virtually anyone to launch an attack from a remote and anonymous location. But once these attacks occur, it raises several important questions. Who should respond, and how? How should nation-states effectively deal with a cyber-attack? Will the United States and other nation-states be able to survive in a world where virtual boundaries are limitless?"

No contexto europeu, a Autoridade Europeia para a Proteção de Dados (AEPD)[103] e a *European Banking Authority* (EBA)[104] também desempenham papéis cruciais na formulação de diretrizes de proteção de dados e segurança da informação para o setor bancário, incentivando a conformidade com os regulamentos da UE e facilitando a colaboração entre as autoridades reguladoras nacionais.

3. Ameaças à Privacidade e Segurança dos Dados Bancários

A segurança e privacidade dos dados bancários têm sido constantemente ameaçadas à medida que a digitalização dos serviços financeiros avança. O setor bancário é alvo constante de diversos tipos de ciberataques, fraudes e vulnerabilidades, em grande parte devido à sua natureza crítica e à quantidade de dados sensíveis que os bancos processam. Este ponto, visa explorar as principais ameaças que colocam em risco a segurança dos dados bancários, com um foco especial nas ameaças cibernéticas, fraudes e ataques de *phishing*.

3.1 Principais Ameaças Cibernéticas

O setor bancário tem sido um alvo preferencial para cibercriminosos devido à quantidade de dados financeiros sensíveis que são processados e armazenados diariamente. As principais ameaças cibernéticas a que os bancos estão expostos incluem ataques de *malware, ransomware, phishing* e ataques de negação de serviço (DDoS). Estes ataques podem comprometer a integridade dos sistemas bancários, prejudicar a confiança do consumidor e resultar em perdas financeiras significativas.

- ***Malware*** e ***Ransomware***: O *malware* é um tipo de software malicioso que pode ser introduzido nos sistemas bancários de várias formas, como através de *emails* ou *websites* comprometidos. Uma vez instalado, o *malware* pode «roubar» dados sensíveis ou até mesmo danificar o sistema. O *ransomware*, por sua vez,

---

[103] A Autoridade Europeia para a Proteção de Dados (AEPD), é a autoridade independente de proteção de dados da União Europeia (UE). Cuja missão é: monitorar e garantir a proteção de dados pessoais e privacidade quando instituições e órgãos da UE processam informações pessoais de indivíduos; aconselhar instituições e órgãos da UE sobre todos os assuntos relacionados ao processamento de dados pessoais, mediante solicitação ou por nossa própria iniciativa. Em particular, somos consultados pela Comissão Europeia sobre propostas de legislação, acordos internacionais, bem como atos de implementação e delegados com impacto na proteção de dados e privacidade; monitorar novas tecnologias que possam afetar a proteção de informações pessoais; intervir perante o Tribunal de Justiça da UE para fornecer aconselhamento especializado sobre a interpretação da legislação sobre proteção de dados; cooperar com autoridades nacionais de supervisão e outros órgãos de supervisão para melhorar a consistência na proteção de informações pessoais. Disponível em: https://www.edps.europa.eu/about/about-us_en

[104] A *European Banking Authority (*EBA), é uma autoridade independente da UE, embora seja responsável perante o Parlamento Europeu, o Conselho e a Comissão Europeia. É um organismo do Sistema Europeu de Supervisão Financeira (ESFS), que consiste nas autoridades nacionais de supervisão e nas três autoridades europeias de supervisão dos bancos, dos mercados de valores mobiliários e das empresas de seguros (EBA,ESMA,EIOPA), o Conselho Europeu do Risco Sistémico (CERS) e o Comité Conjunto das Autoridades Europeias de Supervisão. Disponível em: https://www.eba.europa.eu/

criptografa os dados do banco e exige um pagamento para a sua liberação, causando interrupções operacionais e enormes prejuízos financeiros.

- ***Phishing*** *e* ***Spear Phishing***: *O phishing é* uma técnica comum usada para enganar os consumidores e obter informações confidenciais, como senhas e números de cartões de crédito. Os atacantes frequentemente fazem-se passar por fontes confiáveis, como bancos ou outras entidades financeiras, para solicitar esses dados. *O spear phishing é* uma variante mais direcionada, onde os atacantes personalizam as suas mensagens para uma vítima específica, tornando a fraude ainda mais difícil de identificar.
- **Ataques DDoS (*Distributed Denial of Service*)**: Os ataques DDoS visam interromper os serviços bancários *online*, sobrecarregando os servidores com tráfego excessivo até que estes falhem. Esses ataques podem resultar em tempos de inatividade do serviço e perda de acesso aos dados dos clientes, prejudicando a reputação do banco e a confiança do consumidor.
- **Exposição de Dados e Ataques a Infraestruturas de Nuvem**: Com a crescente adoção de soluções baseadas na nuvem, os bancos tornaram-se mais vulneráveis a violações de dados e ataques às suas infraestruturas de IT. Os dados bancários podem ser armazenados em servidores de terceiros, e qualquer «brecha» de segurança pode resultar na exposição de informações sensíveis dos clientes.

3.2 Fraudes, *Phishing* e Vulnerabilidades no Setor Bancário

Além das ameaças cibernéticas, o setor bancário enfrenta desafios relacionados à fraude e vulnerabilidades sistémicas, que podem resultar em perdas financeiras significativas para os clientes e para as próprias instituições financeiras. As fraudes no setor bancário incluem desde esquemas complexos de branqueamento de capitais até fraudes simples, como o uso de informações de contas bancárias «roubadas». As principais vulnerabilidades incluem falhas nos sistemas de autenticação e protocolos de segurança que podem ser exploradas por criminosos.

- **Fraudes Bancárias**: As fraudes bancárias podem ser realizadas de várias formas, como a manipulação de transações, a criação de contas falsas, ou até o desvio de fundos através de sistemas de pagamento digitais. Um exemplo clássico de fraude bancária é o uso de cartões clonados, onde os criminosos copiam as informações de um cartão de crédito ou débito para realizar compras não autorizadas.
- ***Phishing*** **e Fraudes Eletrónicas**: *O phishing* continua a ser uma das formas mais comuns de fraude no setor bancário. Este tipo de ataque envolve o envio de *emails* ou mensagens falsas que imitam comunicações legítimas de um banco, solicitando que os clientes forneçam informações confidenciais, como detalhes bancários ou senhas. *O smishing* (*phishing* via SMS) e o *vishing* (*phishing* via chamadas telefónicas) são variantes que também têm aumentado, aproveitando-se da confiança dos clientes em canais de comunicação que estes consideram seguros.
- **Vulnerabilidades em Sistemas de Autenticação**: Muitos ataques no setor bancário têm como alvo as vulnerabilidades nos processos de autenticação, como senhas fracas, autenticação de dois fatores ineficaz ou falhas no

reconhecimento biométrico. A ausência de medidas de segurança adequadas permite que atacantes acedam a contas bancárias e realizem transações fraudulentas, prejudicando tanto as instituições financeiras como os seus clientes.

- **Ameaças Internas e Engenharia Social**: Além dos ataques externos, as instituições bancárias também enfrentam ameaças internas. Funcionários ou ex-funcionários que têm acesso a dados sensíveis podem ser responsáveis por vazamentos de informações ou fraudes financeiras. A engenharia social, que envolve manipular as pessoas para que revelem informações confidenciais, também é uma ameaça significativa, visto que muitos ataques têm origem no comportamento humano e na falta de sensibilização sobre segurança.

4. Medidas de Segurança no Setor Bancário

À medida que os bancos e outras instituições financeiras adotam soluções digitais para facilitar o acesso aos seus serviços e aumentar a eficiência operacional, a segurança da informação torna-se cada vez mais crítica. No setor bancário, a proteção de dados financeiros e pessoais dos clientes não só é uma questão ética e legal, mas também uma questão de confiança e sustentabilidade do negócio. Este ponto explora as principais medidas de segurança implementadas pelas instituições bancárias, destacando a criptografia, a autenticação multifatorial e as tecnologias emergentes, bem como o uso crescente de inteligência artificial no combate a fraudes e ciberameaças.

4.1 Criptografia, Autenticação Multifatorial e Tecnologias Emergentes

As medidas de segurança no setor bancário devem ser robustas, multifacetadas e em conformidade com as regulamentações legais, como o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia[105]. Entre as medidas mais eficazes, destacam-se a criptografia de dados, a autenticação multifatorial (AMF) e a adoção de tecnologias emergentes, como a biometria e o blockchain.

Criptografia de Dados

A criptografia é uma das medidas fundamentais para garantir a segurança dos dados no setor bancário. Uma vez que transforma informações sensíveis, como números de contas bancárias, transações financeiras e dados pessoais, em códigos ilegíveis para qualquer pessoa que não possua a chave de decriptação. Impedindo que, mesmo em caso de violação de sistemas, os dados não sejam acedidos ou usados indevidamente.

---

[105] A cifragem é apontada como uma medida de controlo dos riscos de segurança no tratamento de dados pessoais, "tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a danos físicos, materiais ou imateriais", (considerando 83 do RGPD). Que se baseia, fundamentalmente, num processo de transformar uma mensagem ou dado em um formato ilegível (texto cifrado) usando um algoritmo de cifragem, com a finalidade de garantir que a mensagem seja ilegível para quem não possui a chave correta para decifrá-la. *V. g.*, Algoritmos como AES (*Advanced Encryption Standard*) ou DES (*Data Encryption Standard*). A cifragem é um dos mecanismos, ou técnica específica, usada para implementar a criptografia.

A criptografia é utilizada tanto para dados em trânsito quanto para dados em repouso. A criptografia de dados em trânsito é crucial para proteger as informações enquanto estão a transmitidas entre o banco e os clientes, seja via plataformas *online* ou dispositivos móveis. Já a criptografia de dados em repouso garante a proteção das informações armazenadas em servidores e bases de dados. A implementação de algoritmos robustos, como AES (*Advanced Encryption Standard*)[106] e RSA (*Rivest–Shamir–Adleman*)[107], é fundamental para garantir a segurança e a confidencialidade das informações.

Autenticação Multifatorial (AMF)

A autenticação multifatorial (AMF) é uma das principais defesas contra o acesso não autorizado a contas bancárias e outros sistemas financeiros. Exigindo que os usuários forneçam mais de uma forma de identificação para validar sua identidade, combinando algo que sabem (*v.g.*, uma senha), algo que possuem (*v.g.*, um cartão de segurança ou um dispositivo móvel), e algo que são (*v.g.*, a biometria).

O uso de AMF diminui significativamente a probabilidade de acesso indevido, uma vez que a simples captura de uma senha ou de um código de acesso não é suficiente para garantir o acesso ao sistema. Para os bancos, a adoção dessa medida tornou-se essencial, especialmente num ambiente digital onde as tentativas de *phishing, hacking* e outras formas de fraude são cada vez mais sofisticadas. Além disso, a AMF também facilita a conformidade com normas como o PSD2 (*Payment Services Directive* 2)[108] da União Europeia, que exige um nível mais elevado de segurança para transações *online*.

---

[106] AES (*Advanced Encryption Standard*) é um algoritmo de criptografia altamente confiável usado para proteger dados, convertendo-os num formato ilegível sem a chave adequada. Desenvolvido pelo *National Institute of Standards and Technology (NIST*), a criptografia AES usa vários comprimentos de chave (128, 192 ou 256 bits) para fornecer proteção forte contra acessos não autorizados. Esta medida de segurança de dados é eficiente e amplamente inovadora na proteção de comunicação na Internet, proteção de dados proporcionada e criptografia de arquivos. AES, é uma pedra angular da criptografia moderna, é reconhecida globalmente pela sua capacidade de manter as informações seguras contra ameaças cibernéticas.

[107] A criptografia *Rivest-Shamir-Adleman (RSA*) é uma criptografia assimétrica algoritmo. Este método utiliza um par de chaves: uma chave pública, que é compartilhada abertamente, e uma chave privada, que deve ser mantida em segredo. Os dados criptografados com a chave pública só podem ser descriptografados usando a chave privada para garantir a comunicação segura em redes abertas, como a Internet. O processo reverso, onde os dados são criptografados com a chave privada, é normalmente usado para assinaturas digitais, permitindo que qualquer pessoa com a chave pública verifique a origem e a autenticidade da mensagem. A criptografia RSA é usada no Protocolo SSL / TLS para a troca segura de chaves de criptografia simétricas e desempenha um papel crítico na segurança de transferências de arquivos pela Internet e redes privadas virtuais (VPNs). RSA é um robusto método de criptografia porque é extremamente difícil descriptografar mensagens sem a chave correspondente.

[108] A Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 (Diretiva de Serviços de Pagamento revista ou PSD2) foi publicada com o propósito de atualizar o quadro regulatório dos serviços de pagamento e promover uma maior integração europeia neste domínio. Embora mantendo a substância do quadro regulatório adotado na Diretiva 2007/64/CE do Parlamento Europeu e do Conselho de 13 de novembro de 2007, esta Diretiva introduziu alterações relevantes ao quadro regulatório que rege os serviços de pagamento. A PSD2 foi transposta para a legislação

Tecnologias Emergentes: Biometria e *Blockchain*

Além da criptografia e da autenticação multifatorial, o setor bancário tem explorado tecnologias emergentes para fortalecer a segurança e a confiança dos consumidores. A biometria é uma dessas inovações, utilizando características físicas ou comportamentais do indivíduo, como impressões digitais, reconhecimento facial ou análise da íris, para autenticar o acesso aos serviços bancários. Essas tecnologias oferecem uma solução de segurança altamente eficaz e difícil de falsificar, sendo cada vez mais adotadas por bancos em soluções de autenticação para transações móveis e *online*.

Outro exemplo de tecnologia emergente no setor bancário é o *blockchain*, uma tecnologia de registo distribuído que assegura a integridade das transações financeiras. A *blockchain* pode ser usada para criar registos transparentes e imutáveis de transações bancárias, prevenindo fraudes e melhorando a segurança em sistemas de pagamento e transferências internacionais.

4.2 O Uso de Inteligência Artificial

O uso de Inteligência Artificial (IA) no setor bancário tem-se expandido rapidamente, principalmente no que diz respeito à segurança e proteção de dados. A IA oferece uma gama de ferramentas para detetar padrões suspeitos, identificar fraudes e melhorar as defesas cibernéticas de forma dinâmica e em tempo real.

Deteção de Fraudes e Análise Comportamental

Uma das principais aplicações da IA no setor bancário é a deteção de fraudes. Através de algoritmos de aprendizado de máquina, os sistemas podem analisar grandes volumes de transações e comportamentos de clientes em busca de padrões que indiquem atividades fraudulentas. Esses sistemas podem identificar comportamentos anómalos em tempo real, como compras incomuns, tentativas de *login* a partir de localizações inesperadas ou transações que fogem do padrão habitual de um determinado cliente. Quando detetadas, essas

---

portuguesa pelo Decreto-Lei n.º 91/2018, de 12 de novembro de 2018. Este Decreto-Lei regula a prestação de serviços de pagamento em Portugal e altera significativamente a forma como os prestadores de serviços de pagamento disponibilizam os seus serviços e como os clientes (particulares, empresas e administração pública) realizam transações de pagamento. Sob esta legislação, os usuários têm a possibilidade de usar dois novos serviços de pagamento – *Payment Initiation Services* (PIS) e *Account Information Services* (AIS). Os usuários também se beneficiam de maiores condições de segurança para a execução de transações de pagamento por meio da aplicação de mecanismos fortes de autenticação de clientes. O Regulamento Delegado da Comissão (UE) 2018/389 de 27 de novembro de 2017 foi publicado no Jornal Oficial da União Europeia em 13 de março de 2018 para complementar a PSD2. Este Regulamento estabelece os padrões técnicos regulatórios para autenticação forte do cliente e padrões abertos comuns e seguros de comunicação a serem observados pelos provedores de serviços de pagamento. *Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho* de 25 de novembro de 2015. Diretiva de Serviços de Pagamento revista ou PSD2. Diretiva relativa aos serviços de pagamento no mercado interno. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015L2366

atividades podem ser imediatamente sinalizadas para investigação ou até mesmo bloqueadas automaticamente.

Além disso, a IA permite que os bancos construam modelos preditivos para identificar fraudes antes que elas aconteçam. Por exemplo, ao analisar as transações passadas, o sistema pode prever possíveis fraudes e tomar medidas preventivas, como bloquear temporariamente uma conta até que o cliente confirme a autenticidade da atividade.

Automação de Processos e Segurança de Dados

A automação dos processos bancários através da IA também tem sido uma estratégia eficaz para aumentar a segurança. Por meio de *bots* inteligentes, os bancos podem melhorar a eficácia na verificação de documentos, análise de pedidos de crédito e em processos de autenticação. O que reduz a necessidade de interação humana, diminuindo o risco de erro e a possibilidade de fraude interna.

Além disso, a IA tem um papel importante na gestão da segurança de dados, monitorando continuamente as redes para identificar vulnerabilidades e responder a incidentes de segurança de forma ágil. A IA de defesa cibernética, como sistemas de prevenção de intrusão e *firewalls* baseados em inteligência artificial, são utilizados para proteger os dados bancários contra ataques avançados e ameaças em constante evolução.

Privacidade e Conformidade Regulatória com IA

A aplicação de IA também pode ser importante para garantir a conformidade com as regulamentações de proteção de dados, como o Regulamento Geral sobre a Proteção de Dados (RGPD). A IA pode automatizar o processo de auditoria, ajudando as instituições bancárias a monitorizar e documentar os acessos e usos de dados pessoais, assegurando que estejam em conformidade com as exigências legais de privacidade e segurança.

5. O Futuro da Proteção de Dados no Setor Bancário

A evolução tecnológica no setor bancário[109], aliada ao aumento da digitalização, está a transformar rapidamente a forma como as instituições financeiras operam, oferecendo aos clientes novas formas de interagir com os seus serviços. Contudo, com as oportunidades de inovação vêm também novos desafios, principalmente no que diz respeito à privacidade e segurança dos

[109] "A chamada *Era da Comunicação*. O progresso científico tecnológico transformou este nosso Mundo numa pequena Aldeia Global, dotando o Homem não apenas da possibilidade de dar a Lua de presente aos seus filhos, mas também do poder de autodestruição enquanto espécie (pense-se nas «adormecidas» ogivas nucleares e nas armas bioquímicas), e ainda na possibilidade de criar o Frankenstein perfeito através de manipulações genéticas e de duplicar formas de vida humana (pense-se na clonagem de embriões humanos). Cfr. Pereira, Alexandre Libório Dias - *Direito da Informática* (Estudos) - Vol. III. Faculdade de Direito da Universidade de Coimbra. [Em linha]. 2020 [Consultado em 9 nov. 2024]. Disponível em: https://estudogeral.uc.pt/bitstream/10316/92036/1/Dto%20Informatica%20Estudos%20Vol.%20III.pdf p. 11.

dados bancários. Este ponto explora as inovações tecnológicas que estão a moldar o futuro da proteção de dados, os desafios emergentes que as instituições financeiras terão de enfrentar, e a importância da colaboração entre as partes envolvidas na segurança digital.

5.1 Inovações Tecnológicas e Desafios Emergentes

O setor bancário tem experimentado um avanço significativo no uso de tecnologias disruptivas para melhorar a experiência do cliente e aumentar a eficiência operacional. Algumas das inovações mais notáveis, como a inteligência artificial (IA), o *blockchain*, a computação quântica e os *smart contracts*, estão a redefinir os parâmetros da segurança bancária. Contudo, estas inovações também trazem consigo riscos de segurança e privacidade que exigem uma vigilância constante e adaptações regulatórias adequadas.

Inteligência Artificial e *Machine Learning*

A inteligência artificial (IA) e o *machine learning* são tecnologias[110] que têm um impacto crescente na segurança bancária. Estas tecnologias permitem aos bancos monitorizar e analisar grandes volumes de dados em tempo real, o que facilita a identificação precoce de padrões anómalos e atividades suspeitas. No entanto, a utilização de IA também apresenta desafios de segurança, como o risco de ataques cibernéticos mais sofisticados e a possibilidade de manipulação de algoritmos.

Além disso, o uso de IA pode levantar questões sobre privacidade, uma vez que a análise preditiva feita através de algoritmos pode permitir um acesso profundo às informações pessoais dos clientes. A forma como os dados são recolhidos, processados e utilizados pela IA necessitou de regulamentação rigorosa para garantir a conformidade com a legislação de proteção de dados, como o Regulamento Geral sobre a Proteção de Dados (RGPD).

Neste sentido, a União Europeia aprovou o Regulamento Europeu para Inteligência Artificial (*AI Act*)[111] pelo Parlamento Europeu, a 13 de junho, e publicado no Jornal Oficial da União Europeia em 12 de julho de 2024, a União Europeia estabelece um marco decisivo rumo à regulação da Inteligência Artificial (IA).

---

[110] Anote-se que a Inteligência artificial se subdivide em três principais subtipos de algoritmos IA, distinguem-se pelo nível de autonomia que apresentam, são estes: *Machine learning* (Aprendizagem da Máquina) , *Deep learning* (Aprendizagem Profunda), e *Generative AI* (Inteligência Artificial Generativa). Machine learning é um subtipo de IA, caracterizado pela capacidade de, a partir de um conjunto estruturado de dados, fazer previsões e tomar decisões com base nos dados recebidos, como uma forma altamente sofisticada de análise estatística.

[111] Regulamento Europeu para Inteligência Artificial (*AI Act*). REGULAMENTO (UE) 2024/1689 DO PARLAMENTO EUROPEU E DO CONSELHO de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) n.º 2018/858, (UE) n.º 2018/1139 e (UE) n.º 2019/2144 e as Diretivas n.º 2014/90/UE, n.º 2016/797 (UE) e n.º 2020/1828 (UE). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689

O *AI Act*[112] coloca a Europa na vanguarda global em matéria de regulamentação da Inteligência Artificial, aspirando a um duplo objetivo: garantir a segurança e a conformidade com os direitos fundamentais dos cidadãos europeus e, simultaneamente, fomentar a inovação no espaço europeu, e definição de várias regras para classificação dos sistemas de IA como de alto risco com a proibição de certas práticas, a inclusão de modelos de IA para fins gerais, uma nova arquitetura de governação e medidas de apoio à inovação e de transparência e proteção dos direitos fundamentais. O Regulamento prevê coimas por infrações que são fixadas em percentagem do volume de negócios anual global da empresa infratora no exercício financeiro anterior ou num montante predeterminado, consoante o que for mais elevado, sendo que as pequenas e médias empresas e as *startup* estão sujeitas a coimas administrativas proporcionais.

São inquestionáveis os avanços da Inteligência Artificial (IA) nos mais variadíssimos setores de atividade, porém, o impacto sobre a privacidade e proteção de dados pessoais, constitui um desafio (e preocupação). Pela capacidade de processar grandes volumes de dados em tempo real, a IA facilita a deteção de padrões e anomalias que poderiam indicar uma violação de dados e identificar e neutralizar ameaças cibernéticas com uma precisão e velocidade que seriam impossíveis de alcançar com métodos tradicionais. Contudo, a utilização de IA também levanta questões éticas e de privacidade – é fundamental encontrar um equilíbrio entre o potencial da IA e a necessidade de proteção da privacidade[113].

***Blockchain*[114] e Segurança em Transações Financeiras**

O *blockchain* tem sido amplamente discutido no contexto das *criptomoedas*, mas a sua aplicação no setor bancário vai além disso. Utilizando uma rede

---

[112] O *AI Act* entrará em vigor 20 dias após a sua publicação no jornal oficial da UE e terá várias datas de aplicação. Será plenamente aplicável 24 meses após a sua entrada em vigor, exceto no que se refere a proibições de práticas proibidas (aplicáveis seis meses após a data de entrada em vigor), aos códigos de conduta (nove meses após a entrada em vigor), regras gerais de IA, incluindo a governação (12 meses após a entrada em vigor) e obrigações para sistemas de alto risco (36 meses).

[113] O *AI Act* remete no seu art.º 10.º remete a preocupação sobre a proteção de dados pessoais para o RGPD.

[114] Blockchain é uma tecnologia de registo distribuído (*Distributed Ledger Technology - DLT*) que permite armazenar informações de forma descentralizada, segura e imutável. Trata-se de uma cadeia de blocos de dados interligados, onde cada bloco contém um conjunto de transações ou informações e está ligado ao bloco anterior através de um identificador único, chamado de *hash*. Esta ligação sequencial e criptograficamente protegida garante a integridade e a autenticidade dos dados armazenados. A principal característica do blockchain é a sua descentralização, sendo mantido por uma rede de nós (computadores) que validam e registam transações de forma consensual, eliminando a necessidade de intermediários confiáveis. Esta tecnologia é amplamente utilizada em diversos contextos, como criptomoedas (por exemplo, Bitcoin e *Ethereum*), contratos inteligentes, rastreabilidade na cadeia de suprimentos e identidade digital. Veja-se, NAKAMOTO, Satoshi - *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Em linha]. 2018 [Consultado em 9 nov. 2024]. Disponível em: https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf

descentralizada e imutável, o *blockchain* oferece uma maneira de garantir a integridade das transações financeiras, prevenindo fraudes e aumentando a transparência. No entanto, embora o *blockchain* tenha um grande potencial para melhorar a segurança das transações, também enfrenta desafios, como a escalabilidade e a necessidade de maior adoção e harmonização com as normas existentes.

Satoshi Nakamoto justifica as vantagens da utilização de *blockchain*, uma vez que o modelo bancário tradicional atinge um nível de privacidade ao limitar o acesso à informação as partes envolvidas e a um terceiro confiável. A necessidade de anunciar publicamente todas as transações impede esse método, mas a privacidade ainda pode ser mantida interrompendo o fluxo de informações noutro lugar: mantendo as chaves públicas anónimas. O público pode ver que alguém está a enviar uma quantia para outra pessoa, mas sem informações que vinculem a transação a ninguém. Isso é semelhante ao nível de informação divulgado pelas bolsas de valores, onde o tempo e a duração das negociações individuais, são divulgados, mas sem informar a identidade das partes[115].

Além disso, a implementação de *blockchain* requer uma adaptação tecnológica significativa por parte das instituições financeiras, que devem investir em novos sistemas, dar formação especializada aos seus funcionários e colaboradores e garantir que as plataformas sejam seguras contra novos tipos de ataques cibernéticos.

Computação Quântica[116] e Riscos Emergentes

A computação quântica representa uma inovação tecnológica com grande potencial disruptivo para o setor bancário. Essa tecnologia pode alterar a forma

---

[115] Tradução nossa de: "The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were." NAKAMOTO, Satoshi. *Ob. Cit.*, p. 6.

[116] A computação quântica é um paradigma computacional baseado nos princípios da mecânica quântica, que utiliza qubits (bits quânticos) como unidade fundamental de informação. Diferentemente dos bits clássicos, que assumem valores binários (0 ou 1), os qubits podem estar em estados de 0, 1 ou numa superposição de ambos, permitindo que várias operações sejam realizadas em paralelo. Além disso, a computação quântica explora fenómenos como o entrelaçamento quântico e a interferência quântica para resolver problemas com uma eficiência que supera os limites dos computadores clássicos em certas tarefas específicas. Esta abordagem é particularmente poderosa para problemas como a factorização de números grandes, a simulação de sistemas moleculares, a otimização complexa e a aprendizagem de máquina, áreas em que os algoritmos quânticos (*v.g.*, o algoritmo de *Shor* e o algoritmo de *Grover*) mostram vantagens significativas. Veja-se: NIELSEN, Michael A.; CHUANG, Isaac L. - *Quantum Computation and Quantum Information*. 10th Edition. Massachusetts Institute of Technology, 2010.

como os dados são processados e criptografados, permitindo uma capacidade de computação exponencialmente maior do que a das máquinas tradicionais. Embora a computação quântica ofereça novos recursos para a segurança dos dados, também poderá tornar obsoletas muitas das técnicas de criptografia utilizadas atualmente, criando novos desafios para a proteção de dados bancários (*v.g.*, Capacidade de quebrar sistemas clássicos, como *RSA*, com algoritmos quânticos - algoritmo de *Shor*). A transição para sistemas quânticos exigirá um esforço colaborativo internacional para estabelecer novos padrões de segurança e proteger as infraestruturas bancárias contra novas ameaças.

***Smart Contracts*[117] e a Automação no Setor Bancário**

Outra inovação tecnológica relevante no futuro da proteção de dados bancários são os *smart contracts*. Esses contratos autoexecutáveis, baseados em *blockchain*, permitem que transações financeiras sejam realizadas de forma transparente, sem a necessidade de intermediários. Podendo aumentar a segurança e reduzir o risco de fraude, pois são imutáveis e transparentes. No entanto, a implementação de *smart contracts* em larga escala exigirá que os bancos adaptem os seus sistemas operacionais para garantir que os contratos sejam cumpridos de forma segura e sem falhas.

5.2 O Papel da Colaboração no Fortalecimento da Segurança e Privacidade

Embora as inovações tecnológicas possam proporcionar novos métodos de proteção de dados, o sucesso na gestão da privacidade e segurança dos dados bancários não depende apenas da adoção de novas tecnologias. A colaboração entre diferentes partes interessadas – bancos, reguladores, empresas de tecnologia e consumidores – será essencial para enfrentar os desafios de segurança que surgem com a transformação digital.

Colaboração entre Bancos e Entidades Reguladoras

As entidades reguladoras, como o Banco de Portugal (BdP) e a Comissão Nacional de Proteção de Dados (CNPD), desempenham um papel vital no desenvolvimento de políticas de segurança e na definição de normas de proteção de dados. A colaboração entre bancos e reguladores é crucial para garantir que as regulamentações evoluam juntamente com as novas tecnologias. A criação de um ambiente regulatório flexível e dinâmico, que permita inovação sem comprometer a segurança, será essencial para que os

---

[117] *Smart contracts* são programas computacionais armazenados numa rede *blockchain* que automaticamente executam, verificam e fazem cumprir os termos de um contrato previamente estabelecido entre partes. Estes contratos utilizam lógica condicional do tipo "se-então" (*if-then*) para assegurar que as cláusulas acordadas sejam cumpridas sem a necessidade de intermediários ou autoridades centralizadas. A lógica por trás dos *smart contracts* é baseada na transparência, imutabilidade e segurança oferecidas pela tecnologia *blockchain*, sendo os contratos executados de forma descentralizada. Uma vez implantados, os *smart contracts* operam de forma autónoma, permitindo transações confiáveis em ambientes que envolvem dados digitais. Neste sentido, ANTONOPOULOS, A. M.; WOOD, G. - *Mastering Ethereum: Building Smart Contracts and DApps*. 1st Edition. O'Reily Media, 22 January 2019 e NAKAMOTO, Satoshi. *Ob. Cit*.

bancos consigam implementar soluções tecnológicas sem comprometer a privacidade dos clientes.

Parcerias com Empresas de Tecnologia

As instituições financeiras também precisam de estabelecer parcerias estratégicas com empresas de tecnologia especializadas em segurança cibernética e proteção de dados. Ao trabalhar com fornecedores que possuem expertise em segurança digital, os bancos podem implementar soluções de segurança mais robustas e avançadas, como sistemas de IA para deteção de fraudes, plataformas baseadas em *blockchain* para transações financeiras seguras e criptografia de última geração.

Envolvimento do Consumidor e Educação Digital

Os consumidores (clientes bancários) também desempenham um papel fundamental na proteção dos seus próprios dados pessoais. A educação digital e a conscientização sobre as melhores práticas de segurança são essenciais para que os clientes bancários possam proteger as suas informações pessoais, como senhas e dados bancários. Os bancos devem investir em campanhas de educação, ensinando os seus clientes a reconhecer ameaças como *phishing, malware* e outras fraudes cibernéticas. Além disso, os consumidores devem ser incentivados a utilizar medidas de segurança, como a autenticação multifatorial, para proteger as suas contas.

Colaboração Internacional e Harmonização das Normas

O setor bancário opera num contexto global, onde a proteção de dados não respeita fronteiras nacionais. Por isso, a colaboração internacional será fundamental para garantir a segurança dos dados bancários a nível global. A harmonização das regulamentações e a cooperação entre diferentes jurisdições ajudarão a estabelecer padrões de segurança comuns e a reduzir a complexidade regulatória para as instituições financeiras que operam em várias regiões[118]. A implementação de normas internacionais de segurança cibernética,

---

[118] Neste sentido veja-se: Bygrave, Lee A. - Core Principles of Data Privacy Law. In, *Data Privacy Law: An International Perspective*. [Em linha]. Oxford, 16 de abril de 2014. [Consultado em 23 nov. 2024]. Disponível em: https://doi.org/10.1093/acprof:oso/9780199675555.003.0005, Quando nos diz que: "os instrumentos internacionais têm sido fundamentais na definição de regimes nacionais e internacionais de privacidade de dados. Estes instrumentos foram elaborados no âmbito dos respetivos quadros institucionais do Conselho da Europa, da Organização para a Cooperação e Desenvolvimento Económico (OCDE), das Nações Unidas, da União Europeia, da Cooperação Económica Ásia-Pacífico (APEC), da Associação dos Países do Sudeste Asiático Nações Unidas (ASEAN) e a Comunidade Económica dos Estados da África Ocidental. O papel especial dos tratados de direitos humanos está presente em todos os instrumentos descritos". Tradução nossa de: "on international instruments that have been central in shaping national and other international data privacy regimes. These instruments have been drafted within the respective institutional frameworks of the Council of Europe, the Organisation for Economic Cooperation and Development (OECD), the United Nations, the European Union, Asia-Pacific Economic Cooperation (APEC), the Association of Southeast Asian Nations (ASEAN), and the Economic Community of West African States. The special role of human rights treaties is also described."

como a ISO 27001, pode proporcionar uma base sólida para a proteção de dados bancários num mundo cada vez mais digital e interconectado.

O *AI Act* em articulação com o RGPD na proteção da privacidade

O *AI Act* regula as aplicações de inteligência artificial, identificando os riscos associados ao seu uso e criando um sistema de classificação baseado nesses riscos. As categorias de risco variam desde baixo risco, passando por risco alto, até risco inaceitável. Algumas das áreas reguladas incluem sistemas de IA utilizados em recrutamento, finanças, justiça penal, segurança pública, saúde, entre outros. Visa:

(i) **Garantir a segurança e a confiança**: As tecnologias de IA devem ser usadas de forma transparente, segura e justa, sem prejudicar os direitos e a liberdade dos indivíduos.

(ii) **Classificação de risco**: A IA será classificada em diferentes categorias, com regulamentações mais rigorosas para aplicações de alto risco (por exemplo, em sistemas de avaliação de crédito ou em câmaras de vigilância).

(iii) **Requisitos de conformidade**: Empresas que desenvolvem ou utilizam IA devem cumprir certos requisitos técnicos e éticos, incluindo a documentação da IA, monitorização contínua dos sistemas e garantir que as decisões baseadas em IA sejam auditáveis.

O RGPD regula a proteção de dados pessoais e estabelece as bases legais para o tratamento de dados na União Europeia. Aborda direitos como o direito à privacidade, o direito ao consentimento explícito e o direito à explicabilidade nas decisões automatizadas. Visto que muitos sistemas de IA lidam com grandes quantidades de dados pessoais (como nos casos de reconhecimento facial ou sistemas de avaliação de crédito), o *AI Act* e o RGPD são complementares, ambos com o objetivo de proteger os direitos dos indivíduos em face de tecnologias disruptivas. Mas comporta intersecções e complementaridades:

a) **Decisões automatizadas e explicabilidade**: O RGPD estabelece que os indivíduos têm o direito de não ser sujeitos a decisões exclusivamente automatizadas, incluindo a definição de perfis[119], que produzem efeitos legais ou afetam significativamente. Isto é particularmente relevante para sistemas de IA, que muitas vezes tomam decisões automaticamente com base em grandes volumes de dados. O *AI Act* também aborda a necessidade de transparência e explicabilidade, exigindo que as decisões de IA sejam explicáveis para os cidadãos, o que complementa a exigência do RGPD.

b) **Consentimento**: O RGPD exige que as empresas obtenham o consentimento explícito dos indivíduos para o tratamento de seus dados pessoais, especialmente em sistemas de IA que lidam com dados sensíveis (como dados biométricos ou dados de saúde). O *AI Act*, por sua vez, exige que qualquer IA de alto risco seja desenvolvida com mecanismos de proteção para garantir que o tratamento de dados pessoais seja realizado de forma legal e justificada.

c) **Segurança dos Dados**: O RGPD impõe a obrigação de segurança ao tratamento de dados pessoais, exigindo que as empresas adotem medidas

[119] Cfr. art.º 22.º do RGPD, com as devidas limitações previstas no art.º 23.º do RGPD.

técnicas e organizativas adequadas para proteger esses dados. Da mesma forma, o *AI Act* exige que sistemas de IA sejam projetados com segurança em mente, com requisitos específicos para sistemas de IA de alto risco, que podem envolver dados pessoais.

d) **Responsabilidade e Conformidade**: O RGPD também exige que as organizações sejam responsáveis pelo tratamento de dados pessoais, sendo responsáveis por provar conformidade com as normas de proteção de dados. O *AI Act* introduz a responsabilidade sobre os fornecedores e usuários de IA, exigindo a manutenção de registos e a implementação de auditorias para garantir que os sistemas de IA não resultem em danos aos direitos dos cidadãos.

e) **Exemplos de Convergência**: Sistemas de reconhecimento facial: Se uma instituição bancária ou uma força policial usar IA para reconhecimento facial, terá de garantir que o RGPD seja cumprido (exigindo, por exemplo, consentimento explícito ou bases legais para o tratamento de dados biométricos). Além disso, o *AI Act* regulando o uso da IA nesses contextos exigirá que o sistema seja de baixo risco ou, em alguns casos, alto risco, com salvaguardas adicionais para evitar discriminação ou violação dos direitos individuais.

f) **Sistemas de crédito baseados em IA**: Bancos que utilizam IA para avaliar o crédito dos consumidores devem cumprir com as exigências de transparência do RGPD (explicando como os dados dos consumidores são usados) e garantir que o processo de decisão automatizada seja auditável. Além disso, o *AI Act* pode impor requisitos adicionais para sistemas de IA de alto risco, exigindo maior monitorização e relatórios sobre o impacto das decisões automatizadas nos consumidores.

O *AI Act* e o RGPD complementam-se para garantir que o uso de inteligência artificial na União Europeia ocorra de forma ética e segura, enquanto protege os direitos fundamentais dos cidadãos. O RGPD assegura a proteção dos dados pessoais, enquanto o *AI Act* visa garantir que as tecnologias de IA sejam seguras, transparentes e não discriminatórias. A intersecção entre ambos os regulamentos asseguram que a inovação tecnológica possa ocorrer sem comprometer a privacidade, a segurança e a dignidade das pessoas.

Conclusão

A transformação digital que o setor bancário tem experienciado nas últimas décadas trouxe benefícios substanciais, como maior acessibilidade e eficiência, mas também trouxe consigo novos e complexos desafios relacionados com a proteção de dados pessoais. A digitalização das operações bancárias, o uso de plataformas móveis e *online*, e o crescente volume de dados gerados pelas transações financeiras exigem soluções de segurança robustas e uma adaptação contínua a novas ameaças. Neste contexto, a proteção de dados não é apenas uma exigência legal, mas uma questão central para a sustentabilidade e a confiança no setor bancário. Neste ponto, final, procuramos recapitular os principais desafios e estratégias de proteção de dados discutidos

ao longo do texto e refletir sobre a importância da proteção de dados para a confiança no setor bancário.

Resumo dos Desafios e Estratégias de Proteção de Dados

Ao longo deste artigo, identificaram-se diversos desafios críticos enfrentados pelo setor bancário no que diz respeito à proteção de dados. O aumento da digitalização das operações bancárias introduziu um vasto conjunto de riscos, desde ataques cibernéticos sofisticados, como *phishing e ransomware*, até a crescente preocupação com a privacidade dos dados pessoais dos clientes. A utilização de tecnologias emergentes, como inteligência artificial e *blockchain*, oferece um grande potencial para a inovação e para melhorar a segurança das transações, mas também exige uma vigilância constante quanto à sua vulnerabilidade a novas ameaças e à necessidade de regulamentações adequadas.

Além disso, a conformidade com legislações rigorosas, como o Regulamento Geral sobre a Proteção de Dados (RGPD), tornou-se um pilar fundamental na gestão da privacidade e segurança dos dados bancários. O RGPD impõe exigências rigorosas no tratamento de dados pessoais, obrigando as instituições financeiras a implementar medidas técnicas e organizativas para garantir a segurança e a confidencialidade das informações.

Entre as estratégias de proteção de dados destacadas, a criptografia, a autenticação multifatorial e a utilização de tecnologias emergentes têm se mostrado cruciais para a mitigação de riscos. As instituições bancárias também têm adotado sistemas de inteligência artificial para detetar padrões anómalos de comportamento e *blockchain* para garantir a transparência e a segurança das transações. Essas tecnologias não só melhoram a proteção dos dados, mas também permitem maior eficiência nas operações financeiras, tornando o setor bancário mais seguro e competitivo.

Além disso, a colaboração entre bancos, reguladores, empresas de tecnologia e consumidores foi identificada como um fator determinante para o fortalecimento da segurança dos dados. A parceria entre as partes envolvidas permite a criação de um ecossistema mais seguro e resiliente, capaz de se adaptar a novas ameaças e de garantir a privacidade dos clientes.

Importância da Proteção de Dados para a Confiança no Setor Bancário

A proteção de dados é, sem dúvida, um dos pilares mais importantes para a confiança do consumidor no setor bancário. Num ambiente digital cada vez mais integrado, onde as transações bancárias são realizadas a partir de dispositivos móveis e plataformas *online*, os consumidores precisam de sentir que as suas informações pessoais e financeiras estão seguras. A violação dessa confiança pode resultar em danos irreparáveis, não apenas para os clientes, mas também para as próprias instituições bancárias, que podem enfrentar prejuízos financeiros e danos à sua reputação.

A confiança é um ativo valioso no setor bancário – é na confiança que reside o negócio bancário -, e a privacidade dos dados está intrinsecamente ligada à construção dessa confiança. Os consumidores precisam de estar seguros de que

as suas informações são tratadas de forma ética, em conformidade com as normas legais, e que as instituições financeiras tomam todas as medidas necessárias para proteger essas informações contra riscos cibernéticos e fraudes. Qualquer falha nesse sentido pode resultar na perda de clientes e na imposição de pesadas sanções legais, além de prejudicar a imagem da instituição.
Por outro lado, a implementação de boas práticas de proteção de dados pode ser um diferencial competitivo significativo. Instituições financeiras que adotam tecnologias de ponta e sigam rigorosamente as normas de proteção de dados transmitem uma imagem de responsabilidade e compromisso com a segurança e privacidade dos seus clientes. Isso não só fortalece a confiança, mas também contribui para a sustentabilidade a longo prazo das empresas no mercado, gerando um ambiente mais seguro e confiável para a realização de transações financeiras.

Bibliografia

ANTONOPOULOS, A. M.; WOOD, G. (2019). Mastering Ethereum: Building Smart Contracts and DApps. 1st Edition. O'Reily Media.

Brenner, S. W. (2009). Cyber Threats: The Emerging Fault Lines of the Nation State. [Em linha]. New York. https://doi.org/10.1093/acprof:oso/9780195385014.001.0001.

Bygrave, L. A. (2014). Core Principles of Data Privacy Law. In, Data Privacy Law: An International Perspective. [Em linha]. Oxford. https://doi.org/10.1093/acprof:oso/9780199675555.003.0005

California Consumer Privacy Act (CCPA). Última atualização em 13 de março de 2024. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 e https://oag.ca.gov/privacy/ccpa

Decreto-Lei n.º 91/2018, de 12 de novembro. Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, transpondo a Diretiva (UE) 2015/2366.

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2954&tabela=leis&so_miolo=

Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015. Diretiva de Serviços de Pagamento revista ou PSD2. Diretiva relativa aos serviços de pagamento no mercado interno. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015L2366

European Banking Authority (EBA). [Em linha]. https://www.eba.europa.eu/

Instrução n.º 7/2021, de 15 de abril, do Banco de Portugal (BdP). [Em linha]. Instrução que acolhe na ordem jurídica interna o Portal do Sistema de Gestão de Informação do BCE e altera a declaração para cumprimento do dever de informação relativamente ao tratamento de dados pessoais https://www.bportugal.pt/sites/default/files/anexos/instrucoes/449350810_1.docx.pdf

Lei n.º 58/2019, de 8 de agosto. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Lei da Proteção de Dados Pessoais. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3118A0002&nid=3118&tabela=leis&ficha=1&nversao=

NAKAMOTO, S. (2018). Bitcoin: A Peer-to-Peer Electronic Cash System. https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf

NIELSEN, M. A.; CHUANG, I. L. (2010). Quantum Computation and Quantum Information. 10th Edition. Massachusetts Institute of Technology.

PEREIRA, A. L. D. (2020). Direito da Informática (Estudos) - Vol. III. Faculdade de Direito da Universidade de Coimbra. https://estudogeral.uc.pt/bitstream/10316/92036/1/Dto%20Informatica%20Estudos%20Vol.%20III.pdf

REGULAMENTO (UE) 2024/1689 DO PARLAMENTO EUROPEU E DO CONSELHO de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) n.º 2018/858, (UE) n.º 2018/1139 e (UE) n.º 2019/2144 e as Diretivas n.º 2014/90/UE, n.º 2016/797 (UE) e n.º 2020/1828 (UE). https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito

ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2961&tabela=leis

Além do Rótulo: Ética, IA e Off-Label no Tratamento das Doenças Neurodegenerativas

Inês Filipa Leal Alverca [120]

Resumo

Neste artigo, exploramos o impacto da Inteligência Artificial (IA) e do Big Data no tratamento de doenças neurodegenerativas, com especial enfoque na utilização off- label de medicamentos. Através da análise de grandes volumes

[120] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

de dados clínicos e genéticos, a IA possibilita a identificação de tratamentos mais eficazes e a aceleração da descoberta de novas aplicações para medicamentos já existentes. No entanto, a utilização dessas tecnologias levanta desafios éticos e regulatórios, nomeadamente em relação à privacidade dos dados, à autonomia do paciente e à responsabilidade em caso de efeitos adversos. A análise comparativa entre Portugal e a Suíça revela diferenças significativas nas abordagens regulatórias, salientando a necessidade de harmonização das normas a nível europeu e internacional. Entre as sugestões regulatórias, destacam- se a implementação de princípios de transparência, auditabilidade e proteção de dados, bem como uma abordagem ética robusta para garantir a segurança e a eficácia da utilização da IA na saúde. Apesar dos desafios, as oportunidades para melhorar a eficiência dos tratamentos e reduzir custos são consideráveis, exigindo uma adaptação contínua das normas e uma colaboração estreita entre os vários intervenientes. A integração eficaz da IA no tratamento de doenças neurodegenerativas depende de uma regulamentação ética, clara e adaptável, que equilibre a inovação, a segurança e os direitos dos pacientes.

Palavras-chave: Off-Label, Inteligência Artificial, Big Data, Doenças Neurodegenerativas

Abstract

In this article, we explore the impact of Artificial Intelligence (AI) and Big Data on the treatment of neurodegenerative diseases, with a particular focus on the off-label use of medicines. By analysing large volumes of clinical and genetic data, AI makes it possible to identify more effective treatments and accelerate the discovery of new applications for existing drugs. However, the use of these technologies raises ethical and regulatory challenges, particularly in relation to data privacy, patient autonomy and liability in the event of adverse effects. The comparative analysis between Portugal and Switzerland reveals significant differences in regulatory approaches, highlighting the need to harmonise standards at European and international level. Among the regulatory suggestions are the implementation of principles of transparency, auditability and data protection, as well as a robust ethical approach to guarantee the safety and effectiveness of the use of AI in healthcare. Despite the challenges, the opportunities for improving treatment efficiency and reducing costs are considerable, requiring continuous adaptation of standards and close

collaboration between the various players. The effective integration of AI in the treatment of neurodegenerative diseases depends on clear and adaptable ethical regulations that balance innovation, safety and patients' rights.

Keywords: Off-Label, Artificial Intelligence, Big Data, Neurodegenerative Diseases.

Introdução

Na Europa, e particularmente em Portugal, as doenças neurodegenerativas representam uma preocupação crescente devido ao envelhecimento acelerado da população (Instituto Nacional de Estatística, 2020). Relatórios da União Europeia indicam que condições como Alzheimer e Parkinson's afetam milhões de pessoas (Parlamento Europeu, 2010), causando um impacto significativo nos sistemas de saúde nacionais, bem como na qualidade de vida das famílias. Em Portugal, onde o Sistema Nacional de Saúde (SNS) enfrenta largas limitações ao nível dos recursos, a necessidade de terapias acessíveis e eficazes é ainda mais urgente. Nesse contexto, o uso off-label de medicamentos surge como uma alternativa promissora, embora ainda careça de um suporte científico extensivo, e enfrente barreiras regulatórias, particularmente no que concerne ao cenário europeu heterogéneo (European Commission: Directorate-General for Health and Food Safety et al., 2019). O equilíbrio entre inovação terapêutica e segurança do paciente nunca foi, deste modo, tão essencial.

O investimento em tecnologias de Inteligência Artificial (IA) e Big Data tem vindo a crescer no panorama português (Projeto DREAMS, 2024) e europeu (Projeto SIMPATHIC, 2024), apresentando grandes potencialidades para a

descoberta de terapias off-label. As novas tecnologias oferecem uma abordagem inovadora na identificação de tratamentos para doenças neurodegenerativas, explorando dados de saúde e padrões de tratamento de maneira mais eficiente e personalizada . Prova disto é a capacidade da IA em identificar padrões e correlações em grandes volumes de dados médicos (Shaban-Nejad et al., 2018), enquanto o Big Data permite que se processem informações de forma mais eficaz e abrangente (Auffray et al., 2016). Juntas, estas tecnologias podem ajudar na descoberta de novos usos para medicamentos já existentes, acelerando o processo de identificação de terapias off-label.

No entanto, a implementação dessas tecnologias exige um sistema regulatório robusto e uma fundamentação ética clara. A ética no uso dessas tecnologias envolve questões complexas, como a privacidade de dados, a responsabilidade em caso de erros dos algoritmos e a autonomia do paciente (Char et al., 2018). Em particular, no uso off-label de medicamentos, surgem preocupações sobre o consentimento informado dos pacientes e a segurança de tratamentos não amplamente testados (Gazarian et al., 2006; Zdanys & Tampi, 2008). Além disso, a transparência dos algoritmos utilizados na tomada de decisão médica é essencial para garantir que as decisões sejam interpretáveis e confiáveis pelos profissionais de saúde (Wachter et al., 2017). A regulação da IA na saúde exige uma adaptação das normas existentes para garantir a proteção de dados e a segurança do paciente.

A União Europeia enfrenta o desafio de criar uma regulamentação harmonizada para a utilização dessas tecnologias no setor da saúde, garantindo que a inovação não comprometa a segurança dos pacientes e seus direitos (Comissão Europeia, 2021). De fato, o Regulamento Geral sobre a Proteção de Dados (RGPD) já estabelece diretrizes rigorosas sobre a utilização de dados sensíveis na área da saúde, mas a evolução da IA levanta novas questões sobre a governança dos algoritmos e a responsabilidade em casos de erro (RGPD, 2018; Rajkomar et al., 2019). Além das regulamentações, um dos principais desafios está na necessidade de validação rigorosa dos sistemas de IA antes de sua adoção clínica. Estudos destacam que algoritmos de aprendizado profundo podem apresentar viés e erros inesperados quando aplicados a populações distintas daquelas usadas no treinamento dos modelos (Ching et al., 2018; Esteva et al., 2019). Por esse motivo, especialistas defendem a criação de diretrizes internacionais que padronizem a avaliação da segurança e eficácia desses sistemas antes da sua implementação. A criação de normas claras sobre como os sistemas de IA devem ser desenvolvidos e implementados em tratamentos médicos é crucial para que a inovação beneficie os pacientes sem colocar em risco sua segurança e privacidade.

Para além disto, é de notar que ainda existe uma grande lacuna na literatura no que concerne a aplicação destas tecnologias no contexto das doenças neurodegenerativas, além de nas questões éticas e regulatórias que advém da sua implementação.

O uso off-label de medicamentos, embora frequentemente utilizado para tratar doenças neurodegenerativas, apresenta então desafios significativos.

Apesar de ser uma prática médica reconhecida, o uso de medicamentos fora das indicações para as quais foram oficialmente aprovados pode gerar incertezas quanto à sua segurança e eficácia. Em doenças como Alzheimer e Parkinson's, onde os tratamentos disponíveis são limitados, o uso off-label oferece uma possibilidade terapêutica, mas exige uma maior atenção regulatória que se deve, em grande parte, à falta de uma norma uniforme que regule a aplicação de IA e Big Data na saúde em toda a União Europeia.

Assim, e de forma resumida pois tudo será desenvolvido nas respetivas secções deste artigo, o estado da arte encontra-se desenvolvido para cada uma das facetas do problema central, mas não para o problema no seu todo, de forma integrada. Zdanys, K., & Tampi, R. R. (2008) e Rascol et al., (2021) desenvolveram trabalhos de base no que diz respeito à utilização de medicamentos off-label para o tratamento de doenças neurodegenerativa, mas sem alusão à potencial utilização das novas tecnologias. Já Gazarian et al., (2006) e Gaspar et al. (2020), desenvolveram trabalhos de base fulcrais para o entendimento das bases regulamentares, guidelines e desafios da utilização e prescrição off-label, no contexto internacional e português respetivamente. Shaban- Nejad et al., (2018) e Raghupathi, W., & Raghupathi, V. (2014) contribuem finalmente de maneira imperativa trazendo para o debate a Inteligência Artificial e o Big Data no cenário médico e da biotecnologia, mas sem abordar em concreto a sua aplicabilidade ao contexto das doenças neurodegenerativas e abordando superficialmente o tema da prescrição off-label.

Neste contexto, este estudo visa explorar a viabilidade da integração do uso off-label de medicamentos no tratamento de doenças neurodegenerativas em Portugal e na Europa, com foco nas novas tecnologias, como IA e Big Data. Esta investigação pretende analisar as implicações éticas e regulatórias desse processo, propondo possíveis avanços na prática clínica e nos sistemas de saúde, além de gerar contribuições valiosas para a academia e sugerir soluções regulatórias, tanto no contexto nacional, como no internacional.

Deste modo, há que colocar a questão central: quais são os principais desafios éticos e regulatórios na integração do uso off-label de medicamentos com a Inteligência Artificial e Big Data, no tratamento de doenças neurodegenerativas, em Portugal e na Europa? Para responder a esta questão, a metodologia adotada será Exploratória-Comparativa, com o objetivo de entender o contexto e os desafios na integração dessas tecnologias no tratamento de doenças neurodegenerativas. Para além disto, comparar-se-á as abordagens regulatórias de Portugal e Suíça. Assim, a hipótese central deste estudo será a de que a integração do uso off-label de medicamentos com novas tecnologias, em Portugal e na Europa, pode ser viabilizada por meio de uma regulamentação adaptada, investimentos em infraestrutura digital e abordagens éticas claras, superando os desafios éticos e regulatórios.

Este estudo foi desenhado e pensado com intuito de responder às questões éticas e regulatórias, que se revelam de extrema importância, especialmente quando se lida com novas tecnologias no setor da saúde. As implicações éticas envolvem, mas não se cingem, a privacidade dos dados, a

tomada de decisões autónomas por sistemas baseados em IA e o consentimento informado dos pacientes. O uso off-label de medicamentos também levanta preocupações sobre os riscos e os benefícios para os pacientes, especialmente no caso de tratamentos não amplamente testados, que são habituais no contexto das doenças neurodegenerativas. No âmbito regulatório, as leis existentes precisam ser adaptadas de modo a lidar com as novas realidades tecnológicas, garantindo que a inovação não comprometa a segurança e os direitos dos pacientes.

Este artigo será estruturado em seis secções principais, organizadas para proporcionar uma análise sistemática e integrada do tema. Após esta introdução, a secção de Metodologia detalhará os métodos exploratórios e comparativos adotados, com enfoque nas técnicas de coleta e análise de dados, utilizadas para abordar os desafios éticos e regulatórios. Em seguida, a secção de O Uso Off-Label no Contexto das Doenças Neurodegenerativas apresentará o arcabouço teórico do uso off-label, as suas aplicações específicas em condições como Alzheimer e Parkinson's, e as implicações para os sistemas de saúde nacionais. A quarta secção, Novas Tecnologias no Contexto do Uso Off-Label, explorará como a Inteligência Artificial e o Big Data podem ser utilizados para identificar novos fins e utilizações terapêuticas, destacando estudos e exemplos relevantes. Na quinta secção, Desafios e Oportunidades na Integração do Uso Off-Label com IA e Big Data, discutem-se as barreiras éticas, regulatórias e tecnológicas, bem como as possibilidades de inovação no tratamento de doenças neurodegenerativas. Em seguida, apresenta-se uma secção com Propostas e Sugestões de modo a auxiliar no desenvolvimento de melhores cenários regulamentares, tanto em Portugal como na Suíça, e ultimamente em toda a Europa Por fim, em Conclusões, o artigo irá resumir os principais pontos-chave e propor direções futuras para pesquisas e iniciativas políticas na área.

Este estudo propõe-se então a contribuir para um enquadramento jurídico que concilie inovação terapêutica com a proteção de direitos no contexto europeu das doenças neurodegenerativas.

A metodologia adotada neste estudo é Exploratória-Comparativa, com o objetivo de investigar o uso off-label de medicamentos no tratamento de doenças neurodegenerativas e como as novas tecnologias, como Inteligência Artificial (IA) e Big Data, podem ser integradas nesse processo. A abordagem exploratória foi escolhida para identificar lacunas na literatura e explorar novas questões que ainda não foram amplamente discutidas, como os desafios éticos e regulatórios associados a essas práticas. A pesquisa busca compreender os aspectos teóricos e práticos da implementação dessas tecnologias no contexto regulatório, que está em constante mudança.

Neste sentido, a pesquisa é exploratória, uma vez que permite uma análise aprofundada de um tema pouco estudado, sendo complementada por uma análise comparativa entre dois países Europeus: Portugal e Suíça. A análise comparativa visa identificar as semelhanças e as diferenças nas regulamentações e no uso das tecnologias emergentes, fornecendo assim insights sobre as melhores práticas no cenário europeu. A escolha destes países

deve-se às diferenças nos seus sistemas regulatórios e modelos de saúde, com Portugal integrando a União Europeia e a Suíça a operar com um sistema regulatório próprio, embora em estreita colaboração com a UE. Ambos enfrentam desafios semelhantes no tratamento de doenças neurodegenerativas, mas abordam o uso de IA e big data de formas distintas, refletindo as variações no acesso e na implementação dessas tecnologias. A comparação permitirá identificar melhores práticas, desafios e oportunidades para a aplicação de soluções tecnológicas inovadoras na descoberta de novos usos terapêuticos, além de fornecer insights sobre como otimizar a integração de tecnologias emergentes em sistemas de saúde com estruturas e capacidades distintas.

A recolha de dados foi realizada através de análise documental, com o foco em documentos legais, regulamentares, artigos acadêmicos e relatórios técnicos de organizações governamentais e não governamentais. Os documentos foram selecionados com base na sua relevância e proximidade com o tema, atualidade – tentamos, sempre que possível utilizar fontes com não mais de cinco a sete anos desde a sua publicação - e credibilidade, aferida com base no número de citações dos artigos por outros trabalhos de interesse na área. A análise desses materiais permitiu entender o quadro normativo sobre o uso off-label e a aplicação de IA e Big Data, além de explorar as implicações tecnológicas no tratamento de doenças neurodegenerativas.

Embora a análise documental tenha sido abrangente, o estudo possui algumas limitações. A pesquisa depende dos materiais disponíveis publicamente, o que pode excluir informações mais específicas ou recentes. Além disso, ao focar em apenas dois países, os resultados não podem ser totalmente generalizados para outros contextos da União Europeia. No entanto, essas limitações não comprometem os objetivos do estudo e abrem caminho para pesquisas futuras que possam aprofundar ainda mais o tema.

1. O Uso Off-Label no Contexto das Doenças Neurodegenerativas

Conforme destacado por Gaspar et al., (2020), a prescrição off-label de medicamentos é uma prática frequente na medicina, especialmente em situações onde as opções terapêuticas oficialmente aprovadas são limitadas ou inexistentes. Esta abordagem permite explorar novas utilizações de medicamentos já existentes, mas envolve riscos consideráveis, pois a segurança e a eficácia dos tratamentos fora das indicações aprovadas nem sempre são bem documentadas. A EMA (Agência Europeia do Medicamento) define o uso off-label como a utilização de medicamentos para uma indicação não aprovada, ou em faixas etárias, dosagens ou formas de administração não autorizadas. Segundo Gaspar et al., (2020), em Portugal, para que o uso de um medicamento se considere off-label, ele não pode ser descrito no Resumo das Características do Medicamento, um documento aprovado pelas entidades reguladoras como o Infarmed e a EMA. O uso off-label assenta na liberdade de decisão dos médicos, que devem escolher o medicamento que consideram ser mais benéfico para os seus pacientes (Carneiro & Costa, 2013; Gazarian et al., 2006).

Em termos técnicos, o uso off-label pode ocorrer em diferentes situações: em indicações clínicas não aprovadas, em populações não aprovadas ou com métodos de administração ou dosagem não aprovados, conforme a definição de off-label mencionada. Além disso, o uso pode ser baseado em efeitos de classe, em que se assume que medicamentos de uma mesma classe terão efeitos semelhantes em determinadas condições, ou em efeitos de extensão de terapias aprovadas para situações de maior severidade, presumindo-se resultados semelhantes. Também se pode usar off-label com base em efeitos de relação, quando a condição tratada partilha características com a indicação aprovada, ou ainda com base em efeitos de ampliação, quando se espera que o tratamento off-label seja igualmente eficaz para condições distintas, mas relacionadas (Fernandes, 2022; Carneiro & Costa, 2013).

O Conselho Nacional de Ética para as Ciências da Vida (CNECV, 2023) distingue três situações em que o uso off-label é permitido: (1) o uso de medicamentos off-label com suporte em evidências clínicas robustas, já estabelecidas na prática clínica, permitindo um processo de aprovação simplificado; (2) o uso pontual de medicamentos off-label em pacientes específicos, com base na avaliação caso a caso e na prova científica disponível; (3) o uso de medicamentos inovadores off-label em pacientes específicos, exigindo uma análise detalhada sobre o valor terapêutico adicional e o perfil de custo- efetividade. Não é considerado uso off-label a utilização de medicamentos que ainda não foram aprovados pelas autoridades competentes ou que se encontrem em fase de ensaio clínico, uma vez que não é possível fazer uso fora das indicações já aprovadas.

O uso off-label é particularmente relevante no tratamento de doenças neurodegenerativas, dada a escassez de opções terapêuticas amplamente eficazes. A maioria dos tratamentos disponíveis oferece apenas alívio sintomático, sem impedir a progressão da doença. Por exemplo, em doentes com Alzheimer, a memantina, inicialmente aprovada para formas moderadas a graves da doença, tem sido utilizada off-label em outras formas de demência, incluindo a doença de Parkinson, com resultados diversos (Zdanys & Tampi, 2008). Da mesma forma, a amantadina, um antivírico, tem mostrado potencial no tratamento de sintomas motores e não motores em doentes com Parkinson, apesar de não ter indicação específica para esse uso (Rascol et al., 2021).

Embora o uso de medicamentos off-label possa trazer benefícios a muitos pacientes, ele envolve riscos consideráveis. A falta de estudos clínicos rigorosos que comprovem a eficácia e segurança desses tratamentos fora das indicações aprovadas é um dos maiores desafios. A ausência de evidências robustas pode dificultar a avaliação dos benefícios e riscos por parte dos médicos, expondo os pacientes a potenciais efeitos adversos. Além disso, os tratamentos off-label nem sempre são monitorizados com o mesmo rigor que os tratamentos aprovados, o que pode deixar lacunas na segurança do paciente (Carneiro & Costa, 2013).

Um exemplo pertinente é o uso de clozapina no tratamento de distúrbios comportamentais em doentes com Parkinson. Embora a clozapina tenha demonstrado eficácia no controlo de sintomas psicóticos, o seu uso off-label

está associado a efeitos secundários graves, como agranulocitose e disfunções metabólicas, o que exige um acompanhamento médico rigoroso (Zdanys & Tampi, 2008).

Em Portugal, a utilização de medicamentos off-label no tratamento de doenças neurodegenerativas não reflete apenas uma necessidade médica, mas também as limitações do Sistema Nacional de Saúde (SNS). Com recursos limitados e uma população envelhecida, o uso de medicamentos off-label pode ser uma alternativa acessível para oferecer tratamentos eficazes, embora com custos menores em comparação com medicamentos novos. Contudo, para garantir a segurança dos pacientes, é fundamental um sistema regulatório robusto que forneça diretrizes claras sobre a prescrição e assegure o acompanhamento contínuo dos pacientes (Gaspar et al., 2020).

Além disso, o elevado custo de desenvolvimento e aprovação de novos medicamentos representa uma barreira significativa para muitos sistemas de saúde. O uso off-label pode acelerar o acesso a tratamentos promissores, reduzindo a necessidade de grandes investimentos em pesquisa e desenvolvimento. No entanto, esta abordagem deve ser acompanhada por uma supervisão clínica rigorosa, para evitar a exposição dos pacientes a riscos associados à falta de evidência ou a uma regulamentação inadequada (Rascol et al., 2021).

Portanto, a prática de prescrição off-label exige um equilíbrio delicado entre inovação terapêutica e a segurança do paciente. No contexto das doenças neurodegenerativas, onde as opções de tratamento são muitas vezes limitadas, é crucial que as regulamentações, tanto a nível europeu como nacional, evoluam para permitir o uso seguro e eficaz desses medicamentos.

2. Novas Tecnologias no Contexto do Uso Off-Label

Nos últimos anos, a Inteligência Artificial (IA) e o Big Data têm vindo a tornar-se ferramentas cruciais na área da saúde, principalmente na descoberta de novos
ratamentos e na otimização dos cuidados médicos preexistentes. Essas tecnologias oferecem uma abordagem inovadora para o uso off-label de medicamentos, permitindo explorar novos usos para fármacos existentes, com grande potencial no tratamento de doenças neurodegenerativas, como Alzheimer e Parkinson (Esteva et al., 2019; Rajkomar et al., 2019).

A Inteligência Artificial (IA) é definida pelo Parlamento Europeu (2010) como a capacidade de uma máquina para reproduzir competências semelhantes às humanas, como é o caso do raciocínio, a aprendizagem, o planeamento e a criatividade, ou seja, tratando-se de sistemas computacionais que são projetados para simular processos cognitivos biológicos, com o objetivo de resolver problemas de forma autónoma. Na saúde, a IA tem sido aplicada em diversas áreas, incluindo diagnóstico médico, análise de imagens médicas, e até na personalização de tratamentos. A IA pode processar grandes volumes de dados de forma rápida e precisa, identificando padrões que poderiam passar despercebidos pelos métodos tradicionais (Ching et al., 2018). Por

exemplo, a IA tem sido utilizada para otimizar diagnósticos precoces de doenças como o cancro e para prever a evolução de condições crônicas como a diabetes (Esteva et al., 2019).

Já no que respeita ao Big Data, este envolve a análise de grandes volumes de dados que são gerados em diferentes contextos, como registos de saúde eletrónicos, dados clínicos, imagens médicas e até informações genéticas. Quando combinados com a IA, esses dados podem ser analisados para fornecer insights valiosos sobre tratamentos e medicamentos, incluindo os usos off-label. A combinação de Big Data com IA proporciona um potencial imenso para inovar na medicina personalizada, com a análise de grandes conjuntos de dados sobre saúde de pacientes, permitindo identificar padrões e correlacionar tratamentos com resultados específicos.

Ambas as tecnologias, IA e Big Data, podem ser usadas de maneira integrada para explorar o uso off-label de medicamentos, especialmente no tratamento de doenças complexas e de difícil tratamento, como as doenças neurodegenerativas, ainda que a sua utilização neste último âmbito ainda se encontre em estados precoces, fundamentando a necessidade deste artigo científico.

As doenças neurodegenerativas, como a Doença de Alzheimer e Parkinson, são caracterizadas pela falta de tratamentos eficazes que possam interromper ou reverter a

progressão das doenças. Muitas vezes, os medicamentos existentes oferecem apenas alívio sintomático como já vimos anteriormente. O uso off-label pode, portanto, ser uma solução interessante para explorar novas formas de tratamento.

A IA pode ser utilizada para analisar grandes conjuntos de dados de ensaios clínicos, registos de saúde de pacientes e outras fontes, identificando padrões que sugiram que um medicamento, aprovado para uma condição, possa ser eficaz no tratamento de outra. Por exemplo, a IA pode descobrir relações entre a estrutura molecular de um medicamento e a forma como ele pode afetar outros sistemas biológicos, além de prever novos usos terapêuticos.

O Big Data, por sua vez, pode ser usado para compilar e analisar imensos volumes de dados de diferentes fontes. Isso pode incluir registos clínicos de pacientes que receberam tratamentos off-label, resultados de testes de laboratório, dados genómicos e até mesmo informações provenientes de ensaios clínicos prévios. A combinação de IA com Big Data permite um mapeamento mais eficiente dos medicamentos que podem ter efeitos positivos em outras condições de saúde (Interprocess, 2023).

Um exemplo relevante de como a IA pode ser utilizada na descoberta de novos usos para medicamentos é o trabalho realizado pela empresa Insilico Medicine. A empresa usou a IA para analisar grandes bancos de dados de compostos farmacológicos existentes e identificou candidatos a serem usados para tratamentos off-label. Eles conseguiram prever que o sildenafil, tradicionalmente utilizado para tratar disfunção erétil, poderia ser eficaz para o tratamento de doenças neurodegenerativas, como Alzheimer, devido ao seu efeito sobre a circulação sanguínea no cérebro (Doctrow, 2021).

Outro exemplo envolve a plataforma IBM Watson for Drug Discovery, que utiliza IA para combinar e analisar dados de pesquisa, históricos médicos e outros recursos, a fim de descobrir novos usos para medicamentos já aprovados. A plataforma pode identificar correlações entre medicamentos e condições de saúde, permitindo que pesquisadores explorem tratamentos off-label com maior precisão (Yu et al., 2018). A IA também tem sido usada em plataformas como Google DeepMind, que utilizam redes neurais para prever interações de medicamentos e identificar novas indicações terapêuticas para medicamentos existentes (Silver et al., 2016).

No entanto, todo o progresso vem com agregado aos seus desafios, e o avanço tecnológico a par e passo com a descoberta de usos off-label para tratamento de doenças neurodegenerativas não é exceção. As tecnologias de IA e Big Data oferecem grandes promessas, mas também trazem desafios técnicos e éticos que devem ser cuidadosamente considerados. Um desafio técnico é a qualidade dos dados. A eficácia da IA depende diretamente da qualidade e quantidade de dados disponíveis. Dados incompletos ou imprecisos podem comprometer os resultados das análises e gerar conclusões errôneas (Raghupathi & Raghupathi, 2014). Além disso, é necessário garantir a interoperabilidade entre os diferentes sistemas de Big Data e IA, para garantir que os dados provenientes de diferentes fontes possam ser analisados de forma eficaz.

No que diz respeito aos desafios éticos, a privacidade é uma das maiores preocupações. O uso de dados clínicos e genómicos para treinar algoritmos de IA levanta questões sobre como proteger as informações pessoais dos pacientes. As regulamentações de proteção de dados, como o Regulamento Geral sobre a Proteção de Dados (RGPD) na União Europeia, exigem que os dados pessoais dos pacientes sejam tratados com extrema cautela, com consentimento informado e medidas adequadas de segurança (Wachter et al., 2017). Outro problema ético significativo é a responsabilidade. Caso um medicamento seja prescrito com base em uma recomendação de IA e cause efeitos adversos, é preciso definir claramente quem será responsabilizado — o desenvolvedor do sistema de IA, os médicos que prescreveram o tratamento, ou ambos (Char et al., 2018).

Além disso, a validação científica dos novos usos de medicamentos identificados por IA requer estudos clínicos rigorosos. A IA pode ser eficaz para prever potenciais tratamentos, mas somente ensaios clínicos controlados podem confirmar sua eficácia e segurança (Rajkomar et al., 2019). Portanto, a integração da IA no uso off-label deve ser acompanhada de protocolos rigorosos de monitoramento e validação científica.

Deste modo, é claro que as tecnologias de IA e Big Data apresentam o potencial de transformar a forma como abordamos as doenças neurodegenerativas, permitindo a identificação de novos usos para medicamentos já existentes e, assim, expandindo as opções terapêuticas para essas condições complexas. No entanto, é essencial que a aplicação dessas tecnologias seja cuidadosamente regulada, com atenção para os desafios técnicos e éticos envolvidos. A utilização de IA no campo da saúde deve ser

aliada a uma análise crítica e a testes clínicos rigorosos, para garantir a segurança dos pacientes e a eficácia dos tratamentos.

3. Desafios e Oportunidades na Integração do Uso Off-Label com a IA e Big Data: Uma Perspetiva Comparada entre Portugal e Suíça

A utilização de Inteligência Artificial (IA) e Big Data no tratamento de doenças neurodegenerativas oferece novas perspectivas, mas também acarreta desafios significativos, como já começamos a indiciar anteriormente. A aplicação destas tecnologias no uso off-label de medicamentos abre novas possibilidades, mas também levanta questões complexas em termos éticos, regulatórios e operacionais. Para explorar este tema de forma aprofundada, é necessário compreender os desafios éticos, as questões regulatórias e as oportunidades criadas pelo uso dessas tecnologias, especificamente no contexto de doenças neurodegenerativas como o Alzheimer e o Parkinson.

3.1. Desafios Éticos: Privacidade e Autonomia do Paciente

Um dos maiores desafios éticos associados ao uso de IA e Big Data na área da saúde, se não o maior, está relacionado com a privacidade dos dados. Doentes com doenças neurodegenerativas frequentemente requerem monitorização contínua, o que implica a recolha de uma grande quantidade de dados pessoais, incluindo informações médicas, exames de imagem, e dados genéticos. Estes dados, sendo extremamente sensíveis, precisam de ser manuseados de forma a garantir que os direitos de privacidade dos pacientes sejam respeitados.

Em particular, no contexto da IA, surge a preocupação com o uso de grandes volumes de dados pessoais para desenvolver modelos preditivos sem o consentimento explícito dos pacientes, ou até mesmo sem uma total compreensão do uso que está a ser dado a esses dados. O Regulamento Geral de Proteção de Dados (RGPD) da União Europeia tem um papel crucial aqui, impondo limites claros à forma como os dados podem ser recolhidos e utilizados. No entanto, a implementação desses regulamentos pode variar de país para país, o que cria desafios na sua aplicação uniforme.

Outro ponto importante relacionado com as questões éticas é a autonomia do paciente na tomada de decisões sobre os tratamentos. A IA pode, em alguns casos, recomendar tratamentos off-label baseados em padrões identificados em grandes conjuntos de dados. Porém, a implementação dessas recomendações pode levantar a questão da autonomia informada. O paciente pode não compreender completamente as implicações da utilização de um tratamento off-label sugerido por uma máquina, o que pode limitar a sua capacidade de tomar decisões fundamentadas sobre a sua saúde (Rajkomar et al., 2019).

3.2. Desafios Regulatórios: Diferenças Legais e Lacunas na Regulação

Em termos de regulação, a principal dificuldade reside na falta de uma norma uniforme que regule a aplicação de IA e Big Data na saúde em toda a União Europeia. Embora existam regulamentações europeias que governam a aprovação de medicamentos, como a Agência Europeia de Medicamentos (EMA), a aplicação dessas normas ao uso off-label com o auxílio de IA não está totalmente definida. A Suíça, não sendo membro da União Europeia (UE), adota abordagens distintas em relação à regulamentação da inteligência artificial (IA). Atualmente, o país não possui uma legislação específica para IA, o que proporciona maior flexibilidade para a realização de testes e implementações dessa tecnologia. No entanto, essa ausência de regulamentação específica pode resultar em desafios relacionados à falta de harmonização com as normas da UE. Por exemplo, enquanto a UE está a avançar com o "AI Act", que visa estabelecer diretrizes claras para o uso seguro e ético da IA, a Suíça ainda não implementou medidas equivalentes. Isso pode levar a discrepâncias regulatórias, especialmente para empresas suíças que operam no mercado europeu.

No caso de Portugal, o uso off-label de medicamentos está bem regulado pelo Infarmed e exige a aprovação formal de entidades de saúde. No entanto, a utilização de IA para definir novos usos para medicamentos existentes fora das indicações aprovadas carece de uma legislação específica, o que coloca os profissionais de saúde e investigadores numa posição de incerteza quanto à legalidade e regulamentação desses tratamentos. Para que as tecnologias de IA sejam integradas de forma eficaz, é necessário que existam normas claras e que as autoridades de saúde se adaptem rapidamente às novas realidades tecnológicas (Wachter et al., 2017).

3.3. Oportunidades: Melhoria na Eficiência dos Tratamentos e Redução de Custos

Apesar dos desafios, as oportunidades oferecidas pela combinação de IA, Big Data e o uso off-label de medicamentos são significativas. Em primeiro lugar, a eficiência no diagnóstico e na escolha do tratamento pode ser imensamente melhorada. A IA pode analisar grandes volumes de dados clínicos, como imagens médicas, registos de saúde e respostas a tratamentos anteriores, a velocidades cada vez mais elevadas, permitindo a identificação de padrões que passariam de outro modo despercebidos aos humanos. Isso pode resultar em tratamentos mais rápidos e mais eficazes, algo crucial no tratamento de doenças neurodegenerativas como o Alzheimer e Parkinson, onde o tempo é um fator importante no sucesso do tratamento.

Além disso, a IA pode acelerar a identificação de novos usos para medicamentos existentes, permitindo que tratamentos off-label sejam explorados mais rapidamente. Em vez de realizar ensaios clínicos demorados e caros, a IA pode

identificar potenciais novas indicações para medicamentos com base em padrões de dados já existentes, acelerando assim o acesso dos pacientes a tratamentos eficazes e potencialmente mais baratos. Esta abordagem pode, além disso, reduzir custos significativos para os sistemas de saúde, uma vez que o desenvolvimento de novos medicamentos é um processo demorado e dispendioso. Ao reutilizar medicamentos já existentes, pode-se minimizar os custos com pesquisa e desenvolvimento, ao mesmo tempo que oferece alternativas terapêuticas para doenças sem tratamento eficaz (Silver et al., 2016).

Outra grande vantagem do uso de Big Data é a personalização dos tratamentos. As tecnologias atuais permitem analisar o perfil genético e clínico de cada paciente para recomendar tratamentos que são mais adequados à sua condição. Isto é particularmente relevante no contexto das doenças neurodegenerativas, onde as respostas aos tratamentos podem variar consideravelmente de paciente para paciente. A utilização de IA permite uma abordagem mais precisa e individualizada, ajudando a garantir que cada paciente receba o tratamento que tem maior probabilidade de resultar em benefícios reais.

A integração de IA e Big Data no uso off-label de medicamentos apresenta uma série de desafios, especialmente em termos de privacidade e regulação, mas também abre portas para oportunidades significativas de melhorar a eficiência dos tratamentos e reduzir os custos no tratamento de doenças neurodegenerativas. Para que essas tecnologias sejam plenamente eficazes, será necessário um esforço contínuo de harmonização regulatória em toda a União Europeia e uma adaptação das normas éticas à realidade da medicina do futuro. A colaboração internacional e uma legislação mais adaptável serão cruciais para maximizar o impacto positivo da IA e Big Data no tratamento de doenças neurodegenerativas, garantindo que os benefícios superem os riscos.

4. Propostas e Sugestões para um Melhor Enquadramento Regulamentar

Como já explorámos a fundo anteriormente, a aplicação de algoritmos de IA e Big Data para a descoberta de usos off-label de medicamentos apresenta grande potencial para o tratamento de doenças neurodegenerativas, como Alzheimer e Parkinson. Contudo, os contextos regulamentares de Portugal e Suíça revelam abordagens diferentes que impactam o desenvolvimento e a implementação destas tecnologias.

Portugal, como membro da União Europeia (UE), está alinhado às diretrizes propostas pelo AI Act, que enfatiza a transparência, rastreabilidade e auditabilidade dos algoritmos (Comissão Europeia, 2021). Isso inclui a obrigatoriedade de documentar os dados de treinamento e os métodos usados pelos algoritmos, permitindo auditorias externas. Por outro lado, a Suíça, que não é membro da UE,

adota uma abordagem mais flexível. Embora não exista uma legislação específica para IA, o governo suíço recomenda a adesão a padrões voluntários e promove a autorregulação (swissinfo.ch, 2023).

Sugere-se que Portugal e Suíça implementem um sistema que garanta a explicabilidade dos algoritmos, especialmente para aplicações médicas sensíveis, promovendo confiança mútua entre os dois países.

No que respeita à proteção de dados em Portugal, sendo esta regida pelo Regulamento Geral sobre a Proteção de Dados (RGPD), e estabelecendo normas rigorosas para a anonimização de dados de pacientes, bem como exigindo o consentimento explícito para o uso de informações sensíveis (GDPR, 2018). Na Suíça, a proteção de dados é assegurada pela Lei Federal de Proteção de Dados (FADP), que também prioriza a privacidade, mas novamente com maior flexibilidade em termos de processamento de dados para fins de pesquisa (FDPIC, 2021). Recomenda-se, neste âmbito, que ambos os países explorem formas de harmonizar as suas regulamentações de proteção de dados, permitindo a troca segura de informações para pesquisas transnacionais.

Passando agora para as questões éticas, Portugal segue de perto os princípios éticos definidos pela UE e pela OMS, enquanto a Suíça adota uma abordagem descentralizada, onde os comitês de ética regionais desempenham um papel crucial na supervisão de projetos relacionados à saúde (WHO, 2021; swissinfo.ch, 2023). No contexto de IA, essa abordagem descentralizada pode dificultar a harmonização de práticas entre regiões suíças, ao passo que Portugal se beneficia de uma supervisão mais uniforme. Para assegurar um impacto ético adequado, sugere-se que ambos os países exijam a realização de avaliações éticas antes da aplicação de IA na descoberta de usos off-label, incluindo consultas com pacientes, médicos e especialistas jurídicos.

Tanto Portugal quanto Suíça poderiam beneficiar-se de parcerias transnacionais que incentivem a harmonização de normas para o uso de IA na saúde. A Suíça já participa em iniciativas como a International Medical Informatics Association (IMIA), enquanto Portugal colabora com organismos da UE e a European Health Data Space. A criação de uma estrutura conjunta para a partilha de dados e metodologias pode acelerar descobertas off-label e facilitar a aprovação regulatória em ambos os países.

Finalmente, em Portugal, a monitorização de medicamentos é liderada pela Infarmed, enquanto na Suíça é supervisionada pela Swissmedic. Apesar de ambos os países possuírem sistemas robustos de farmacovigilância, a Suíça oferece maior flexibilidade no uso de IA para monitoramento contínuo, devido à ausência de barreiras regulatórias impostas pela UE. Essa flexibilidade pode servir de exemplo para Portugal, incentivando a adoção de sistemas mais dinâmicos e baseados em IA para vigilância pós-autorização. A adoção dessas propostas pode melhorar a descoberta de usos off-label em ambos os países, promovendo tratamentos mais eficazes e acessíveis para doenças neurodegenerativas. Contudo, desafios incluem

as diferenças nas abordagens regulamentares e a necessidade de investimentos em infraestrutura e treinamento.

Conclusão

O impacto da Inteligência Artificial (IA) e do Big Data na área da saúde tem vindo a crescer de forma significativa, oferecendo novas possibilidades de tratamento para doenças complexas e neurodegenerativas, como Alzheimer e Parkinson. Estas tecnologias têm o potencial de transformar o diagnóstico, a personalização dos tratamentos e a descoberta de novos usos para medicamentos já existentes, melhorando assim as opções terapêuticas para condições que, até há pouco tempo, apresentavam poucas alternativas eficazes. A IA pode analisar grandes volumes de dados de forma mais eficiente do que qualquer ser humano, identificando padrões e associações que permitem prever tratamentos e soluções mais rápidos e adequados a cada paciente.

A aplicação de IA e Big Data ao uso off-label de medicamentos surge como uma solução promissora, pois permite explorar novos potenciais terapêuticos para fármacos já existentes, sem a necessidade de realizar longos e dispendiosos ensaios clínicos. Este processo pode acelerar o acesso dos pacientes a tratamentos que, de outra forma, demorariam anos a chegar ao mercado. Além disso, ao utilizar medicamentos já aprovados para outras indicações, os custos de pesquisa e desenvolvimento podem ser significativamente reduzidos, tornando os tratamentos mais acessíveis para sistemas de saúde sobrecarregados.

No entanto, a implementação dessas tecnologias no sistema de saúde enfrenta vários desafios, especialmente no que diz respeito à privacidade dos dados dos pacientes. Como as doenças neurodegenerativas exigem uma monitorização contínua, são recolhidos grandes volumes de dados clínicos, genéticos e de imagem, que devem ser manuseados com extrema cautela. A regulamentação da proteção de dados, como o Regulamento Geral sobre a Proteção de Dados (RGPD), é fundamental para assegurar que os direitos dos pacientes sejam respeitados. Contudo, a forma como as leis são aplicadas pode variar de país para país, o que gera dificuldades para garantir uma implementação uniforme desses regulamentos.

Outro desafio relevante é o respeito pela autonomia do paciente. Embora a IA possa recomendar tratamentos off-label com base na análise de dados, a decisão final sobre o tratamento deve sempre envolver o paciente. Muitas vezes, os pacientes podem não compreender completamente as implicações de um tratamento sugerido por um sistema automatizado, o que levanta questões sobre a capacidade de tomar decisões informadas. Isto torna-se ainda mais claro quando o assunto é a necessidade de consentimento prévio para a utilização dos dados pessoais, não só para a sua utilização direta através do algoritmo de modo

a obter as recomendações de utilização *off-label*, mas também para o próprio treinamento de algoritmos em estágios de desenvolvimento. Além disso, deve haver uma definição clara sobre a responsabilidade em caso de efeitos adversos relacionados com tratamentos recomendados pela IA, uma vez que é preciso saber se a responsabilidade recai sobre os médicos, os desenvolvedores da IA ou ambos.

A nível regulatório, embora existam algumas normas gerais para a aprovação de medicamentos e tratamentos na União Europeia, a aplicação dessas normas no uso off- label assistido por IA ainda não está completamente definida. A situação em Portugal é um exemplo de como a regulamentação é fundamental, pois o uso off-label de medicamentos exige a aprovação das autoridades de saúde, mas o uso da IA para propor novos tratamentos carece de uma legislação mais específica. Já na Suíça, que não faz parte da União Europeia, há mais flexibilidade, o que cria oportunidades para testar novas abordagens, mas também dificulta a harmonização com os países da UE.

Apesar dos desafios, as oportunidades trazidas pela combinação de IA, Big Data e o uso off-label de medicamentos são enormes. A personalização dos tratamentos, através da análise de dados clínicos e genéticos de cada paciente, permite uma abordagem mais precisa, o que é particularmente relevante para doenças neurodegenerativas, onde os tratamentos podem ter respostas muito variáveis entre os pacientes. A utilização destas tecnologias pode acelerar o processo de adaptação dos tratamentos às necessidades específicas de cada doente, melhorando assim a eficácia e aumentando as probabilidades de sucesso terapêutico.

Portanto, o futuro da medicina e o tratamento de doenças neurodegenerativas dependem da integração eficaz dessas tecnologias, mas também de uma regulamentação adequada e de uma abordagem ética robusta. Para isso, propõe-se que as regulamentações incluam princípios de transparência e auditabilidade, alinhados às diretrizes europeias e internacionais, bem como a proteção rigorosa de dados e avaliações éticas para minimizar riscos. Além disso, a colaboração entre governos, organizações de saúde e empresas de tecnologia será fundamental para garantir que os benefícios da IA e do Big Data possam ser aproveitados de forma segura, eficaz e acessível. O desenvolvimento de normas mais claras, tanto a nível europeu como global, será essencial para garantir que a aplicação da IA no uso off-label de medicamentos se realize de forma ética e segura, promovendo a inovação no tratamento das doenças neurodegenerativas e beneficiando todos os pacientes.

Referências

Auffray, C., Balling, R., Barroso, I., Bencze, L., Benson, M., Bergeron, J., Bernal-Delgado, E., Blomberg, N., Bock, C., Conesa, A., Del Signore, S., Delogne, C., Devilee, P., Di Meglio, A., Eijkemans, M., Flicek, P., Graf, N., Grimm, V., Guchelaar, H. J., ... Zanetti, G. (2016). Making sense of big data in health research: Towards an EU action plan. Genome Medicine, 8(1), 71. https://doi.org/10.1186/s13073-016-0323-y

Carneiro V. A. & Costa J. (2013) A prescrição fora das indicações aprovadas (off-label): prática e problemas. *Rev Port Cardiol. 32*: 681---686 https://www.revportcardiol.org/pt- pdf-S2174204913001803

Char, D. S., Shah, N. H., & Magnus, D. (2018). Implementing machine learning in health care—addressing ethical challenges. *The New England Journal of Medicine, 378*(11), 981-983. https://doi.org/10.1056/NEJMp1714229

Ching, T., Himmelstein, D. S., Beaulieu-Jones, B. K., Kalinin, A. A., Do, B. T., Dunn, J., & Greene, C. S. (2018). Opportunities and obstacles for deep learning in biology and medicine. *Journal of The Royal Society Interface, 15*(141), 20170387. https://doi.org/10.1098/rsif.2017.0387

CNECV. (2023) Parecer n.º 123/CNECV/2023 sobre o uso off-label de medicamentos - Implicações Éticas. https://www.cnecv.pt/pt/deliberacoes/pareceres/parecer-n-123- cnecv-2023-sobre-o-uso-off-label-de-medicamentos-i

Doctrow B. (2021, Dezembro 14) *Viagra associated with reduced risk of Alzheimer's disease*. National Institutes of Health https://www.nih.gov/news-events/nih-research-matters/viagra-associated-reduced-risk-alzheimers-disease

EMA (s.d.) Off-Label use. https://www.ema.europa.eu/en/glossary-terms/label-use

European Commission: Directorate-General for Health and Food Safety, Marjolein, W., Lisman, J., Hoebert, J., Moltó Puigmarti, C., Dijk, L., Langedijk, J., Marchange, S., Damen, N., & Vervloet, M. (2019). Study on off-label use of medicinal products in the European Union: report, *Publications Office*. https://data.europa.eu/doi/10.2875/464022

European Commission. (2021). *Proposal for a regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu/

Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2019). Dermatologist-level classification of skin cancer with deep neural networks. *Nature, 542*(7639), 115-118. https://doi.org/10.1038/nature21056

FDPIC. (2021). *Federal Act on Data Protection (FADP)*. https://www.edoeb.admin.ch/ Fernandes, A. F. (2022) USO OFF-LABEL. *Centro de investigação de Direito Privado https://www.cidp.pt/revistas/rjlb/2023/3/2023_03_1523_1547.pdf*

Gaspar, A., Morgado, S., & Morgado, M. (2020) Estudo retrospetivo do uso off-label de medicamentos num hospital universitário português. *Centro de informação do medicamento* https://www.researchgate.net/publication/344633578_Medicamentos_frequentement_e_sujeitos_a_prescricao_off-label

Gazarian, M., Kelly, M., McPhee, J. R., Graudins, L. V., Ward, R. L., & Campbell, T. J. (2006). Off-label use of medicines: consensus recommendations for evaluating appropriateness. *The Medical journal of Australia*, *185*(10), 544–548. https://doi.org/10.5694/j.1326-5377.2006.tb00689.x

GDPR. (2018). *General Data Protection Regulation*. https://gdpr-info.eu/

Interprocess (2023, Dezembro 15). *Big Data e o uso de dados analíticos na saúde*

https://interprocess.com.br/big-data-dados-na-saude/

Instituto Nacional de Estatística. (2020). *Projeções da população residente em Portugal 2018-2080*.

https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=426127543&att_display=n&att_download=y

Parlamento Europeu. (2010). Relatório - A7-0366/2010. https://www.europarl.europa.eu

Projeto DREAMS. (n.d.). DREAMS Horizon: Big data and AI in rare neuromuscular diseases. https://dreamshorizon.eu

Projeto SIMPATHIC. (n.d.). SIMPATHIC: Accelerating drug repurposing for rare neurological disorders. https://simpathic.eu

Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: Promise and potential. *Health Information Science and Systems,* *2*(1), 3. https://doi.org/10.1186/2047-2501-2-3

Rajkomar, A., Dean, J., & Kohane, I. (2019). Machine learning in medicine. *New England Journal of Medicine,* *380*(14), 1347-1358. https://doi.org/10.1056/NEJMra1814259

Rascol, O., Goetz, C., Koller, W., Poewe, W., & Sampaio, C. (2021). Amantadine in the treatment of Parkinson's disease and other movement disorders. *Lancet Neurology,* *20*(12),1048-056. https://www.sciencedirect.com/science/article/am/pii/S1474442221002490

Shaban-Nejad, A., Michalowski, M., & Buckeridge, D. L. (2018). Health intelligence: How artificial intelligence transforms population and personalized health. NPJ Digital Medicine, 1(1), 53. https://doi.org/10.1038/s41746-018-0058-9

Silver, D., Hubert, T., & Schrittwieser, J. (2016). Mastering the game of Go with deep neural networks and tree search. *Nature,* *529*(7587), 484-489.

https://doi.org/10.1038/nature16961

Swissinfo (2023). *Qual a posição da Suíça no que respeita à regulamentação da inteligência artificial?* https://www.swissinfo.ch/por/ciencia/qual-a-posi%C3%A7%C3%A3o-da-su%C3%AD%C3%A7a-no-que-respeita-%C3%A0-regulamenta%C3%A7%C3%A3o-da-intelig%C3%AAncia-artificial/48596508

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law, 7*(2), 76-99. https://doi.org/10.1093/idpl/ipx009

WHO. (2021). *Ethics and governance of artificial intelligence for health. Organização Mundial da Saúde*. https://www.who.int/publications/

Yu, K. H., Beam, A. L., & Kohane, I. S. (2018). Artificial intelligence in healthcare. Nature Biomedical Engineering, 2(10), 719-731. https://doi.org/10.1038/s41551-018-0305-z

Zdanys, K., & Tampi, R. R. (2008). A systematic review of off-label uses of memantine for psychiatric disorders. *Progress in neuro-psychopharmacology & biological psychiatry*, *32*(6), 1362–1374. https://doi.org/10.1016/j.pnpbp.2008.01.008

Consentimento informado e consentimento para o tratamento de dados pessoais na área da saúde: sinônimos ou institutos diferentes?

Thamara Consul Gavazza [121]

Resumo

Não há como pensar no avanço científico no setor de saúde sem o processamento de dados pessoais e, como não é admitido o tratamento desenfreado dessas informações, o consentimento emerge como uma tábua de salvação para essa questão. Contudo, há grande confusão entre os consentimentos, de forma que o presente artigo tem como objetivo apenas trazer diferenças entre o consentimento informado e consentimento enquanto base legal legitimadora (prevista na legislação brasileira de proteção de dados pessoais e no regulamento europeu) e analisar, brevemente, alternativas que legitimem esse processamento, explorando suas limitações e desafios associados, por meio do emprego da metodologia doutrinal-dogmática comparativa. Os resultados indicam que, além dos institutos não serem sinônimos, o consentimento, embora importante, não é a única opção viável que autoriza o tratamento de dados pessoais no âmbito da saúde. Conclui-se que a adoção de alternativas traz maior equilíbrio entre o tratamento adequado de dados pessoais e o fomento do avanço científico-tecnológico.

Palavras-chave: Dados pessoais sensíveis, dados de saúde, consentimento informado, base legal, Lei Geral de Proteção de Dados.

[121] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Abstract
It is impossible to envision scientific advancement in the healthcare sector without the processing of personal data, which cannot be handled unrestrainedly. In this context, consent emerges as a lifeline for this issue. Thus, the aim of this article is not only to highlight the differences between informed consent and consent as a legitimizing legal basis (as provided in the Brazilian data protection legislation and the European regulation), but also to propose alternatives that legitimize this processing, exploring its limitations and associated challenges. The study employs a comparative doctrinal-dogmatic methodology. The results indicate that consent, although important, is not the only viable option for authorizing the processing of personal data in healthcare and scientific research. The conclusion is that the adoption of alternatives provides a better balance between the proper processing of personal data and the promotion of scientific and technological progress.

Keywords: Sensitive personal data, health data, informed consent, legal basis, General Data Protection Law.

Introdução

O avanço tecnológico tem transformado o setor de saúde, promovendo inovações nos tratamentos, nos diagnósticos e na realização de pesquisas. Nesse cenário, o uso de dados pessoais, como os dados de saúde, torna-se essencial. No entanto, a proteção de dados dessa natureza apresenta desafios únicos, em razão de seu caráter sensível e do potencial impacto em direitos fundamentais, como a privacidade.

Com o advento da Lei Geral de Proteção de Dados Pessoais brasileira (Lei 13.709/2018 – LGPD), vigente desde 18 de setembro de 2020 e inspirada no Regulamento Geral sobre a Proteção de Dados europeu (EU – 2016/679 – RGPD), a questão acerca da legitimidade no tratamento de dados pessoais tem sido cada vez mais discutida. Neste contexto, a utilização do consentimento surge como uma tábua de salvação para legitimar o tratamento de dados pessoais, se mostrando como uma opção viável, plausível e muito bem aceita, já que legitima o tratamento de dados pessoais "comuns" e sensíveis, tanto na LGPD (respectivamente, art. 7º, inciso I e art. 11, inciso I), quanto no RGPD (art. 6º e art. 9º). Contudo, considerando a área da saúde, há grande confusão entre os conceitos envolvendo o consentimento, pois, de um lado, há o consentimento informado (consentimento livre, por vezes coletado antes de um procedimento médico) e de outro o consentimento enquanto base legal. Embora haja estudos sobre o tema na área médica e jurídica, a literatura carece de análise aprofundada que conecte e diferencie ambos os conceitos os quais, por vezes, aparecem como sendo sinônimos. Para tanto, é necessário questionar quais as diferenças entre consentimento informado e consentimento enquanto base legal, e quais alternativas podem complementar sua aplicação no tratamento de dados sensíveis? Desta forma, o presente artigo científico surge com objetivo central de distinguir esses dois institutos, os quais, apesar de contarem com algumas semelhanças (como a nomenclatura e certos requisitos, como serem coletados de forma livre, específica e informada), possuem diferenças latentes, em especial quanto ao seu âmbito de aplicação, natureza e finalidade. Assim, eles não podem ser considerados como sinônimos, uma vez que, dentro de uma atividade de tratamento, podem coexistir (quando se coleta o consentimento informado do paciente e a base legal aplicável é o consentimento) ou não, considerando as alternativas que legitimem o tratamento de dados pessoais, de acordo com as hipóteses brevemente[122] levantadas, como o emprego de outras bases legais e exemplos de sua aplicação na área da saúde, a aplicação de anonimização e o uso de dado sintético.

Espera-se que o presente artigo possa trazer um novo panorama frente à temática aqui levantada, por relacionar a área da saúde com o universo jurídico, assessorando os operadores do Direito a não confundirem conceitos e se libertarem de alguns mitos e crenças defendidas por muitos, como a ilusória projeção de que

[122] Em razão da complexidade, estes institutos serão abordados de forma breve, uma vez que o objetivo central do artigo é o levantamento das diferenças e semelhanças entre o consentimento informado e consentimento enquanto base legal.

apenas o consentimento legitima o tratamento de dados pessoais. Isto porque os resultados indicam que o consentimento, apesar de ser muito importante, não é a única opção viável que autoriza o tratamento de dados pessoais, em especial na área da saúde, pois a dependência exclusiva do consentimento limita o potencial científico e dificulta o avanço tecnológico em áreas como a saúde DONEDA (2019).

Para a construção deste artigo, optou-se pela utilização da metodologia doutrinal-dogmática, considerada apropriada para a interpretação e sistematização das normas jurídicas. Este método permitiu uma análise aprofundada com base em fontes como leis e doutrina. A coleta de dados foi centrada em uma revisão bibliográfica abrangente, envolvendo legislação, artigos científicos e livros, que serviu como o alicerce para o desenvolvimento do trabalho. Durante o processo de pesquisa, constatou-se que alguns autores não diferenciam adequadamente os dois tipos de consentimento, utilizando o termo de forma genérica, como DALLARI (2020), que não apresenta os contornos necessários para distinguir esses institutos, enquanto outros, como SOARES (2021) e LIMA e PIEROTE (2022), destacam brilhantemente as diferenças entre eles. Adicionalmente, foi utilizada a metodologia comparativa, que possibilitou a análise do tema sob a ótica da legislação brasileira e europeia. O artigo está estruturado em três seções principais: na primeira, discute-se conceitualmente dados pessoais e dados pessoais sensíveis, sendo que essa classificação impacta diretamente na escolha a hipótese legal autorizadora para o tratamento (base legal). Na segunda seção, aprofunda-se a análise das semelhanças e diferenças entre o consentimento enquanto base legal e o consentimento informado. Por fim, na terceira seção demonstram-se os problemas relacionados ao consentimento enquanto base legal, ensejando a necessidade de alternativas para legitimar o tratamento de dados pessoais, tudo como forma de viabilizar o tratamento de dados de forma ética e legal, considerando suas vantagens e desvantagens.

1. Tratamento de dados pessoais na área da saúde

Em que pese a privacidade e a proteção de dados pessoais sejam direitos fundamentais consagrados na Constituição da República Federativa do Brasil (CRFB) nos incisos X e LXXIX do art. 5º, seus conceitos possuem características distintas e complementares. A privacidade foi inicialmente definida no artigo "*The Right to Privacy*" (WARREN, BRANDEIS, 1890) como o "direito de ser deixado em paz", sendo frequentemente associada ao princípio da exclusividade, com atributos como solidão (donde o desejo de estar só), segredo (donde a exigência de sigilo) e autonomia (donde a liberdade de decidir sobre si mesmo com o centro emanador de informações), conforme os ensinamentos de FERRAZ JÚNIOR (1993). Ela também é considerada uma liberdade negativa, que visa proteger o indivíduo contra interferências externas, assegurando sua autonomia e sigilo. Já a proteção de dados

pessoais está diretamente ligada à sociedade da informação e caracteriza-se como uma liberdade positiva, pois concede aos titulares maior controle sobre suas informações pessoais (autodeterminação informativa).

A evolução tecnológica e o crescente uso de dados pessoais impulsionaram a criação de normas que visavam regular a privacidade e a proteção de dados, como a Declaração Universal dos Direitos Humanos[123] (DUDH) de 1948, a Convenção Europeia de Direitos Humanos[124] (CEDH) de 1950, a Convenção para a Proteção de Indivíduos no que diz respeito ao Processamento Automático de Dados Pessoais (Convenção 108) de 1980, a Carta dos Direitos Fundamentais da União Europeia[125] (CDFUE) de 2000, até se chegar ao Regulamento Geral sobre a Proteção de Dados (UE - 2016/679 - RGPD), que revogou a Diretiva de Proteção de Dados 95/46/CE de 24 de outubro de 1995. O mesmo ocorreu no âmbito brasileiro, como se destaca pelo Código Civil[126] (CC - Lei nº. 10.406/2002), a Lei de Acesso à Informação (LAI – Lei nº. 12.527/2011), a Lei nº. 12.737/2011 (popularmente conhecida como Lei Carolina Dieckmann), o Marco Civil da Internet (MCI – Lei nº. 12.965/2014), até ser aprovada a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/2018), a qual não veio para revogar ou se se sobrepor a outros ramos do direito ou demais normas, mas sim para sedimentar e positivar regras sobre o tratamento de dados pessoais, tanto em ambiente físico, quanto digital. Por isso, é comum observar estudos sobre sua incidência em diversos segmentos da economia, pois a LGPD é aplicável para pessoa física e jurídica (de direito público ou privado), desde que realize o tratamento de dados pessoais[127], conceito compreendido, de forma geral, como tudo aquilo relacionado ao manuseio de dados pessoais, desde o momento de sua coleta até sua exclusão, ou seja, durante todo o seu ciclo de vida.

Neste contexto, o tratamento de dados pessoais na área da saúde ganha especial importância, isto porque, antes mesmo do advento da LGPD, já havia relevante preocupação com o manuseio de informações neste setor, devido à sua relação direta com direitos fundamentais (vida e a saúde) e o uso ético desses dados, razão pela qual algumas legislações e normativas setoriais traziam contornos

---

[123] Em especial o art. 12, que dispõe: "Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".

[124] Em especial o art. 8º, que dispõe: "1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência".

[125] Em especial o art. 7º: "Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações", e art. 8º: "1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito".

[126] Em especial o art. 21, o qual traz o direito à proteção à privacidade como um direito da personalidade: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

[127] De acordo com art. 5º, inciso X, da LGPD, é: "Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

acerca da proteção dessas informações, como o Código de Ética Médica[128] (Resolução CFM nº. 2.217 de 27 de setembro de 2018), a Lei nº 13.787/2018 (que regula o arquivamento e uso de prontuários médicos), além de normativos da Agência Nacional de Saúde Suplementar (ANS) e da Comissão Nacional de Ética em Pesquisa (CONEP), bem como o próprio Código de Defesa do Consumidor (CDC - Lei 8.078/1990). Com o advento da LGPD, consolidou-se a necessidade de cuidados rigorosos no tratamento de dados pessoais e para que esse tratamento seja considerado legítimo, é imprescindível a observância dos princípios previstos na referida lei e a existência de uma base legal que o justifique.

1.1 Princípios norteadores do tratamento de dados pessoais

A LGPD é considerada como uma legislação principiológica, eis que sua coluna vertebral está sedimentada em princípios que auxiliam na sua interpretação e aplicação, servindo como um norte a ser observado pelos agentes de tratamento[129], conforme esculpido nos incisos do art. 6º do referido texto legal. Para facilitar a compreensão, a tabela a seguir apresenta a definição de cada princípio e exemplos práticos de sua aplicação no contexto da área da saúde.

Tabela 1 –Princípios da LGPD e respectivos exemplos práticos do tratamento de dados na área da saúde

Princípios	Conceito legal (definição LGPD)	Exemplo
I - Finalidade	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.	Uma clínica médica não pode utilizar os dados de saúde coletados durante uma consulta médica para finalidade diversa que não seja compatível com o atendimento médico (ex. envio de *newsletter* pela clínica), sem o prévio conhecimento e autorização/ cadastramento do titular.
II - Adequação	Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.	Um hospital informa ao paciente que coletará seus dados para agendar seu exame. Esses dados

[128] Em especial o capítulo IX, que aborda especificamente acerca do sigilo médico.

[129] De acordo com art. 5º, incisos VI, VII e IX, da LGPD, entende-se por agentes de tratamento o controlador (pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais) e o operador (pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador).

		não podem ser compartilhados com terceiros, como empresas de seguro, sem uma relação direta com a finalidade inicial.
III - Necessidade	Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.	Ao agendar uma consulta médica, inicialmente, são coletados dados cadastrais e de contato. Outras informações não relacionadas com o agendamento médico podem ser excessivas (ex. signo).
IV - Livre Acesso	Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.	Um laboratório de diagnóstico deve disponibilizar canal gratuito e de fácil acesso para que as pessoas possam exercer seus direitos enquanto titulares (ex. paciente solicitar acesso aos seus dados).
V - Qualidade dos Dados	Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.	Um hospital mantém os registros médicos dos pacientes atualizados, corrigindo imediatamente informações desatualizadas ou incorretas, seja de ofício ou mediante requisição do titular.
VI - Transparência	Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.	Uma clínica de fisioterapia disponibiliza em todos os pontos de coleta de dados seu Aviso de Privacidade voltado ao público externo, como em seu site ou fisicamente, em sua recepção.
VII - Segurança	Utilização de medidas técnicas e administrativas aptas a	Um hospital adota criptografia em seu sistema

	proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.	de prontuários eletrônicos e implementa autenticação em dois fatores para acesso pelos médicos.
VIII - Prevenção	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.	Um laboratório realiza teste de penetração (*PenTest*) para avaliar as vulnerabilidades de segurança de seus sistemas, como forma de prevenir eventuais violações de dados.
IX - Não Discriminação	Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.	Um médico não pode recusar-se a prestar seus serviços ou impor condições menos favoráveis a uma pessoa em razão de sua etnia.
X - Responsabilização e Prestação De Contas	Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.	Uma clínica médica mantém o registros das atividades de tratamento de dados (ROT) atualizado, bem como mantém suas políticas e procedimentos em repositório centralizado, estando apta a apresentar e demonstrar a conformidade com a LGPD.

Fonte: autora

Por sua vez, de maneira semelhante à legislação brasileira, o RGPD também estabelece princípios relativos ao tratamento de dados pessoais em seu art. 5º, os quais guardam grande semelhança com os previstos na LGPD, como: licitude, lealdade e transparência; limitação das finalidades; minimização dos dados; exatidão; limitação do armazenamento; integridade e confidencialidade; e responsabilidade com prestação de contas.

1.2 Bases legais para o tratamento de dados pessoais

Antes de abordar as hipóteses legais para o tratamento de dados pessoais (bases legais), é fundamental distinguir dados pessoais e dados pessoais sensíveis (ou de categoria especial), conforme previsto tanto na legislação brasileira quanto na europeia. Essa diferenciação ocorre pois os dados pessoais sensíveis dizem respeito a informações mais íntimas do titular, sendo potencialmente discriminatórios e podendo gerar riscos significativos para os direitos e liberdades fundamentais, conforme disposto no Considerando 51 do RGPD.

Assim, entende-se por dado pessoal "toda informação relacionada a pessoa natural identificada ou identificável" (LGPD, art. 5º, inciso I), sendo, portanto, um conceito amplo e abrangente. Por sua vez, o conceito de dado pessoal sensível é mais restrito, de forma que ambas as legislações trazem um rol taxativo das categorias de dados que são considerados sensíveis, sendo apenas os dados sobre: i) origem racial ou étnica; ii) convicção religiosa ou filosófica; iii) opinião política; iv) filiação a sindicato; v) dado referente à saúde ou à vida sexual ou orientação sexual; vi) dado genético; vii) dado biométrico, quando vinculado a uma pessoa natura.

Para fins deste estudo, dar-se-á maior enfoque no denominado "dado relativo à saúde" ou "dado de saúde", que de acordo com o art. 4º, nº.15, do RGPD, é definido como aquele "relacionado com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revele informações sobre o seu estado de saúde". Por sua vez, SARLET, CALDEIRA (2019) complementam o conceito de dados de saúde, ao indicar que cabem todas as informações relativas à saúde de uma pessoa, especificamente os dados registrados nos processos clínicos, os resultados de análises e de outros exames subsidiários, das intervenções e dos diagnósticos, que são manejadas pelos profissionais de saúde na sua relação assistencial. Em adição, o Considerando 35 do RGPD também contribuiu para a referida conceituação[130].

Além disso, quando um dado pessoal comum será tratado como um dado pessoal sensível quando puder, por si só, revelar um dado pessoal sensível e causar dano ao titular (art. 11, §1º da LGPD), por exemplo, a avaliação do gênero da pessoa que o titular declara ser o seu cônjuge, a qual pode indicar a orientação sexual dos envolvidos[131].

---

[130] Considerando 35 - Deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. O que precede inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, conforme referido na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho (9), a essa pessoa singular; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro.

[131] SOARES, Flaviana Rampazzo. Consentimento no direito da saúde nos contextos de

Com o objetivo de reforçar a proteção a esses dados, o legislador brasileiro não apenas os diferenciou conceitualmente, mas também refletiu essa distinção nas hipóteses autorizadoras para seu tratamento, pois algumas bases legais aplicáveis ao tratamento de dados pessoais não se estendem aos dados pessoais sensíveis, enquanto outras são exclusivas para seu processamento, como se ilustra pela tabela abaixo.

Tabela 2 –Bases legais da LGPD e sua aplicação ao tratamento de dados pessoais sensíveis

Base legal LGPD	Dado pessoal	Dado pessoal sensível	Exemplo prático considerando a área da saúde
Consentimento (art. 7º, inciso I e art. 11, inciso I).	Aplicável	Aplicável	Um paciente autoriza explicitamente o envio de mensagens promocionais de tratamentos estéticos por uma clínica que acessará os procedimentos anteriormente realizados.
Cumprimento de obrigação legal (art. 7º, II e art. 11, I, "a")	Aplicável	Aplicável	Preenchimento de formulários exigidos por normas da Anvisa.
Execução de políticas públicas (art. 7º, III e art. 11, I, "b").	Aplicável	Aplicável	Programas de vacinação do SUS utilizam dados de cidadãos para mapear cobertura vacinal em uma região.
Realização de estudos por órgão de pesquisa (art. 7º, IV e art. 11, I, "c").	Aplicável	Aplicável	Realização de projeto de pesquisa com dados coletados de hospitais ou de investigações científicas, sempre que possível, com anonimização de dados. Essa base surge em especial

atendimento médico e de LGPD: diferenças, semelhanças e consequências no âmbito dos defeitos e da responsabilidade. Revista IBERC, Belo Horizonte, v. 4, n. 2, p. 18-46, maio/ago. 2021. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/170. Data de acesso 26/01/2025.

			para os casos de investigações científicas[132].
Execução de contrato (art. 7º, V).	Aplicável	Não aplicável	No âmbito do contrato assinado com o plano de saúde, é realizado reembolso de despesa médica, considerando que neste tratamento não haverá o tratamento de nenhum dado pessoal sensível, como dados de saúde.
Exercício regular de direitos (art. 7º, VI e art. 11, I, "d").	Aplicável	Aplicável, com adição da expressão "inclusive em contrato"	Um hospital fornece dados do prontuário de um paciente em uma ação judicial para provar a correta prestação de serviço.
Proteção da vida ou da incolumidade física do titular ou de terceiro (art. 7º, VII e art. 11, I, "e")	Aplicável	Aplicável	Informar ao SAMU o histórico médico relevante de um paciente inconsciente, no âmbito da prestação de socorro em emergências médicas.
Tutela da saúde (art. 7º, VIII e art. 11, I, "f")	Aplicável	Aplicável	Durante a consulta médica, o profissional coleta informações sobre histórico de saúde do paciente atendido.
Legítimo interesse (art. 7º, IX)	Aplicável	Não aplicável	Envio de link para o paciente participar de pesquisa de satisfação, sem que haja qualquer

[132] De acordo com o Guia Orientativo Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas da ANPD, o art. 13 ratifica a autorização para disponibilização de acesso a dados pessoais para fins de realização de estudos e pesquisas, estipulando, em acréscimo, medidas específicas de prevenção e segurança a serem observadas no campo dos estudos de saúde pública. Assim, os dados pessoais devem ser tratados exclusivamente dentro do órgão e para o atendimento à estrita finalidade da pesquisa, vedada a sua transferência para terceiros. Além disso, devem ser armazenados em ambiente controlado e seguro, com a sua anonimização ou pseudonimização sempre que possível. Por fim, devem ser observados os padrões éticos aplicáveis à hipótese, não se admitindo a revelação de informações pessoais por ocasião da publicação do resultado do estudo. Disponível em <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf>.

			tratamento de dados pessoais sensíveis.
Proteção do crédito (art. 7º, X)	Aplicável	Não aplicável	Uma clínica médica consulta o histórico de crédito de um paciente antes de permitir o parcelamento de procedimentos de alto custo.
Garantia da prevenção à fraude e à segurança do titular (art. 11, I, "g").	Não	Sim	Um hospital utiliza biometria para identificar pacientes e evitar fraudes no atendimento.

Fonte: autora

Igualmente, o regulamento europeu também traz distinções específicas para o tratamento de dados pessoais sensíveis, em especial para a área da saúde, sob a ótica do tratamento para fins assistenciais, conforme disposto no art. 9º, no qual destaca-se o tratamento para a proteção dos interesses vitais do titular; o tratamento for necessário para efeitos de medicina preventiva ou do trabalho; o tratamento por motivos de interesse público no domínio da saúde pública.

Conforme se demonstrará a diante, algumas das bases legais previstas na LGPD possuem especial relevância quando se objetiva legitimar o tratamento de dados no âmbito da saúde, contudo, no momento, a base legal mais usualmente empregada e, que por muitas vezes, emerge como uma tábua de salvação para o tratamento de dados pessoais, é o consentimento.

2. Consentimento como base legal vs. consentimento informado

Nesta seção, objetivo central deste trabalho, serão analisados esses dois conceitos sob as perspectivas de aplicação, estrutura e requisitos.

2.1 Consentimento enquanto base legal

Conforme indicado no item 1.2 deste artigo, a LGPD traz tanto em seu art. 7º, quanto 11, diversas opções de justificativas legais para o tratamento de dados pessoais. Contudo, não é incomum deparar-se com o mito há muito difundido de que a "rainha das bases legais" é o consentimento, devendo ser utilizada prioritariamente, sendo que as outras hipóteses autorizadoras atribuídas de maneira secundária. Apesar de a base legal do consentimento ser apresentada geograficamente em primeiro lugar, no inciso I dos referidos artigos, tal entendimento não se sustenta, uma

vez que não há hierarquia entre as bases legais. Entretanto, a ilusão de que o consentimento se sobrepõe às outras bases legais não se mostra uma mera ficção na mentalidade dos indivíduos, tendo origem, na verdade, em algumas vertentes, como i) a existência de legislações anteriores que já se debruçavam acerca do consentimento (ex. Marco Civil da Internet[133]); ii) o disposto nas legislações de países da América do Sul, que determinam o uso do consentimento como fonte primária para o tratamento de dados pessoais[134]; e iii) o próprio projeto da LGPD, que, em seu primeiro texto submetido à consulta pública em 2010, trazia o consentimento como regra[135]. Contudo, o texto aprovado e promulgado da LGPD, assemelhou-se ao regulamento europeu, no sentido de que não há prevalência de uma base legal sob a outra, conforme se verifica pelo Considerando 40 do RGPD.

A LGPD (art. 5º, XII) e o RGPD (art. 4º, n. 11) indicam o consentimento como uma das bases legais cabíveis para o tratamento de dados pessoais e, concatenando os entendimentos, define-se o consentimento como sendo a manifestação livre, específica, informada, inequívoca e explícita de vontade do titular, por meio de declaração ou ato positivo, para o tratamento de seus dados pessoais com finalidade determinada. Cinco requisitos são essenciais para sua validade: i) manifestação de vontade; ii) livre; iii) específico; iv) informado; e v) inequívoco, de forma que, com base na Diretriz 05/2020 do EDPB[136] e o RGPD (especialmente, os Considerandos 32, 42 e 43), serão analisados cada um desses requisitos.

Quanto ao primeiro requisito, entende-se que o consentimento deve ser uma declaração ou ato afirmativo inequívoco do titular, ou seja, uma ação ativa[137] mas sem forma definida, podendo ser escrito ou verbal, excluindo-se a presunção de consentimento pelo silêncio ("quem cala consente"). Em relação ao segundo requisito, o titular deve consentir livre e espontaneamente, sem coação ou desequilíbrio de poder (como em relações empregatícias). A granularidade do consentimento é essencial, assim, quando o tratamento abranger múltiplas

---

[133] Em especial o art. 7º, inciso VII (não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei) e art. 16, inciso I (dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente).

[134] Como se observa pela legislação da Argentina (Lei nº 25.326 de 2000 – PDPA), Colômbia (Lei Estatutária nº 1.581 de 2012), Chile (Lei nº 19.628 de 1998) e Peru (Lei nº 29.733 de 2011).

[135] Conforme ensinamentos de BIONI (2021): Art. 9º - O tratamento de dados pessoais somente pode ocorrer após o consentimento livre, expresso e informado do titular, que poderá ser dado por escrito ou por outro meio que o certifique, após a notificação prévia ao titular das informações constantes no art. 11.

[136] EDPB (European Data Protection Board). (2020). *Diretriz 05/2020 relativa ao consentimento na acepção do Regulamento 2016/679*. Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf. Acessado em 26 de janeiro de 2025.

[137] No mesmo sentido, o art. 8º, *caput* e inciso I indicam que o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular e, caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

operações e finalidades, o titular deve poder consentir individualmente para cada uma delas.

Quanto ao terceiro e quarto requisito, o consentimento deve ser específico, assegurando controle do usuário e transparência, bem como o controlador tem o dever de informar[138] o titular sobre o tratamento antes de obter o consentimento. Por isso, alterações na finalidade do tratamento que sejam incompatíveis com o consentimento original exigem comunicação prévia ao titular, que poderá revogar seu consentimento (art. 9º, §2º, LGPD). Quanto ao último requisito, entende-se que o consentimento deve ser fornecido de forma inequívoca, ou seja, sem ambiguidades ou dubiedades que possam deixar o titular com dúvida sobre aquilo que está consentindo.

Ademais, recai sobre o controlador a responsabilidade de: i) comprovar que obteve o consentimento de maneira válida; ii) gerir o consentimento coletado; iii) fornecer, de modo facilitado, opção para a revogação do consentimento; e iv) quando solicitado pelo titular, excluir os dados tratados com base no consentimento. Portanto, no contexto da proteção de dados pessoais, o consentimento desempenha um papel central como base legal para o tratamento de dados, mas com características e finalidades distintas em relação ao consentimento informado.

2.2 Consentimento informado na área da saúde

A ideia da coleta do consentimento informado na relação médico-paciente emerge desde o tempo da Grécia antiga, por meio do médico Hipócrates, conforme destacado por MILES (2009) "os tratados médicos da época do Juramento retratam um modelo atraente para os médicos – a comunicação do paciente e garantia do consentimento[139]" (tradução nossa). Contudo, a relevância do consentimento informado ganha força no cenário pós II Guerra Mundial, especificamente com o Código de Nuremberg, que dispõe não apenas sobre a autonomia do paciente, mas também traz os contornos essenciais acerca do denominado consentimento informado, reforçado pela Convenção de Helsinque de 1964, a qual traz mais contornos ao "Termo de Consentimento Livre e Esclarecido" (TCLE), utilizado para fins de pesquisas e investigações científicas e clínicas, que não será objeto deste estudo,

[138] De acordo com o art. 9º da LGPD, devem ser fornecidas ao titular, minimamente, as seguintes informações: finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; responsabilidades dos agentes que realizarão o tratamento; e direitos do titular. Ainda, o RGPD adiciona informações acerca da utilização dos dados para decisões automatizadas (art. 22.º, n.º 2, alínea c), quando pertinente, e Informações sobre os possíveis riscos de transferências de dados devido à inexistência de uma decisão de adequação e de garantias adequadas (art. 46).

[139] MILES, Steven H. Hippocrates and Informed Consent. *The Lancet*, v. 374, n. 9698, p. 1322-1323, oct. 2009. Disponível em: < https://pubmed.ncbi.nlm.nih.gov/19847959/ >. Acesso em: 26 de janeiro de 2025.

o qual foca apenas no consentimento informado para o tratamento médico, cirúrgico ou terapêutico.

Assim, o consentimento informado é um princípio fundamental da ética médica, garantindo que os pacientes possam tomar decisões sobre seus cuidados de saúde de forma livre, informada e consciente, sendo essencialmente reconhecido no contexto clínico, uma vez que este documento ético-jurídico constitui o reconhecimento do valor da autonomia do paciente, pois observa fundamentalmente regras institucionais e legais para formalizar a relação profissional de saúde e paciente (DALLARI, apud Oliveira, 2020).

Por sua vez, no Brasil, a Recomendação 1/2016 do Conselho Federal de Medicina dispõe que o consentimento consiste no ato de decisão, concordância e aprovação do paciente ou de seu representante legal, após a necessária informação e explicações, sob a responsabilidade do médico, a respeito dos procedimentos diagnósticos ou terapêuticos que lhe são indicados[140]. Já o Código de Ética Médica brasileiro também dispõe acerca do consentimento livre e esclarecido do paciente, qualificando a autonomia do paciente, nas escolhas referentes à assistência médica e veda, ao médico, deixar de obter consentimento do paciente, ou de seu representante legal, após esclarecê-lo sobre o procedimento a ser realizado, salvo em caso de risco iminente de morte[141].

Por sua vez, LIMA, PIEROTE (2022), indicam que em Portugal, o Regulamento nº 707/2016,[142] que aprovou o Código Deontológico da Ordem dos Médicos, condiciona a validade do consentimento à capacidade do paciente, podendo ser de forma oral ou escrita, desde que a decisão seja livre e precedida das informações pertinentes, inexistindo coações físicas ou morais, devendo, ainda, existir um tempo entre o esclarecimento e o consentimento, para que o paciente possa pensar ou até pedir conselhos, sem previsão da revogação do consentimento.

Ainda no âmbito do ordenamento jurídico português, de acordo com a leitura da Norma nº 015/2013 da Direção-Geral da Saúde[143] (DGS), pode-se definir o consentimento informado como uma autorização, livre e esclarecida, dada por um paciente após ser devidamente informado.

Tal qual o consentimento enquanto base legal, o consentimento informado também possui certos requisitos a serem observados: i) deve ser esclarecido e informado, ou

---

[140] Recomendação 1/2016 do CFM. Disponível em <https://portal.cfm.org.br/images/Recomendacoes/1_2016.pdf> Acessado em 26 de janeiro de 2025.

[141] Código de Ética Médica[141] (Resolução CFM nº. 2.217 de 27 de setembro de 2018). Disponível em <https://portal.cfm.org.br/images/PDF/cem2019.pdf> Acessado em 26 de janeiro de 2025.

[142] PORTUGAL. Ordem dos Médicos. Regulamento nº 707/2016. Regulamento de deontologia médica. Diário da República: série II, Porto, n. 139, 21 jul. 2016. Disponível em: <https://dre.pt/home/-/dre/75007439/details/maximized>. Acesso em 26 de janeiro de 2025.

[143] PORTUGAL, DIREÇÃO GERAL DA SAÚDE (2013). Norma nº 015/2013 relativa ao Consentimento informado, esclarecido e livre para atos terapêuticos ou diagnósticos e para a participação em estudos de investigação. Disponível em <https://static.sanchoeassociados.com/DireitoMedicina/Omlegissum/legislacao2013/Outubro/DGS_015_2013.pdf>. Acessado em 26 de janeiro de 2025.

seja, o paciente deve receber informações completas, compreensíveis e relevantes sobre a natureza, os benefícios, os riscos e as alternativas de um procedimento, ato terapêutico ou diagnóstico; ii) deve ser livre, ou seja, deve ser voluntário, sem coerção ou influência indevida (interna ou externa), de forma que o paciente deverá ter liberdade de escolha; iii) deve ser fornecido por paciente que tenha a capacidade de entender e compreender com o que o está consentindo.

De acordo com Djenane Nodari, para a conclusão da existência dessa capacidade de compreensão (ligada ao conceito de autonomia) devem ser observadas as seguintes escalas: a) a capacidade de expressar ou comunicar uma preferência; b) entender a própria situação e suas consequências; c) entender as informações relevantes; d) oferecer um motivo; e) deve fundamentar sua motivação de forma racional; f) oferecer motivos relacionados com riscos e benefícios; e g) chegar a uma decisão razoável (tendo por base o modelo de uma pessoa razoável)[144].

Na prática, o consentimento informado é indispensável em contextos como cirurgias, tratamentos experimentais e estudos clínicos, sendo uma ferramenta que equilibra os direitos do paciente e a responsabilidade do profissional de saúde, além de trazer proteção ao direito fundamental à vida, à saúde e, incidentalmente, à privacidade, sendo comumente coletado o denominado Termo de Consentimento Informado[145], que não se confunde com o consentimento enquanto base legal.

Isto porque, de acordo com SOARES (2021), o consentimento informado não diz respeito aos dados do titular-paciente, os quais são utilizados definição de um diagnóstico, para indicação de um prognóstico, de forma que o consentimento (enquanto base legal) precede o denominado consentimento informado, que se relaciona com o princípio da incolumidade das esferas jurídicas[146].

2.3. Semelhanças e diferenças entre os consentimentos

As tabelas abaixo comparam as semelhanças e diferenças dos institutos, considerando os principais pontos.

Tabela 3 – Semelhanças entre consentimento informado e consentimento enquanto base legal

Aspecto	Semelhanças entre os consentimentos

[144] NODARI, Djenane. Requisitos e exceções do consentimento informado na relação médico-paciente. ordem democrática. Disponível em <https://ordemdemocratica.com.br/requisitos-e-excecoes-do-consentimento-informado-na-relacao-medico-paciente/>. Acessado em 26 de janeiro de 2025.

[145] Para melhor exemplificação, a Sociedade Brasileira de Dermatologia disponibiliza modelo do referido documento em https://www.sbd.org.br/mm/cms/2019/03/21/termodeconsentimento-edit.pdf.

[146] De acordo com SOARES (2021), esse princípio impede a interferência desautorizada de terceiros na esfera de uma pessoa, a qual é integrada pelos direitos de personalidade, inerentes à condição humana, que contemplam a vida, a saúde e o direito ao próprio corpo.

Manifestação da vontade	Tanto o consentimento enquanto base legal, quanto o consentimento informado, são instrumentos que exprimem a vontade de um indivíduo, na forma de um ato positivo, que visa comprovar e validar determinada permissão fornecida por ele próprio, para que um terceiro possa atuar, seja esta pessoa considerada um agente de tratamento ou um profissional da saúde, por exemplo.
Forma de concessão	O consentimento enquanto base legal possui forma livre de manifestação, pode ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (art. 8º, *caput,* LGPD) contudo, o mais usual é sua coleta em formato escrito e destacado, em especial quando se trata de dados pessoais sensíveis, sendo uma maneira de posterior comprovação da validade do consentimento, inclusive para fins de *accountability* e para sua própria gestão. O mesmo se aplica ao consentimento informado, coleto por escrito ou de outra maneira, como apenas acenar com a cabeça ou, ainda, um paciente pode estender o braço para uma injeção sem indicar[147].
Momento da obtenção	Os consentimentos devem ser coletados antes do tratamento de dados pessoais e antes do atendimento/procedimento médico ou antes da realização de pesquisa científica.
Liberdade de concessão	Ambos os consentimentos são pautados no requisito principal da liberdade, ou seja, o consentimento deve ser fornecido de forma livre, sem coação, pressão ou constrangimento.
Dever informacional	Apesar da diferença entre ao que deve ser informado (conforme apontado nos itens 2.1 e 2.2) , ambos os consentimento exigem que o indivíduo receba instruções mínimas sobre ao que está consentindo. De forma que informações enganosas, dúbias ou que não sejam devidamente esclarecidas, podem invalidar o consentimento fornecido. Ainda, caso haja

[147] SINGLETON, WADSWORTH (2006). Confidentiality and consent in medical research - Consent for the use of personal medical data in research. BMJ (Clinical research ed.). 333. 255-8. 10.1136/bmj.333.7561.255. Disponível em <https://www.bmj.com/content/333/7561/255>. Acessado em 26 de janeiro de 2025.

	alteração da finalidade e de demais informações essenciais que pautaram a concessão do consentimento, o indivíduo possui não apenas o direito de revogar o consentimento, quanto deve fornecer nova autorização, caso assim concorde. Inclusive, ambos os consentimentos não podem ser genéricos, sob pena de também serem considerados nulos.
Revogação	Ambos os consentimentos podem ser revogados a qualquer tempo.

Fonte: autora

Tabela 4 – Diferenças entre consentimento informado e consentimento enquanto base legal

Aspecto	Consentimento (Base Legal)	Consentimento Informado
Finalidade	Legitimar o tratamento de dados pessoais em conformidade com normas de privacidade e proteção de dados.	Garantir a autonomia do paciente em decisões sobre tratamentos, intervenções médicas e pesquisas, permitindo a prática de determinado ato profissional, que atinja sua própria esfera física ou psíquica.
Objetivo de aplicação e natureza	Tem como alvo os dados pessoais do paciente, inclusive o seu corpo eletrônico e diz respeito a sua vida virtual ou a real documental[148].	Tem como alvo o corpo físico ou a esfera psíquica do paciente e diz respeito a sua vida não virtual (concreta e real)[27].
Natureza	Para o uso de dados sensíveis o consentimento é ato jurídico *stricto sensu*, conquanto a definição da natureza dependa do	Ato jurídico *sui generis* existencial. Não envolve, em si, contraprestação econômica ou financeira. No entanto, o

[148] SOARES, Flaviana Rampazzo. Consentimento no direito da saúde nos contextos de atendimento médico e de LGPD: diferenças, semelhanças e consequências no âmbito dos defeitos e da responsabilidade. Revista IBERC, Belo Horizonte, v. 4, n. 2, p. 18-46, maio/ago. 2021. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/170. Data de acesso 26/01/2025.

	contexto da relação estabelecida com os demais figurantes e do conteúdo do ajuste que venha a ser estabelecido[149].	consentimento para pesquisa científica pode se aproximar de negócio jurídico, quando a participação do paciente for a moeda de troca para a obtenção de um tratamento envolvido na pesquisa[28].
Ausência de coleta	Caso não seja coletado o consentimento, deve haver alguma outra base legal que legitime o tratamento de dados pessoais. Se inexistente outra base legal, o tratamento será ilegítimo.	O médico não poderá atuar sem o consentimento do paciente, exceto nas hipóteses de atendimento independentemente de consentimento[150].
Âmbito de aplicação	Tratamento de dados pessoais e dados pessoais sensíveis em diversas atividades e segmentos, não se limitando apenas à área da saúde.	Relações médico-paciente, realização de procedimentos e atendimento médicos, cirurgias e tratamentos.
Responsabilidade	O controlador do dado deve comprovar a obtenção do consentimento válido e específico.	O profissional de saúde ou estabelecimento tem o dever de garantir que o paciente compreendeu as informações.
Capacidade em consentir	De acordo com o art. 14, §1º da LGPD, o consentimento para o tratamento de dados de criança deve ser fornecido por menos um dos pais ou pelo responsável legal, de forma que infere-se que adolescente (indivíduo com 12 anos completos, nos termos do Estatuto da Criança e Adolescente)	Deve ser fornecido por aquele que possua capacidade civil, nos termos definido pelos art. 3º, 4º e 5º do Código Civil brasileiro, ou seja, por indivíduo com 18 anos completos ou nos casos das exceções do parágrafo único do art. 5º do Código Civil.

[149] Ibidem.

[150] De acordo com Djenane Nodari, há duas exceções para a ausência da coleta de consentimento: i) a renúncia à informação (paciente quem escolhe não ser informado, não querer receber esclarecimentos sobre eventual diagnóstico negativo e ou sobre o curso de um tratamento por parte do profissional); e ii) o privilégio terapêutico (médico decide que a revelação integral da informação poderá causar prejuízos à saúde do paciente e ou a realização imediata de uma decisão autônoma).

	pode fornecer seu consentimento.

Fonte: autora

Respondendo-se à questão central do presente trabalho, o consentimento informado e o consentimento enquanto base legal não podem ser entendidos como sinônimos, sendo que a principal diferença reside na natureza de sua aplicação, pois de um lado, o consentimento informado é centrado no indivíduo, focando na preservação da autonomia pessoal, enquanto o consentimento como base legal está vinculado ao interesse coletivo e à conformidade normativa, em especial no tratamento de dados pessoais. É necessário reforçar que ambos os institutos podem (ou não) coexistir, pois enquanto para a realização de procedimento médico é necessária a coleta do consentimento informado, o mesmo não se pode falar do consentimento enquanto base legal, isto porque a LGPD traz outras hipóteses autorizadoras que vão além do consentimento e que legitimam o tratamento de dados pessoais, bem como há demais alternativas a serem empregadas.

3. Alternativas à utilização do consentimento enquanto base legal

Conforme indicado nas seções anteriores, a utilização do consentimento enquanto base legal se mostra muito bem aceita, contudo, esse instituto apresenta algumas limitações como indica BIONI (2019), o qual destaca que o consentimento, apesar de essencial, deve ser utilizado com parcimônia, pois atribuir ao consentimento o papel de legitimar todos os tratamentos de dados seria sobrecarregar o titular com decisões que ele, muitas vezes, não está apto a tomar, de forma que haveria uma fadiga do consentimento. Igualmente, DONEDA (2019) alerta que, em muitos casos, o consentimento pode ser ilusório, especialmente em situações em que o titular não possui real liberdade para escolher. Ainda, a utilização exclusiva do consentimento para o tratamento de dados pessoais, em especial dados de saúde, possui alguns reveses, como i) desafio na coleta e gestão, principalmente quando se trata da coleta do consentimento de um elevado número de titulares, em que o controlador terá uma responsabilidade complexa e onerosa em gerir todos os consentimentos, além de garantir que não haja falhas documentais que comprometam a validade do consentimento; ii) ilusão de hierarquia entre as bases legais, uma vez que a utilização massiva do consentimento pode inferir que esta hipótese legal se sobrepõe às demais; iii) dificuldade em garantir a ampla compreensão do titular, uma vez que estudos demonstram que a maioria das pessoas não leem o que estão assinando ou consentindo[151]; iv) desigualdade entre as partes, pois, considerando o âmbito de

[151] A título de exemplo, a pesquisa realizada pela Delloite em 2017 indica que 91% das pessoas concordam com os termos e condições sem lê-los (disponível em https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf).

saúde, por vezes o paciente pode ser considerado hipossuficiente frente ao agente de tratamento (ex. pacientes que precisam urgentemente de atendimento médico podem sentir-se pressionados a fornecer consentimento para o tratamento de seus dados), o que poderia invalidar o consentimento coletado; e v) não adequação a todas as situações, por exemplo, na época da pandemia, havia a obrigação legal de notificação ao Ministério da Saúde acerca dos resultados de testes diagnóstico para detecção da COVID-19, nos termos da Portaria nº. 1.792/2020, neste cenário, haverá o tratamento de dados pessoais de saúde (resultado de exame) será pautado na base do cumprimento de obrigação legal (art. 11, II, a, LGPD).

Por mais que muitos doutrinadores defendam a predominância na utilização do consentimento (como DALLARI, 2020) enquanto base legal para o tratamento de dados pessoais na área da saúde, por se alinhar à autonomia individual, promover a transparência e estar em harmonia com as práticas médicas e éticas, é necessária a utilização de alternativas à coleta do consentimento, quando este não se mostrar a hipótese legal mais adequada, como defendido por BIONI (2019) e DONEDA (2019). A primeira a alternativas ao consentimento é a utilização de outras bases legais, conforme exemplos específicos indicados na tabela 2 do item 1.2 deste artigo, destacando-se:

Tabela 5 – Principais bases legais utilizadas na área da saúde para o tratamento médico ou terapêutico

Base legal	Definição
Tutela da saúde	Base legal exclusiva para profissionais da saúde, serviços de saúde ou autoridade sanitária, justificando o tratamento de dados sensíveis quando estritamente necessário para a prestação de cuidados, prevenção, diagnóstico e tratamento de doenças. A legitimidade reside na preservação e promoção da saúde individual e coletiva.
Proteção a vida ou da incolumidade física do titular ou de terceiros	Aplica-se a situações de risco iminente para a vida ou a integridade física do titular dos dados ou de terceiros, independentemente do setor. Embora não seja exclusiva da área da saúde, é frequentemente aplicada nesse setor
Cumprimento de obrigação legal ou regulatória	Abrange determinações previstas na legislação nacional, internacional ou em normativos de órgãos reguladores
Execução de políticas públicas	Exclusiva para a administração pública direta e indireta, justifica o tratamento de dados sensíveis quando

Já no estudo de Christopher PP quanto à capacidade de leitura de termos de consentimento, com 154 participantes de pesquisa biomédica relativa a doença mental, foi observado que 35% da população não tinha o nível escolar mínimo exigido para compreender o documento (disponível em https://pubmed.ncbi.nlm.nih.gov/17287380/). Com base nisso, não é improvável que os titulares, de fato, deem seu consentimento (enquanto base legal) sem ler ou compreender aquilo que estão autorizando.

necessário para a execução de políticas públicas de saúde, desde que demonstrado o atendimento à finalidade pública e a persecução do interesse público

Fonte: autora

Ainda, é vedada a comunicação ou o uso compartilhado de dados pessoais sensíveis referentes à saúde entre controladores com o objetivo de obter vantagem econômica. Além disso, no caso das operadoras de planos privados de assistência à saúde, é proibido o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, bem como na admissão ou exclusão de beneficiários, nos termos dos §4º e 5º, do art. 11 da LGPD.

Outra alternativa é a anonimização, que é o uso de técnicas que tornam os dados irreversíveis, impedindo a identificação direta ou indireta do titular (art. 5º, XI, LGPD). Quando os dados são anonimizados, eles deixam de ser considerados pessoais, não estando sujeitos às LGPD e não sendo necessária a indicação de uma base legal. Essa solução possui algumas vantagens, como i) reduzir os riscos de violação de privacidade; ii) permitir o uso de dados em larga escala para estudos científicos; e iii) conciliar a inovação e proteção de direitos fundamentais. Um exemplo da utilização da anonimização seria demonstrar ao CRM que o esculápio estava em plantão em uma determinada data e que, na ocasião, atendeu "x" pacientes, em vez de apresentar o prontuário dos "x" pacientes, deverá solicitar ao próprio hospital um relatório anonimizado com o número de atendimentos, complexidade, setor e horário, de forma que o máximo de anonimização deverá ser empregado para que seja atingida a finalidade almejada, sem expor desnecessariamente dados sensíveis de pacientes[152]. Dentre as técnicas a serem utilizadas, destaca-se a supressão generalização, perturbação e microagregação (OLATUNJI, et al. 2024). Contudo, a anonimização também apresenta desvantagens significativas que podem limitar sua aplicação em determinados contextos. Em primeiro lugar, há situações em que a atividade em si exige a rastreabilidade e a identificação do titular, como no caso do uso de prontuários médicos, em que a identificação do paciente é essencial para o atendimento adequado. Além disso, a anonimização enfrenta limitações técnicas quando aplicada a dados não textuais e desestruturados, como imagens, áudios e vídeos, ou a dados em fluxo contínuo, cuja complexidade e dinamicidade dificultam o processo de anonimização.

Outro desafio é o alto custo computacional associado à aplicação de técnicas de anonimização em grandes volumes de dados ou em fluxo contínuo, o que pode tornar sua implementação inviável em cenários que demandam

[152] SOARES, Flaviana Rampazzo. Consentimento no direito da saúde nos contextos de atendimento médico e de LGPD: diferenças, semelhanças e consequências no âmbito dos defeitos e da responsabilidade. Revista IBERC, Belo Horizonte, v. 4, n. 2, p. 18-46, maio/ago. 2021. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/170. Data de acesso 26/01/2025.

processamento em tempo real (ANPD, 2023). Ainda, a eficácia da anonimização pode ser comprometida por técnicas avançadas de reidentificação, como o cruzamento de dados com fontes externas, ataques de reconstrução que exploram padrões nos dados anonimizados, ou o uso de algoritmos de desanonimização capazes de reverter o processo de anonimização (OLATUNJI, et al. 2024). Esses fatores destacam a necessidade de avaliar cuidadosamente os riscos e as limitações da anonimização antes de sua aplicação, garantindo que a proteção dos dados pessoais seja eficaz e alinhada aos requisitos legais e operacionais.

A última alternativa é a utilização de dados sintéticos, que, de acordo com VALENTE (2022) são aqueles dados criados artificialmente ao invés de serem gerados por eventos reais, de forma que estes dados não se baseiam em registos de pacientes, pelo contrário, são gerados a partir dos padrões verificados nos dados de pacientes reais. KOKOSI, HARRON K. (2022) indicam que essa abordagem tem sido cada vez mais utilizada em pesquisas médicas, uma vez que preserva a utilidade estatística enquanto protege a privacidade dos indivíduos, havendo grandes vantagens, como a eliminação do risco de identificação do titular; a facilitação na conformidade com regulamentos de proteção de dados; e a realização de simulações complexas sem expor dados reais. Entretanto, também há suas limitações, como a complexidade na criação de conjuntos de dados precisos e, em alguns casos, nem sempre substituem dados reais em análises específicas, bem como que não conseguem estimar a ocorrência e o efeito de variáveis exógenas (VALENTE, 2022).

Portanto, a utilização de medidas como anonimização, dados sintéticos e atribuição de outras bases legais deve ser avaliada caso a caso, considerando as especificidades da atividade de tratamento em questão, não se esquecendo, contudo, que a coleta do consentimento informado continua a ser necessária, pois trata-se de instituto apartado.

Considerações finais

O presente estudo evidenciou que o consentimento informado e o consentimento como base legal, embora relacionados, possuem características, finalidades e aplicações distintas. O consentimento informado está intrinsecamente vinculado à autonomia do paciente na tomada de decisões clínicas e éticas, enquanto o consentimento como base legal constitui um instrumento jurídico para legitimar o tratamento de dados pessoais em conformidade com as normas de proteção de dados, como a LGPD e o RGPD.

A análise comparativa demonstrou que, apesar de compartilharem elementos como o ser informado, livre e esclarecido, os dois institutos não são sinônimos, mas podem coexistir em determinadas situações. O artigo também desmistificou a visão de que o consentimento, enquanto base legal, é a única solução para legitimar o tratamento de dados pessoais. Essa percepção

centralizadora ignora as limitações práticas desse instituto, como a desigualdade informacional, a revogabilidade e os desafios de sua gestão em cenários complexos. Nesse contexto, alternativas como a utilização de outras bases legais, a anonimização e o emprego de dados sintéticos emergem como estratégias eficazes para mitigar os desafios do consentimento. Essas alternativas oferecem soluções práticas para equilibrar o respeito à privacidade com a necessidade de inovação científica, sendo promissoras no sentido de serem capazes de viabilizar o progresso científico sem comprometer a privacidade dos titulares.

Apesar disso, é fundamental reconhecer que não há uma abordagem única ou universal para legitimar o tratamento de dados pessoais. A escolha da base legal ou da metodologia adequada dependerá das circunstâncias específicas, exigindo uma análise contextualizada caso a caso. Por exemplo, em algumas situações, a base legal do consentimento será aplicável e coexistirá com o consentimento informado; em outras, haverá a aplicação de base legal diversa do consentimento, contudo, será mantida a necessidade da coleta do consentimento informado, por exemplo, durante uma internação hospitalar de urgência, em que o indivíduo assina o termo de consentimento informado, mas que a base legal será a proteção à vida.

Portanto, conclui-se que o tratamento de dados de saúde exige não apenas uma interpretação rigorosa e cuidadosa das normas, mas também uma abordagem inovadora e adaptável, capaz de equilibrar as demandas da ciência e da tecnologia com o respeito aos direitos dos indivíduos.

Referências

BIONI, Bruno (2019). *Proteção de Dados Pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense.

BIONI, Bruno (2021). *Proteção de dados contexto narrativas e elementos fundantes*. Disponível em: https://observatoriolgpd.com/wp-content/uploads/2021/08/1629122407livro-LGPD-Bruno-Bioni-completo-internet-v2.pdf. Acessado em 26 de janeiro de 2025.

BRASIL. (1988). Constituição da República Federativa do Brasil (CRFB). Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acessado em 26 de janeiro de 2025.

BRASIL. (2014). Lei n. 12.965, de 23 de abril de 2014. *Marco Civil da Internet*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acessado em 26 de janeiro de 2025.

BRASIL (2016). Recomendação 1/2016 do CFM. Disponível em: https://portal.cfm.org.br/images/Recomendacoes/1_2016.pdf. Acessado em 26 de janeiro de 2025.

BRASIL. (2018). Lei n. 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acessado em 26 de janeiro de 2025.

BRASIL. (2018). Código de Ética Médica. *Resolução CFM nº 2.217, de 27 de setembro de 2018*. Disponível em: https://portal.cfm.org.br/images/PDF/cem2019.pdf. Acessado em 26 de janeiro de 2025.

BRASIL. (2019). Sociedade Brasileira de Dermatologia. Modelo de Termo de Consentimento Informado para Tratamento Dermatológico. Disponível em https://www.sbd.org.br/mm/cms/2019/03/21/termodeconsentimento-edit.pdf. Acessado em 26 de janeiro de 2025.

BRASIL. (2023). Autoridade Nacional de Proteção de Dados. Guia orientativo Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Disponível em <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf> . Acessado em 26 de janeiro de 2025.

BRASIL. (2023). Autoridade Nacional de Proteção de Dados (ANPD). Estudo técnico sobre anonimização de dados na LGPD: uma visão de processo baseado em risco e técnicas computacionais. Disponível em <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd_uma_visao_de_processo_baseado_em_risco_e_tecnicas_computacionais.pdf>. Acessado em 26 de janeiro de 2025.

Código de Nuremberg. (1997). Tribunal Internacional de Nuremberg. Disponível em: https://www.ghc.com.br/files/codigo%20de%20neurenberg.pdf. Acessado em 26 de janeiro de 2025.

DALLARI, Analluza Bolivar. (2020). *LGPD na saúde*. São Paulo: Revista dos Tribunais.

DONEDA, Danilo. (2019). *Da privacidade à proteção de dados*. São Paulo: Revista dos Tribunais.

EDPB (European Data Protection Board). (2020). *Diretriz 05/2020 relativa ao consentimento na acepção do Regulamento 2016/679*. Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf. Acessado em: 26 de janeiro de 2025.

FERRAZ JÚNIOR, T. S. (1988). Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito, Universidade de São Paulo, 88,* 439-459. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acessado em 26 de janeiro de 2025.

KOKOSI, T., & HARRON, K. (2022). Synthetic data in medical research. *BMJ Medicine, 1,* e000167. doi:10.1136/bmjmed-2022-000167. Disponível em: https://bmjmedicine.bmj.com/content/1/1/e000167. Acessado em: 26 de janeiro de 2025.

LIMA, É. P. S., & PIEROTE, G. A. (2022). Estudo sobre três vertentes do consentimento informado no ambiente de saúde. *Civilistica.com, 11*(2). Disponível em: http://civilistica.com/estudo-sobre-tres-vertentes/. Acessado em: 26 de janeiro de 2025.

MILES, Steven. H. (2009). Hippocrates and informed consent. *The Lancet, 374*(9698), 1322-1323. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/19847959/>. Acessado em: 26 de janeiro de 2025.

NODARI, Djenane. (s/d). Requisitos e exceções do consentimento informado na relação médico-paciente. *Ordem Democrática*. Disponível em: https://ordemdemocratica.com.br/requisitos-e-excecoes-do-consentimento-informado-na-relacao-medico-paciente/. Acessado em 26 de janeiro de 2025.

OLATUNJI, I. E., et al. (2024). A Review of Anonymization for Healthcare Data. *Big data*, *12*(6), 538–555. Disponível em <https://doi.org/10.1089/big.2021.0169>. Acessado em 26 de janeiro de 2025.

PORTUGAL (2013). Direção Geral da Saúde. *Norma nº 015/2013 relativa ao Consentimento informado, esclarecido e livre para atos terapêuticos ou diagnósticos e para a participação em estudos de investigação*. Disponível em: https://static.sanchoeassociados.com/DireitoMedicina/Omlegissum/legislacao2013/Outubro/DGS_015_2013.pdf. Acessado em 26 de janeiro de 2025.

PORTUGAL (2014a). Lei nº 15/2014, de 21 de março de 2014. *Lei consolidando a legislação em matéria de direitos e deveres do utente dos serviços de saúde*. Diário da República: série I, Porto, n. 57, 21 mar. 2014. Disponível em: https://dre.pt/application/conteudo/571943. Acessado em: 26 de janeiro de 2025.

PORTUGAL (2014b). Lei n.º 21/2014. *Lei da Investigação Clínica*. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=2089A0002&nid=2089&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=#artigo. Acessado em: 26 de janeiro de 2025.

SARLET, G. B. S., & CALDEIRA, C. (2019). O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. *Civilistica.com, 8*(1). Disponível em: http://civilistica.com/o-consentimento-informado-e-a-protecao/. Acessado em: 26 de janeiro de 2025.

SINGLETON, P, WADSWORTH. (2006). Confidentiality and consent in medical research: Consent for the use of personal medical data in research. *BMJ (Clinical research ed.), 333,* 255-8. Disponível em: https://www.bmj.com/content/333/7561/255. Acessado em: 26 de janeiro de 2025.

SOARES, Flaviana Rampazzo. (2021). Consentimento no direito da saúde nos contextos de atendimento médico e de LGPD: diferenças, semelhanças e consequências no âmbito dos defeitos e da responsabilidade. *Revista IBERC, 4*(2), 18-46. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/170. Acessado em 26 de janeiro de 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. (2016). Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acessado em: 26 de janeiro de 2025.

VALENTE, António. (2022). Dados sintéticos: o que são e para que servem. *Marketing Farmacêutico*. Disponível em: https://pt.cision.com/cp2013/ClippingDetails.aspx?id=296cfd7d-368d-452c-af4d-5e8e175642f0&analises=1&userid=436c64d9-8659-4b46-8a07-9cd3180a9cff. Acessado em: 26 de janeiro de 2025.

WARREN, S., & BRANDEIS, L. (2013). The right to privacy. *Civilistica.com, 2*(3), 1–22. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/127. Acessado em: 26 de janeiro de 2025.

Espaço Europeu de Dados de Saúde: Big Data de todos para todos. A oportunidade e obrigatoriedade da Inovação e Investigação

César Edgar Machado Penetro [153]

Resumo

Está iminente o Espaço Europeu de Dados de Saúde (EEDS), e com ele o *big data* de dados de saúde acessível a vários atores (públicos e privados). Tem objetivos bem definidos, e um dos quais passa por regular o mercado interno destes dados digitais, que tem elevada relevância na economia digital. O objetivo deste artigo é procurar dar resposta às dúvidas que recaem na utilização secundária de dados de saúde e a sua natureza mercantilista associada. Foi utilizada uma metodologia de pesquisa dogmática e descritiva, que como resultado obteve respostas alinhadas com a necessidade de uma visão de solidariedade e de confiança dos cidadãos na inovação e investigação, pois ao fornecerem os dados de saúde criam uma oportunidade única, para estes, alcançarem a contrapartida desejada de melhores e mais acessíveis cuidados de saúde.

Palavras-chave: Big data; privacidade; dados de saúde; Inovação; Investigação; Solidariedade

[153] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Abstract
The European Health Data Space (EEDS) is imminent, and with it the big data of health data accessible to various actors (public and private). It has well-defined objectives, one of which is to regulate the internal market for this digital data, which is highly relevant to the digital economy. The aim of this article is to address the doubts surrounding the secondary use of health data and its associated mercantilist nature. A dogmatic and descriptive research methodology was used, which resulted in answers in line with the need for a vision of solidarity and citizen trust in innovation and research, since providing health data creates a unique opportunity for them to achieve the desired counterpart of better and more accessible healthcare.

Keywords: Big data; privacy; health data; Innovation; Research; Solidarity

Introdução

A União Europeia (UE) está prestes a avançar com a criação do Espaço Europeu de Dados de Saúde (EEDS), anunciando melhorias na saúde pública a vários níveis, desde a prevenção de doenças ao seu tratamento, impulsionadas em parte pela inovação da indústria, que terá uma grande oportunidade de acesso a dados de qualidade.

Hodiernamente vivemos a era digital, com uma economia digital acompanhada pelo movimento do capitalismo da vigilância, onde ambos vivem da comercialização massiva de dados, e especificamente, os dados de saúde são dos mais valiosos. Os dados digitais são conhecidos como o novo petróleo, e a sua comercialização gera valores avultados. Uma vez mais reiteramos a importância destes dados como sendo dos mais valiosos, na medida que da sua análise e estudo permitem que a indústria parta para a inovação, e alcance a consequente criação de riqueza.

Neste sentido, o EEDS ao congregar dados digitais de saúde dos 27 Estados-membros da União Europeia (EM), recolhidos nos serviços de saúde públicos e privados, criará um *big data* de dados digitais de saúde, para ser compartilhado entre todos aqueles que se afigurarem como parte interessada para a prossecução de um bem comum, ou seja, melhores cuidados de saúde, que se traduz na melhoria do Direito à Saúde. Todavia, é necessário traçar uma linha divisória bem definida sobre os princípios da implementação do EEDS, visto temos vários direitos em conflito, do Direito à Privacidade e Direito à Saúde ao Direito da Autonomia Privada (objetivos comerciais).

Assim, este estudo torna-se importante para esclarecer o público, que é a fonte desses dados, sobre os benefícios reais e efetivos da partilha de dados de saúde para utilização secundária, uma vez que abdicam do seu direito à privacidade por um suposto bem comum. No final, pretende-se que esta pesquisa permita uma resposta esclarecedora a alguma desconfiança existente na sociedade sobre se a partilha de dados para utilização secundária está pensada para o benefício da indústria da saúde.

Para este efeito, o objetivo principal deste estudo é esclarecer se a partilha de dados para uso secundário no EEDS está talhada para contribuir na melhoria da saúde pública, ou para agilizar a comercialização regulada de dados digitais e acabar por ceder a uma mercantilização dos dados de saúde.

Neste artigo científico serão utilizados dois tipos de metodologia de pesquisa, a pesquisa dogmática e a pesquisa descritiva. A pesquisa dogmática/doutrinária, uma vez que se pretende entender os princípios para a implementação do EEDS, para tal será analisado a proposta e o texto aprovado de Regulamento para o Espaço Europeu de Dados de Saúde, bem como pairará sempre um olhar sobre Direitos Fundamentais de acesso à Saúde e de privacidade da vida privada. A pesquisa descritiva será utilizada na medida que se procura saber a dimensão dos benefícios da implementação do EEDS, procurado descrever qual o impacto e

verdadeira dimensão da partilha de dados para utilização secundária, e no fundo avaliar se resultará em benefício do cidadão, ou se apenas beneficiará o acesso a dados à indústria.

Destarte, este artigo científico é construído sobre três temáticas fundamentais, onde primeiramente se procurar dar a conhecer o EEDS seus objetivos e fundamentos, identificando os benefícios e os benificiários. Numa segunda fase é olhado para o fenómeno do *big data* e sobre qual a perspetiva que deve ser encarada, altruísta ou mercantilista. Por último é dado ênfase à oportunidade única que está a ser dada à Investigação e Inovação, da qual se espera a contrapartida de melhoramento da saúde dos cidadãos.

1. O Espaço Europeu de Dados de Saúde

Com origem na Estratégia Europeia para os Dados[154], e na sequência da fragilidade detetada durante a pandemia COVID-19 no acesso oportuno a dados de saúde, a proposta para a criação do Espaço Europeu de Dados de Saúde (EEDS) vem revolucionar a saúde na Europa. Prossegue vários objetivos, como o de dar às pessoas na UE mais controlo sobre os seus dados de saúde, criar sistemas seguros e fiáveis para a utilização de dados para apoio em melhores cuidados de saúde, e ainda para melhorar a decisão política. Permitirá, por isso, o acesso a informações importantes de saúde a investigadores, à indústria, bem como a decisores políticos. Ao mesmo tempo que o EEDS aborda estes desafios de acesso e transmissão de dados de saúde eletrónicos, visa também dar resposta à interoperabilidade limitada e à fragmentação da interpretação de normas entre os Estados-Membros da União Europeia que até então foram detetadas. Além disso, visa também contribuir para a criação de um mercado único de dados de saúde através da harmonização de regras.[155]

Neste sentido o EEDS será regulado em harmonia com os valores fundamentais da União, bem como em atos legislativos de grande relevo.[156] A Comissão Europeia

---

[154] Comissão Europeia. Estratégia Europeia para os Dados (2020). Acesso 02-01-2025, disponível em https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_pt

[155] Comissão Europeia. Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao Espaço Europeu de Dados de Saúde (2022). Acesso 02-01-2025, disponível em https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0010.02/DOC_1&format=PDF

[156] Os atos legislativos de relevo são o Regulamento Geral sobre a Proteção de Dados (RGPD) https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679; Regulamento Governação de Dados https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R0868 ; Regulamento de Dados https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202302854 ; Diretiva Sistemas de Rede e Informação https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32022L2555, conforme Comissão Europeia. Estratégia para União Europeia da Saúde. Acesso em 02-01-2025, disponível em https://health.ec.europa.eu/ehealth-digital-health-and-care/european-

anuncia-o como o pilar fundamental da União Europeia da Saúde para proteger os cidadãos e dotar a UE e os EM de mais e melhores meios para lidar com situações pandémicas futuras.[157]

Na prossecução desta estratégia, a Comissão define essencialmente duas vias de interesse a desenvolver, se por um lado se verifica a preocupação com a melhoria e salvaguarda saúde pública dos cidadãos, um bem comum, por outro lado é também claro o desenvolvimento e regulação de um mercado digital de dados de saúde, ou seja, o mercado interno de dados. Temos assim um rendilhado de Direitos Fundamentais e valores da UE em conflito, de um lado o Direito à Privacidade, do outro o Direito à Saúde (acesso e melhoria) e o Direito da Autonomia Privada naquilo que ao mercado único digital de dados diz respeito.

Em 24 de abril de 2024 o Parlamento Europeu aprovou em primeira leitura um texto com vista a adoção do Regulamento relativo ao EEDS[158], que visa equilibrar e harmonizar estas preocupações, e foi concebido para inovar em dois grandes campos de ação, o primeiro, como já referido, passa por devolver aos cidadãos o controlo total sobre os seus dados de saúde, para que os possam ter de volta à sua esfera a decisão de partilha. O segundo, com intuito altruísta, em nome de um bem comum, é o de permitir o seu uso para inovação, pesquisa e para questões de saúde pública, no entanto, debaixo de condições estritas.[159]

Olhando para a arquitetura do texto aprovado do Regulamento do EEDS[160], e no mesmo sentido de Recuero (2024), podemos distinguir três pilares fundamentais, com objetivos diferentes:

i. O primeiro pilar vem regular o uso primário de dados de saúde eletrónicos, inserido no Capítulo II, dos artigos 3.º ao 24.º do texto aprovado de Regulamento EEDS;
ii. O segundo procura estabelecer regras para a criação do mercado único digital de dados de saúde eletrónicos, inserido no Capítulo III, dos artigos 25.º a 49.º;
iii. O terceiro vem regular o uso secundário de dados de saúde, para que os mesmos sejam utilizados em benefício da sociedade no melhoramento da saúde pública através da investigação e inovação, e da formulação de melhores políticas de saúde publicas, e está inserido no Capítulo IV, dos artigos 50.º a 81.º.

---

health-data-space_pt

[157] Comissão Europeia. Estratégia para União Europeia da Saúde. Acesso em 02-01-2025, disponível em https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-health-union_pt

[158] Parlamento Europeu. Resolução legislativa do Parlamento Europeu sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo ao Espaço Europeu de Dados de Saúde. Acesso em 02-01-2025, disponível em https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_PT.pdf

[159] Comissão Europeia. Comunicado de imprensa de 24 de abril de 2024. Acesso em 02-01-2025, disponível em https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_2250/IP_24_2250_EN.pdf

[160] https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_PT.pdf, acesso em 05-01-2025

Seguimos por destacar os diferentes níveis de uso dos dados de saúde, que serão assegurados pela infraestrutura de partilha de dados MyHealth@EU.[161]

Assim, no uso primário dos dados de saúde eletrónicos, por exemplo é garantido aos cidadãos o direito de aceder ou solicitar a um prestador de cuidados de saúde que transmita todos ou parte dos seus dados de saúde eletrónicos a outro prestador de cuidados de saúde à sua escolha. Esta partilha ocorrerá de forma imediata, gratuita e sem impedimentos por parte do prestador de cuidados de saúde ou dos fabricantes dos sistemas utilizados por esse prestador de cuidados de saúde. Como disposto no art.º 3º do texto aprovado do Regulamento EEDS, e no mesmo sentido de Costa (2022), o EEDS vem ditar desdobramentos dos direitos de acesso, direito de portabilidade e do direito de informação já contemplados no RGPD. Neste âmbito será também permitido aos profissionais de saúde a consulta dos ficheiros dos seus pacientes com o consentimento destes[162], mesmo a partir de outros países da UE. Estes ficheiros, a título de exemplo, irão conter dados como resumos clínicos dos doentes; receitas eletróncias; resultados de exames médicos, como resultados laboratoriais e de outros diagnósticos e relatórios conexos; e ainda no futuro conterão os exames com imagens e relatórios de imagiologia.

Quanto à utilização secundária de dados de saúde, a estratégia assenta na análise de informações médicas para fins diversos, que não os cuidados diretos ao doente, como por exemplo, para o tratamento de dados para melhoria das políticas de saúde pública, investigação e inovação médica. Os dados de saúde para utilização secundária deverão estar acessíveis a entidades publicas e privadas sem fim lucrativos, e também a investigadores individuais para fins de investigação e inovação. No final, a utilização secundária de dados de saúde é anunciada com o fim último de obter conhecimentos e conclusões para melhorar os cuidados de

[161] A Comissão fica encarregue pela criação desta plataforma sobre a qual recai a interoperabilidade dos dados de saúde com a finalidade de facilitar o intercambio dos dados de saúde eletrónicos, art.º 23.º n.º1 e Art.º 75.º n.º 8 do texto aprovado de Proposta de Regulamento EEDS. Já em 2020 era anunciada a primeira vantagem, para o uso primário de dados, no uso deste canal de comunicação: "*É tranquilizador saber que, em caso de doença ou de um problema de saúde urgente durante a estadia noutro país da UE, estarão disponíveis serviços de saúde eletrónicos transnacionais – prescrição eletrónica e resumo de saúde eletrónico – nos países europeus para proteger e ajudar os viajantes, no âmbito da iniciativa «A minha saúde @ UE».*", disponível em European Commission: Directorate-General for Health and Food Safety. (2020). *A minha saúde @ EU : serviços de saúde eletrónicos transnacionais na UE (Portugal)*. Serviço das Publicações. **https://data.europa.eu/doi/10.2875/023738**.

[162] Os Estados-Membros devem garantir a criação de serviços com a funcionalidade de permitir os cidadãos o direito de se opor ao tratamento dos dados de saúde eletrónicos cfr Art.º 71.º, n.º2 do texto aprovado para o Regulamento EEDS "*Os Estados-Membros preveem um mecanismo de autoexclusão acessível e facilmente compreensível para o exercício deste direito, através do qual as pessoas singulares devem poder manifestar explicitamente a sua vontade de que os seus dados de saúde eletrónicos pessoais não sejam tratados para fins de utilização secundária.*"

saúde prestados ao cidadão e à população em geral, especialmente através de investigação e desenvolvimento.[163]

Em suma, o texto aprovado de Regulamento EEDS recai sobre a utilização primária e secundária de dados pessoais no setor da saúde, ao abrigo das exceções contidas no nº 2, alíneas g), h), i) e j), do artigo 9º do RGPD, ao mesmo tempo que regula o mercado digital de dados de saúde eletrónicos, anunciando benefícios em várias dimensões.

1.1 Benefícios e benificiários - visão sobre a natureza dos interesses

Quem beneficia com o EEDS? Uma questão de fácil construção, mas não tão fácil resposta e explicação. Na verdade, por enquanto apenas se podem anunciar intenções, que se esperam exequíveis. Intenções que são por muitos já colocadas em causa, ao ponto de Marelli et al. (2023) afirmar que correrá mesmo o risco de ser contrário aos objetivos e minar o interesse público se não forem feitos ajustes. (p.2)

Os beneficiários anunciados desde o início pela proposta são diversos, engloba atores que tem como finalidade a prossecução do interesse público, e outros essencialmente o interesse privado, pelo que sumariamente os descrevemos[164]:

i. **Pacientes e cidadãos**, a quem é permitido um acesso mais fácil, seguro e eficiente aos seus dados de saúde, independentemente do país onde os dados foram gerados, facilitando também a continuidade dos cuidados, principalmente para aqueles que viajam ou residem em diferentes países da UE. Além disso, os cidadãos ganham maior controlo sobre as suas informações de saúde, promovendo a transparência.
ii. **Profissionais de saúde e prestadores de cuidados de saúde**, o EEDS simplifica o acesso a históricos médicos e outros dados relevantes, permitindo que os profissionais de saúde tomem decisões clínicas mais informadas e seguras. Com dados mais completos e em tempo real, médicos, enfermeiros e outros profissionais podem oferecer um cuidado mais personalizado e eficaz.
iii. **Investigadores**, a iniciativa oferece uma base de dados com a criação de um *big data* de dados de saúde em larga escala, respeitando os valores e legislação da União, o que facilita avanços na investigação médica, como o desenvolvimento de novos tratamentos, vacinas e intervenções. A harmonização dos dados e a forma de partilha dos mesmos entre os países europeus aumenta a qualidade e a relevância da investigação.
iv. **Indústria de tecnologia e inovação em saúde**, o acesso a um volume amplo e diversificado de dados de saúde promove o desenvolvimento de soluções tecnológicas inovadoras, como aplicações de saúde digital, sistemas de apoio à decisão clínica e ferramentas baseadas em inteligência artificial.

[163] Considerando 61 do texto aprovado para o Regulamento EEDS
[164] Comissão Europeia. Perguntas e respostas sobre o Espaço Europeu de Dados de Saúde. (2024). Acesso em 06-01-2025, disponível em https://ec.europa.eu/commission/presscorner/api/files/document/print/pt/qanda_24_2251/QANDA_24_2251_PT.pdf

Assim, é bem explicito que esta iniciativa de criação do EEDS desde o princípio não esconde, na sua natureza e objetivos, a intenção de colocar vários interessados como atores benificiários em medidas de interesse diferenciadas. Já em 2022 num parecer conjunto o Comité Europeu para a Proteção de Dados (CEPD) e a Autoridade para a Proteção de dados (AEPD) afirmava que o EEDS seria uma contribuição significativa "*...tanto para o interesse público como para o interesse dos titulares de dados/doentes a título individual.*"[165] Contudo, Costa (2022) vai mais além acrescentando que com esta proposta são introduzidos novos intervenientes, com interesses próprios:

> "Com efeito, esta nova regulamentação visa colocar em campo novos intervenientes, com interesses próprios, de natureza diversa (e, em alguns contextos, até mesmo contrária) da natureza dos interesses próprios dos titulares de dados e do interesse público, que idealizam o tratamento dos dados de saúde para outras finalidades que não a prestação de cuidados de saúde apenas ou nos moldes tradicionais." (p. 635)

É um facto que passam a existir novos atores, e até se consegue entender que se queira realçar o resultado que a indústria alcançará no campo da inovação e investigação, e prossiga o interesse da Autonomia Privada e o consequente lucro, o que diversifica desde logo a natureza dos interesses. Já quanto à afirmação do interesse contrário ao dos titulares dos dados e interesse público, é uma afirmação mais "*polémica*" de ser tratada, por duas vias de razão, em primeiro que o interesse da autonomia privada nunca é escondido desde o início, e a segunda é que o interesse privado, neste caso a saúde, não é incompatível com o interesse público. Se não olhemos como os sucessos alcançados pela inovação na indústria de saúde rapidamente se refletem em bem-estar e melhores cuidados aos pacientes (prossecução do interesse público), o que não significa que quem inovou não salvaguarde o seu interesse legitimo de obter dividendos resultantes da sua mestria.

Ora, a não ser que existam teorias da conspiração, neste âmbito não parece haver contrariedade de interesses dos atores, mas pelo contrário, que estes possam coexistir em convivência sem "atropelos". Diferente questão poderá ser levantada na tentativa entender em que medida sairão em benefício as partes, haverá equilíbrio na balança?

Ainda sem aferir inclinações na balança, pode afirmar-se, que quanto à utilização primária de dados de saúde são facilmente visíveis os benefícios individuais dos cidadãos e dos operadores de saúde.[166] Agora na questão mais suscetível de interpretações diversas, no que diz respeito ao aproveitamento de dados para

[165] EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space p.3. Acesso a 06-01-2025, disponível em https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en

[166] *Vide* nota de rodapé n. 9

utilização secundária, os benefícios já não sobressaltam na mesma fração de segundos, o que implica uma reflexão esclarecida e mais aprofundada.[167]
Sabemos que a economia de dados é um fenómeno em crescimento, e no campo dos dados de saúde é notável o interesse nesses dados.[168] E se até ao momento na Europa não temos um *big data* de dados de saúde, como são conseguidos dados fiáveis para a inovação na indústria da saúde? Porventura existe esse mesmo acesso sem que o titular dos dados se aperceba[169], e sem que exista algum tipo de retribuição, a não ser um eventual melhoramento do acesso a cuidados de saúde gerado por essa inovação. Poderemos aqui sim, estar perante uma cedência de dados que poderá não ter retorno ao titular de dados.[170]

Enquanto não pudermos quantificar a saúde em valor monetário, o que seria utópico, não podemos fazer uma comparação na mesma medida, todavia, podemos antes aferir outros aspetos, tais como, saber se as novas tecnologias serão colocadas unicamente em instituições privadas de saúde e se apenas alguns cidadãos tem a capacidade de aceder, ou pelo contrário, se serão acessíveis a toda a população sem que para tal seja necessário o aumento de despesas avultadíssimas ao erário público, o que seria desnivelado, uma vez que, quer este globalmente, e cada cidadão individualmente, tiveram já a sua contribuição crucial ao gerar e partilhar os dados de saúde.

Contudo, economicamente falando, prevê-se um potencial de crescimento da economia dos dados de saúde, em que a UE poupa cerca de 11 mil milhões de euros ao longo de dez anos, que significa também um crescimento suplementar do mercado da saúde digital entre 20% e 30%.[171]

---

[167] As preocupações tem sido muitas e de vários quadrantes e quem tema mesmo que tenha efeito contrário ao pretendido, *vide* Marelli, L., Stevens, M., Sharon, T., & Van Hoyweghen, I. (2023). The European health data space: Too big to succeed? Health Policy, 135(4), 104861. https://doi.org/10.1016/j.healthpol.2023.104861; e Costa, T. B. da. (2022). O altruísmo (económico?) de dados: breves considerações sobre o espaço europeu de dados de saúde e a proteção de dados pessoais. In Liber Amicorum Benedita Mac Crorie Volume II (pp. 613–643). UMinho Editora. https://doi.org/10.21814/uminho.ed.105.30

[168] Sobre o enorme impacto dos dados de saúde vide Bahri, S., Zoghlami, N., Abed, M., Tavares, M. R. S., & Tavares, J. M. R. S. (2019). BIG DATA for Healthcare: A Survey. SPECIAL SECTION ON NEW TRENDS IN BRAIN SIGNAL PROCESSING AND ANALYSIS. *IEEE Access*. https://doi.org/10.1109/ACCESS.2018.2889180

[169] Exemplo de um caso do sistema de saúde no Reino Unido (NHS) durante a pandemia de Covid-19, fez acordos com empresas (Google, a Amazon, a Microsoft, a Palantir e a Faculty) para criar um "*armazenamento de dados*" que reunisse dados de todo o NHS para tomada de decisão política, e mais tarde estas empresas treinaram algoritmos para IA para seu próprio lucro (vendendo a quem lhe forneceu os dados), conforme Fitzgerald M, Crider C. We need urgent answers about the massive NHS COVID data deal. Open democracy. 2020. Acesso a 06-01-2025. Disponível em https://www.opendemocracy.net/en/ournhs/we-need-urgent-answers-about-massive-nhs-covid-data-deal/

[170] Sobre a questão da economia de dados e o BIG data na saúde é desenvolvido na próxima secção em 2.

[171] Comissão Europeia. Perguntas e respostas sobre o Espaço Europeu de Dados de Saúde. (2024). Acesso em 06-01-2025, disponível em https://ec.europa.eu/commission/presscorner/api/files/document/print/pt/qanda_24_2251/QANDA_24_2251_PT.pdf; Comissão Europeia. Factsheet on European Health Data Space. (2024). Acesso em 06-01-2025, disponível em

2. *BIG data* da saúde, perspetiva altruísta *vs.* mercantilista

BIG data é definido pela Comissão como "*grandes quantidades de diferentes tipos de dados obtidos a partir de diversas fontes, pessoas, máquinas ou sensores*"[172], todavia, o *big data* necessita de tecnologia de apoio, e não se apoia apenas em tecnologias para o armazenamento. Necessita de tecnologias também para interpretação e valorização dos dados, como algoritmos para identificação de padrões como refere Gonçalves (2024). É criada a expectativa que a tomada de decisão seja melhor e mais informada, mas por outro lado surge também o perigo de estas tecnologias serem empenhadas para a monitorização de humanos e do seu comportamento para fins de vigilância ou marketing. No fundo como conclui Gonçalves (2024) "*O resultado é, como se notou já, a emergência de um modelo de negócio das empresas da Internet baseado no rastreamento da atividade dos indivíduos online.*" (p.221)

No campo da saúde não se passa diferente, e o *big data* é grande no seu tamanho, de diversos tipos e em várias velocidades, Anam e Israrul Haque (2020) descrevem as características em volume, velocidade e variedade.[173]

Assim, quando se fala de *big data* na saúde, fala-se do conjunto massivo e diversificado de dados gerados continuamente a alta velocidade a partir de várias fontes, como por exemplo, registos eletrónicos de saúde de dispositivos móveis e sensores. Dispositivos como *wearables*, incluindo *smartwatches* e monitores de atividades físicas, contribuem significativamente para esta recolha, bem como as aplicações móveis de saúde e plataformas de telemedicina, que geram dados em tempo real sobre as condições de saúde e o comportamento do paciente.[174]

Como, entretanto, se pôde aferir, é grande a quantidade de dados de saúde que são gerados, Costa (2024) usa uma comparação muito esclarecedora que é: se no mundo inteiro fossem compilados todos os livros em suporte físico gerava um *petabyte*[175] de dados, e só no ano de 2023 foram gerados 54 *petabytes* de dados

---

https://ec.europa.eu/commission/presscorner/api/files/attachment/878485/Factsheet%20European%20Health%20Data%20Space_PT.pdf

[172] https://digital-strategy.ec.europa.eu/en/policies/big-data

[173] "*Quantity of data in the datasets is the volume, and mostly, the datasets contain one petabyte of data. Variety is the data from multiple sources (Raghupathi, 2014; Rumsfeld, 2016). Velocity defined as the speed of merging and identifying the datasets to get accurate information for predicting the out-comes (Rumsfeld, 2016)*" Anam & Israrul Haque (2020). Big data analytics in health sector: Need, opportunities, challenges, and future prospects. *In* Big Data Analytics and Intelligence: A Perspective for Health Care. p.18 https://doi.org/10.1108/978-1-83909-099-820201006

[174] Fixe. Filipa (2024). Observador. Saúde inteligente: a era dos dados começou. Podcast GPS Episodio 3 – 20 nov.2024, 10:03. Acesso 08-01-2025. Disponível em https://observador.pt/programas/gps-gestao-pessoas-e-setores/saude-inteligente-a-era-dos-dados-comecou/

[175] "*Um petabyte (PB) é uma das maiores unidades de medição de dados digitais e equivale a aproximadamente 1024 terabytes (TB) ou 2^50 (1,125,899,906,842,624) bytes (B).*
Unidades de medição de dados digitais desse (e maior) tamanho não são usadas para

de saúde, sendo que destes apenas cerca de 3% são utilizados.[176] Esta grande quantidade de dados gerada, tem um senão quanto à sua qualidade, que varia amplamente, pois muitos dispositivos não seguem padrões consistentes de calibração ou validação, o que pode levar a erros ou inconsistências. Os dados de baixa qualidade podem comprometer a precisão das análises e criar riscos, como tratamentos inadequados baseados em informações incorretas. Como conclui Stausberg et al. (2024) representa um desafio para a tecnologia, e ainda não é claro como os grandes modelos de linguagem irão lidar com a qualidade dos dados (p258).[177]

Aqui chegados, podem os *big data* na saúde ser encarados por perspetivas diferentes, uma visão altruísta para aqueles que contribuem com o registo de dados, ou, por outro lado, uma visão mercantilista tendo-se em conta o valor monetário avultado que os dados de saúde geram.

Numa perspetiva altruísta, o foco está na partilha voluntária de dados para o interesse público sem compensação financeira, e como *big data* pode beneficiar a sociedade como um todo, especialmente na saúde pública e no combate a pandemias futuras, tal como anunciado na implementação do EEDS. Neste sentido, os dados compartilhados podem acelerar investigações médicas, melhorar a vigilância epidemiológica e permitir respostas mais rápidas e eficazes a crises sanitárias, e além disso, o acesso a grandes volumes de dados permite o desenvolvimento de modelos preditivos para identificar populações de risco e alocar recursos de forma mais eficiente.

Contudo, isso requer um equilíbrio entre a partilha de dados e a proteção de privacidade, com normas claras para evitar violações de direitos individuais. Costa (2022) desenvolve esta perspetiva e conclui "*Vislumbramos com muita dificuldade que a utilização secundária dos dados de saúde possa ser imposta às pessoas singulares, sob a égide do altruísmo de dados.*" (p.642)

Por outro lado, a perspetiva mercantilista prioriza os ganhos financeiros e a exploração comercial dos dados de saúde. E neste campo nada melhor que olhar para aspetos da economia norte americana, onde empresas de tecnologia como Google e Amazon investem muito em plataformas de saúde digital, e muitas vezes

---

computação diária. Ainda assim, eles são usados para estimar e expressar dados mantidos em arquiteturas complexas de tecnologia da informação, como grandes data centers e infraestrutura de nível empresarial." phoenixNAP. Glossário. Acesso 08-01-2025. Disponível em https://phoenixnap.pt/gloss%C3%A1rio/petabyte

[176] Costa (2024). Observador. Saúde inteligente: a era dos dados começou. Podcast GPS Episodio 3 – 20 nov.2024, 10:03. Acesso 08-01-2025. Disponível em https://observador.pt/programas/gps-gestao-pessoas-e-setores/saude-inteligente-a-era-dos-dados-comecou/

[177] Sobre a qualidade dos dados Stausberg, J., Harkener, S., & Bünz, S. (2024). A Collection of Data Quality Indicators for Health Research: Rationale for an Update. Studies in health technology and informatics, 321, 254–258. https://doi.org/10.3233/SHTI241103; e ainda Alonso, V., Santos, J. V., Pinto, M., Ferreira, J., Lema, I., Lopes, F., & Freitas, A. (2020). Health records as the basis of clinical coding: Is the quality adequate? A qualitative study of medical coders' perceptions. Health information management : journal of the Health Information Management Association of Australia, 49(1), 28–37. https://doi.org/10.1177/1833358319826351

monitoriza os dados recolhidos por meio de algoritmos de análise e IA. Prática esta, que levou a casos controversos de comercialização de dados em massa sem o consentimento dos titulares, por exemplo, em 2019, o escândalo envolvendo a *Ascension* e o *Google* que expôs dados de saúde de milhões de pacientes nos Estados Unidos, que foram partilhados sem notificação prévia ou autorização.[178] Situações semelhantes também ocorreram na Europa, como no caso em que o sistema de saúde do Reino Unido, em que o sistema de saúde (NHS) pode doar os dados de saúde sem consentimento do seu titular à companhia *Deepmind*, o que desencadeou uma série de preocupações éticas.[179]

Para Zuboff (2019) a mercantilização de dados de saúde traduz-se na renderização desses dados[180], que é uma das características do capitalismo de vigilância "… *não pode existir capitalismo de vigilância sem renderização.*" (p.264) Ora, na era do capitalismo de vigilância em que vivemos, a saúde móvel desencadeou uma explosão nesta renderização, com o uso de bandas de fitness e apps. Zuboff (2019) considera que, após estudos comprovados, estes dispositivos e apps transmitiam dados de saúde para empresas de publicidade sem que os utilizadores fossem informados (p.280). Zuboff (2019) afirma ainda que "*Sob o regime do capitalismo da vigilância, os indivíduos não renderizam a sua experiência por escolha ou obrigação, mas por ignorância e ditadura da falta de alternativas (…) a renderização involuntária se tornou facto inescapável." (p.285)* Contribuindo assim para a ideia de que o modelo mercantilista de exploração dos dados de saúde representa um exemplo claro de como as empresas se podem apropriar de dados de saúde para fins lucrativos, sem necessariamente priorizar o bem comum.

Já Véliz (2022), alerta também para os riscos associados à recolha massiva de dados de saúde, argumentando que a falta de controlo sobre essas informações pode comprometer a dignidade e a autonomia dos indivíduos, afirmando mesmo que o avanço da medicina não depende da comercialização de dados (p.216). Acrescenta: "*Não é aceitável usar a população geral como cobaia sem o seu consentimento, sem as salvaguardas necessárias e sem compensação*", defende assim regulações mais rigorosas para impedir que essas práticas coloquem em risco a privacidade e os direitos humanos. (p.221)

Na experiência norte americana, e de acordo com as críticas levadas a cabo pelos autores citados, denota-se uma real preocupação com a forma "*banalizada*" que as autoridades põe e dispõe dos dados de saúde dos pacientes, ao ponto

---

178 https://www.jornaldenegocios.pt/empresas/tecnologias/detalhe/google-recolheu-dados-medicos-de-milhoes-de-pessoas-sem-autorizacao

179 Véliz, Carissa. (2022) Privacidade É Poder. Por Que Razão e como Devemos Recuperar o Controlo dos Nossos Dados p.29, e *vide* nota de rodapé 17.

180 Sobre o tema *vide* Zuboff, Shoshana. (2019) A Era do Capitalismo da Vigilância – A Disputa por Um Futuro Humano na Nova Fronteira do Poder. Relógio D´Água Editores. P.262 e ss. Zuboff (2019) explica que "*renderização*" deriva do verbo "*reproduzir*", como um processo de pelo qual algo se forma através de algo diferente: "*Designa a relação causal que transforma uma coisa noutra...*" (p.263), que é o que acontece com as informações de saúde (experiência) transformada em dados.

mesmo de pedirem mais controlo e regularização, havendo mesmo uma certa desconfiança em quem deveria tutelar a privacidade dos cidadãos. Como tal Véliz (2022) sugere que as instituições de saúde publica que possuem quantidades elevadíssimas de dados de saúde deveriam atuar de forma mais protetora nas relações com empresas:

> "Deviam limitar o acesso das empresas a esses dados. Talvez estas pudessem usá-los, mas não conservá-los, por exemplo. E deviam pedir garantias jurídicas de que qualquer produto desenvolvido seria oferecido às instituições publicas de saúde e ao público, a preços acessíveis." (p.222)

Explanadas as perspetivas, parece correto não atribuir o caracter altruísta da partilha de dados aos cidadãos, pelo que enquanto contribuintes de dados para o *big data* deve ser esperada uma compensação. Compensação que não se traduzirá certamente em quantia monetária, mas, se por um lado é pacifico e aceitável contribuir com dados de saúde para uso secundário[181], será justo esperar uma contrapartida que pode muito bem se traduzir no melhoramento ao acesso a cuidados de saúde, e por valores mais acessíveis. Assim, parece que apenas a inovação e investigação podem alcançar esse benefício, pelo que a oportunidade que lhes é criada com o acesso ao *big data* ganha um caracter de obrigatoriedade para estes criarem benefícios à saúde pública.

3. A oportunidade (com caracter de obrigatoriedade) da Inovação e Investigação

O acesso ao *big data* do EEDS é uma oportunidade sem precedentes para o acesso a dados de saúde reais, em grande escala e de elevada qualidade. Uma vez reunidas estas qualidades, servem também para maiores e melhores avanços nos tratamentos de saúde e pesquisas médicas.

O considerando 61 do texto aprovado para a proposta do EEDS, avança:

> "O acesso aos dados para utilização secundária deverá contribuir para o interesse geral da sociedade. Em especial, a utilização secundária de dados de saúde para efeitos de investigação e desenvolvimento deverá assegurar um benefício para a sociedade sob a forma de novos medicamentos, dispositivos médicos, e produtos e serviços de saúde a preços acessíveis e justos para os cidadãos da União, e deverá também

[181] Comissão Europeia. Consulta pública sobre a Iniciativa EEDS (2024). Acesso em 11-01-2025, disponível em https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12663-A-European-Health-Data-Space/public-consultation_pt ; no mesmo sentido quanto á população alemã Richter *et al* (2024). Attitude towards consent-free research use of personal medical data in the general German population. Heliyon. https://doi.org/10.1016/j.heliyon.2024.e27933

melhorar o acesso a esses produtos e serviços e a sua disponibilidade em todos os Estados-Membros."

Depois do objetivo "*especial*" que é atribuído no texto aprovado da proposta do EEDS à Investigação e Inovação, acrescenta-se o caracter de obrigatoriedade da sua realização para obtenção de valor a retribuir aos pacientes/cidadãos que contribuem para os dados, pois só assim mantém a confiança dos cidadãos.[182]

Aliás, a confiança será a grande base para a construção do *big data* de saúde no EEDS, principalmente no que diz respeito aos dados para utilização secundária e como afirma Marelli *et al* (2023) é crucial manter a confiança do público.[183]

Ao fornecerem dados pessoais de saúde, os cidadãos e pacientes confiam que esses serão utilizados de forma ética e eficiente, e que resultará em benefícios concretos para a melhoria dos cuidados de saúde. Como argumentam Prainsack & Buyx (2017)[184] a solidariedade é a pedra angular para que os cidadãos e pacientes continuem a contribuir com informações sensíveis. Neste sentido, a confiança é abordada implicitamente através do ênfase na governação solidária, que requer um compromisso partilhado e apoio mútuo entre cidadão e comunidade. Esta abordagem sugere que a confiança é um elemento fundamental na construção e manutenção da solidariedade e o mesmo se aplica para a partilha de dados de saúde para uso secundário no EEDS.

Sem a garantia de que esses dados resultarão em soluções acessíveis e inclusivas, corre-se o risco de uma erosão dessa confiança, prejudicando a participação pública no fornecimento de dados de saúde.

O caráter de obrigatoriedade surge, neste contexto, como uma expectativa moral e pragmática que os cidadãos e pacientes, fornecedores de dados, esperam que os avanços decorrentes sejam utilizados para promover cuidados de saúde

---

[182] Costa (2019) refere que nem sempre foi assim, mas a confiança foi novamente conquistada pelo novo quadro do RGPD.

[183] Enquadram mesmo como uma das recomendações políticas: "*It is of crucial importance to preserve public trust in health research. Accordingly, uphold data subjects' rights as enshrined in the GDPR. Reserve informed consent exemptions with regard to secondary use to limited, clearly defined, uses (e.g. cross-border public health threats), or to uses which are already considered 'public interest' in national legislations. In parallel, reinforce the decision-making prerogatives of national health data access bodies, and clarify their relation with ERBs and DPAs*" (p.3)

[184] *Apud* Rhodes,C. (2018) os autores distinguem três "níveis de solidariedade": O nível interpessoal, que envolve interações diretas entre indivíduos; Práticas de grupo, que englobam ações coletivas e compromissos compartilhados dentro dos grupos; e o nível jurídico, que inclui quadros institucionais como sistemas fiscais e administrativos que apoiam a governação solidária. Solidariedade que é definida como um compromisso compartilhado de aceitar custos para apoiar outros que são reconhecidamente semelhantes em algum aspecto. Os autores sugerem ainda que o bem-estar da comunidade é priorizado, potencialmente em detrimento de cálculos individuais de risco-benefício, alinhando-se com a ideia de apoiar outros que são semelhantes em algum aspeto.

acessíveis, tanto em termos de custo como de disponibilidade nos sistemas de saúde públicos.

O caráter de obrigatoriedade reflete, portanto, uma relação de reciprocidade entre os indivíduos e o sistema, pois se os dados são essenciais para avançar na investigação e inovação, o mínimo esperado é que os resultados desses avanços se traduzam em melhorias tangíveis nos cuidados de saúde. Tal abordagem não apenas promove a solidariedade e confiança, mas também garante a sustentabilidade do modelo de compartilhamento de dados no EEDS a longo prazo.

Conclusão

O Espaço Europeu de Dados de Saúde adotou uma postura de transparência total, não escondendo o objetivo de regular um mercado de dados de saúde, com a perfeita noção da economia de dados que hoje domina o mundo. Nesta iniciativa são também claros os diferentes tipos de beneficiários, para além do bem comum de proporcionar um melhor Direito à saúde. E neste sentido não parece haver incompatibilidades de interesses dos diferentes atores e beneficiários, pelo que com a forma regulada que o EEDS pretende implementar, é possível uma perfeita convivência entre todos, com ganhos muito significativos para todos, sendo que no final haverá ganhos substanciais na sociedade.

Para o cidadão são inequívocos os benefícios agregados com a partilha de dados de saúde para uso primário, no entanto a partilha de dados de saúde para utilização secundária pode ser interpretada como uma catapulta para a criação de riqueza na indústria de saúde. Neste aspeto, não podemos pedir uma atitude altruísta por parte dos cidadãos e pacientes ao fornecerem os seus dados de saúde, enfraquecendo o seu Direito à Privacidade. Contudo, uma perspetiva solidária deve ser encarada na partilha de dados de saúde, pelo que devemos depositar confiança na ciência, que através da inovação e investigação, terão uma oportunidade de luxo para aceder a dados de saúde de elevada qualidade em grande escala, e poder, no final, retribuir com avanços na medicina e cuidados de saúde acessíveis, pois será o que todos esperamos como contrapartida.

Conclui-se pela não existência de uma tendência mercantilista no EEDS, pois a forma transparente como se apresenta e desenha, terá regulação e supervisão apertada por parte de entidades Europeias e dos Estados Membros, e a não ser que estes falhem, não ocorrerão erros apontados a outros sistemas de saúde, como o caso Norte Americano ou do Reino Unido. Por último, não podemos colocar na mesma balança os ganhos (lucros) da indústria com as melhorias no acesso e cuidados de saúde, pois são de essências diferentes, todavia, concluímos que mesmo que o fizéssemos, cada um com a medida das suas diferenças, haveria equilíbrio suficiente, devido aos valores imensuráveis inerentes à saúde e à vida humana.

Referências

Anam & Israrul Haque (2020). Big data analytics in health sector: Need, opportunities, challenges, and future prospects. In Big Data Analytics and Intelligence: A Perspective for Health Care. https://doi.org/10.1108/978-1-83909-099-820201006

Alonso, V., Santos, J. V., Pinto, M., Ferreira, J., Lema, I., Lopes, F., & Freitas, A. (2020). Health records as the basis of clinical coding: Is the quality adequate? A qualitative study of medical coders' perceptions. Health information management : journal of the Health Information Management Association of Australia, 49(1), 28–37. https://doi.org/10.1177/1833358319826351

Bahri, S., Zoghlami, N., Abed, M., Tavares, M. R. S., & Tavares, J. M. R. S. (2019). BIG DATA for Healthcare: A Survey. SPECIAL SECTION ON NEW TRENDS IN BRAIN SIGNAL PROCESSING AND ANALYSIS. IEEE Access. https://doi.org/10.1109/ACCESS.2018.2889180

Comissão Europeia. Estratégia Europeia para os Dados (2020). Acesso 02-01-2025, disponível em https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_pt

Comissão Europeia. Estratégia para União Europeia da Saúde. Acesso em 02-01-2025, disponível em https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-health-union_pt

Comissão Europeia. Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao Espaço Europeu de Dados de Saúde (2022). Acesso 02-01-2025, disponível em https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0010.02/DOC_1&format=PDF

Comissão Europeia. Comunicado de imprensa de 24 de abril de 2024. Acesso em 02-01-2025, disponível em https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_2250/IP_24_2250_EN.pdf

Comissão Europeia. Perguntas e respostas sobre o Espaço Europeu de Dados de Saúde. (2024). Acesso em 06-01-2025, disponível em https://ec.europa.eu/commission/presscorner/api/files/document/print/pt/qanda_24_2251/QANDA_24_2251_PT.pdf

Comissão Europeia. Factsheet on European Health Data Space. (2024). Acesso em 06-01-2025, disponível em https://ec.europa.eu/commission/presscorner/api/files/attachment/878485/Factsheet%20European%20Health%20Data%20Space_PT.pdf

Comissão Europeia. Consulta pública sobre a Iniciativa EEDS (2024). Acesso em 11-01-2025, disponível em https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12663-A-European-Health-Data-Space/public-consultation_pt

Costa, T. B. da. (2022). O altruísmo (económico?) de dados: breves considerações sobre o espaço europeu de dados de saúde e a proteção de dados pessoais. In Liber Amicorum Benedita Mac Crorie Volume II (pp. 613–643). UMinho Editora. https://doi.org/10.21814/uminho.ed.105.30

EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space p.3. Acesso a 06-01-2025, disponível em https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en

European Commission: Directorate-General for Health and Food Safety, *A minha saúde @ EU – Serviços de saúde eletrónicos transnacionais na UE (Portugal)*, Serviço das Publicações, 2020, **https://data.europa.eu/doi/10.2875/023738**

Fitzgerald M, Crider C. We need urgent answers about the massive NHS COVID data deal. Open democracy. 2020. Acesso a 06-01-2025. Disponível em https://www.opendemocracy.net/en/ournhs/we-need-urgent-answers-about-massive-nhs-covid-data-deal/

Gonçalves, Maria Eduarda. (2024) Ciberdireito. Liberades, Direitos e Regulação na Era Digital. Almedina

Ganna, A., Carracedo, A., Christiansen, C. F., Di Angelantonio, D., Dykstra, P. A., Dzhambov, A. M., Eils, R., Green, S., Schneider, K. L., Varga, T. V., Vuorinen, A.-L., Zuccolo, L., Hulvej, N., & Hoeyer, K. (2024). The European Health Data Space can be a boost for research beyond borders. *Nature Medicine*. https://doi.org/10.1038/s41591-024-03246-6

Haque, M. I. (2020). Big data analytics in health sector: Need, opportunities, challenges, and future prospects. *In* Big Data Analytics and Intelligence : A Perspective for Health Care (pp. 17-29) https://doi.org/10.1108/978-1-83909-099-820201006

Marelli, L., Stevens, M., Sharon, T., & Van Hoyweghen, I. (2023). The European health data space: Too big to succeed? Health Policy, 135(4), 104861. https://doi.org/10.1016/j.healthpol.2023.104861

Mittelstadt, B. (2017). From individual to group privacy in big data analytics. *Philosophy & Technology*. https://doi.org/10.1007/s13347-017-0253-7

Observador. Saúde inteligente: a era dos dados começou. Podcast GPS Episodio 3 – 20 nov.2024, 10:03. Acesso 08-01-2025. Disponível em https://observador.pt/programas/gps-gestao-pessoas-e-setores/saude-inteligente-a-era-dos-dados-comecou/

Parlamento Europeu. Resolução legislativa do Parlamento Europeu sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo ao Espaço Europeu de Dados de Saúde. Acesso em 02-01-2025, disponível em https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_PT.pdf

Recuero, M. (2024). Secondary Use of Electronic Health Data: The Future Regulation on the European Health Data Space and its Interplay with Data Protection Law. InDret, 2, 525–551. https://doi.org/10.31009/InDret.2024.i2.13

Richter, G., Trigui, N., Caliebe, A., & Krawczak, M. (2024). Attitude towards consent-free research use of personal medical data in the general German population. Heliyon. https://doi.org/10.1016/j.heliyon.2024.e27933

Rhodes,C. (2018) Solidarity in biomedicine and beyond, New Genetics and Society, 37:4, 439-444, DOI: 10.1080/14636778.2018.1451316

Stausberg, J., Harkener, S., & Bünz, S. (2024). A Collection of Data Quality Indicators for Health Research: Rationale for an Update. Studies in health technology and informatics, 321, 254–258. https://doi.org/10.3233/SHTI241103

Véliz, Carissa. (2022) Privacidade É Poder. Por Que Razão e como Devemos Recuperar o Controlo dos Nossos Dados

Zuboff, Shoshana. (2019) A Era do Capitalismo da Vigilância – A Disputa por Um Futuro Humano na Nova Fronteira do Poder. Relógio D´Água Editores.

Moldura Ética da Inteligência Artificial aplicada à Área da Saúde

Rita Maria Colaço Neves [185]

Resumo

A utilização da inteligência artificial no setor da saúde tem demonstrado um potencial significativo, mas também levanta desafios éticos e jurídicos substanciais. Por conseguinte, deve ser estabelecida uma moldura ética robusta para a aplicação responsável da IA na saúde e que permita mitigar os desafios que se colocam a este título, como a opacidade dos algoritmos, o enviesamento dos dados e a ausência de regulamentações específicas. Através da análise dos diplomas já existentes, como o AI Act da União Europeia e da exploração das implicações práticas da IA no contexto médico, propõem-se diretrizes éticas que promovem a transparência, a equidade e a proteção dos direitos humanos, contribuindo-se por esta via para uma correta e adequada implementação da IA na área da saúde, isto é, que simultaneamente permita a inovação tecnológica bem como a proteção dos direitos fundamentais dos indivíduos.

Palavras-chave: Inteligência artificial; Saúde; Moldura ética; Desafios.

[185] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Abstract

The use of artificial intelligence in the healthcare sector has shown significant potential, but it also raises substantial ethical and legal challenges. Therefore, a robust ethical framework must be established for the responsible application of AI in healthcare, one that mitigates the challenges involved, such as algorithmic opacity, data bias, and the lack of specific regulations. Through the analysis of existing regulations, such as the EU's AI Act, and the exploration of the practical implications of AI in the medical context, ethical guidelines are proposed to promote transparency, equity, and the protection of human rights. This contributes to the correct and adequate implementation of AI in healthcare, which simultaneously allows for technological innovation and the protection of individuals' fundamental rights.

Keywords: Artificial intelligence; Healthcare; Ethical framework; Challenges.

Introdução

A saúde configura um dos aspetos mais essenciais da existência humana, talvez o mais importante. A inteligência artificial (IA) tem vindo a transformar o setor da saúde, com avanços notáveis em sede de diagnósticos, tratamentos personalizados, gestão de recursos e em muitos mais campos relacionados com a prestação de cuidados de saúde. Todavia, a aplicação desta ferramenta no setor da saúde cria situações mais sensíveis, nomeadamente quando a IA é utilizada para a tomada de decisões que poderão afetar a saúde dos pacientes ou comprometer a efetividade de outros direitos. Nestes termos a utilização da IA na área da saúde também é fonte de diversas preocupações éticas que poderão colocar em causa o bem-estar físico e psicológico dos indivíduos, como a transparência dos algoritmos, o enviesamento dos dados ou a proteção dos direitos dos pacientes. Tais inquietações impõem a necessidade de uma moldura ética que permita o desenvolvimento e implementação responsável de sistemas de IA no setor da saúde.

Assim, o presente estudo procurará abordar a implementação e o uso dos sistemas de IA nos cuidados de saúde, colocando o foco nos valores e princípios éticos que devem ser respeitados na utilização desta tecnologia.

Embora os benefícios da IA sejam amplamente reconhecidos, há uma lacuna na abordagem sistemática das questões éticas e jurídicas associadas à sua aplicação prática. Regulamentações como o AI Act, ainda não enfrentam plenamente os desafios específicos do contexto médico. Este estudo propõe desenvolver o caminho para a criação de uma moldura ética da utilização da IA na área da saúde que possibilite a inovação tecnológica e os benefícios daí decorrentes, enquanto promove a proteção dos direitos fundamentais do ser humano, mormente daquele que procura cuidados de saúde.

Este estudo propõe-se, por conseguinte, a oferecer uma base sólida para debates éticos sobre a utilização da IA na saúde, apurando quais os principais princípios, desafios éticos, problemas práticos, normas jurídicas e orientações que se colocam neste contexto, com vista à construção de uma moldura ética compatível com o respeito pelos direitos dos indivíduos.

Para alcançar os objetivos estabelecidos, esta pesquisa adotará a técnica de pesquisa bibliográfica, desenvolvida através do método monográfico de procedimento. Empregar-se-á, para tanto, o método lógico-dedutivo, através de análises qualitativas, tendo como recursos a bibliografia nacional e a legislação vigente.

1. INTELIGÊNCIA ARTIFICIAL

1.1. CONCEITO

Pese embora seja muito complexo apurar o exato momento em que surgiu o termo "inteligência artificial", acredita-se que o mesmo tenha tido origem em 1956 nos Estados Unidos da América por conta do trabalho desenvolvido na área da computação, sobretudo o respeitante à possibilidade de programas e sistemas informáticos inteligentes copiarem os atributos do pensamento cognitivo humano (Nunes et. al. 2024), isto é, de realizarem um processo de tomada de decisão de forma semelhante a um ser humano, por intermédio da interpretação de dados externos com vista a aprender a partir deles e a utilizar os conhecimentos para alcançar tarefas e objetivos específicos (Comissão Europeia, 2018).

A verdade é que hodiernamente o conceito de inteligência artificial (IA) pode ser objeto de diferentes interpretações, atenta a evolução a que tem sido sujeita e que lhe conferiu um vasto âmbito de aplicação, englobando diversos tipos de sistemas. Enquanto disciplina científica, a IA inclui diversas abordagens e técnicas, tais como a aprendizagem automática, o raciocínio automático e a robótica. Assim, muitas das tecnologias que existem a título de IA são muito diferenciadas entre si, prosseguindo objetivos distintos. Atente-se, por exemplo, ao algoritmo que efetua a triagem de doentes num hospital ou aquele que propõe a um utilizador de uma plataforma de filmes ou de músicas os diferentes conteúdos de acordo com as suas preferências, apuradas a partir dos conteúdos já acedidos. Não obstante estarem em causa algoritmos bastante distintos, ambos são perspetivados enquanto sistemas de IA.

Não surpreende, por conseguinte, que a aplicação da IA a diferentes contextos e das mais variadas formas tem tornado difícil um consenso acerca da sua definição, sendo avançados diversos entendimentos a este respeito.

No contexto do presente estudo seguiremos de perto as definições de IA perfilhadas pelas instituições e órgãos que integram a União Europeia (UE), atendendo a que, nos termos do artigo 8.º n.º 4 da Constituição da República Portuguesa (CRP), as normas emanadas por tais instituições são aplicáveis à ordem jurídica interna portuguesa e, de acordo com o direito comunitário, este tem primazia sobre o direito nacional. Neste contexto atente-se à definição de AI constante do portal de internet do Parlamento Europeu[186], à definição proposta pelo Grupo de Peritos de Alto Nível sobre Inteligência Artificial da Comissão Europeia[187] ou à

[186] "A IA é a capacidade que uma máquina para reproduzir competências semelhantes às humanas como é o caso do raciocínio, a aprendizagem, o planeamento e a criatividade.", possibilitando que os sistemas pelos quais opera "(…) percebam o ambiente que os rodeia, lidem com o que percebem e resolvam problemas, agindo no sentido de alcançar um objetivo específico." Disponível em https://www.europarl.europa.eu/topics/pt/article/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona

[187] "(…)os sistemas de IA são sistemas de software (e eventualmente também de hardware)

definição inserida no artigo 3.º 1) do Regulamento de Inteligência Artificial da União Europeia[188].

De toda a forma, importa salientar que inexiste uma definição rigorosa da IA, o que constitui uma dificuldade acrescida à sua regulação, desde logo porque o conceito de IA delimita o âmbito de aplicação de qualquer legislação que produza neste contexto (Hacker, 2023).

1.2. IMPLICAÇÕES DA IA PARA A SOCIEDADE

Caracterizando-se por desempenhar de uma forma igual ou superior as tarefas que normalmente são executadas por humanos, o acelerado e constante desenvolvimento da IA tem motivado a sua presença nos mais diversos domínios da vida humana, conferindo inegáveis benefícios àqueles que a utilizam e alterando os comportamentos e as formas de atuação das pessoas e organizações que com ela estão envolvidas e, assim, moldando as sociedades contemporâneas através do impacto que têm na vida individual e coletiva. Por outro lado, cumpre ainda salientar que, à medida que a IA tem assumido um papel fundamental na vida das pessoas, as empresas que se têm servido da IA para vender os seus produtos e serviços têm alcançado lucros consideráveis, tendo a IA passado a ser perspetivada com um importantíssimo recurso económico e financeiro. Nestes termos, a IA apresenta-se hodiernamente com um fator de crescimento económico e de produtividade nas principais economias desenvolvidas do mundo. Veja-se, a este propósito, o considerando 4. do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024[189].

---

concebidos por seres humanos, que, tendo recebido um objetivo complexo, atuam na dimensão física ou digital percecionando o seu ambiente mediante a aquisição de dados, interpretando os dados estruturados ou não estruturados recolhidos, raciocinando sobre o conhecimento ou processando as informações resultantes desses dados e decidindo as melhores ações a adotar para atingir o objetivo estabelecido. Os sistemas de IA podem utilizar regras simbólicas ou aprender um modelo numérico, bem como adaptar o seu comportamento mediante uma análise do modo como o ambiente foi afetado pelas suas ações anteriores.". COMISSÃO EUROPEIA, 2018, Orientações Éticas para uma AI de confiança, p. 47. Disponível em https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

188 Um sistema de IA é "um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais".

189 "A IA é uma família de tecnologias em rápida evolução que contribui para um vasto conjunto de benefícios económicos, ambientais e sociais em todo o leque de indústrias e atividades sociais. Ao melhorar as previsões, otimizar as operações e a repartição de recursos e personalizar as soluções digitais disponibilizadas às pessoas e às organizações, a utilização da IA pode conferir importantes vantagens competitivas às empresas e contribuir para progressos sociais e ambientais, por exemplo, nos cuidados de saúde, na agricultura, na segurança alimentar, na educação e na formação, nos meios de comunicação social, no desporto, na cultura, na gestão das infraestruturas, na energia, nos transportes e na logística, nos serviços públicos, na segurança, na justiça, na eficiência energética e dos recursos, na monitorização ambiental, na preservação e recuperação da biodiversidade e dos ecossistemas e na atenuação das alterações climáticas e adaptação às mesmas."

Além da capacidade de ser utilizada em diversos domínios, a aplicação da IA à realidade humana pode ainda ser realizada de diferentes formas. Desde logo pela utilização de automatismos físicos ou virtuais na prossecução de tarefas repetitivas, mas também pela realização de ações mais complexas, nomeadamente através do "machine learning", um ramo da IA baseado na ideia de que as máquinas podem aprender sozinhas através da análise dos dados, identificar padrões e tomar decisões com uma reduzida intervenção humana (Saias et. al.;2018). O uso do *machine learning* traduz-se em diversas aplicações, como, por exemplo, em recomendações de produtos e serviços, em veículos autónomos, em deteção de fraudes ou em diagnósticos médicos. Apesar de muitos dos algoritmos de *machine learning* serem já conhecidos a algum tempo, nos últimos tempos verifica-se um novo impulso neste contexto, impulsionado pelos avanços na capacidade de processamento dos sistemas informáticos e, consequente, aplicação de cálculos matemáticos complexos a grandes volumes de dados (Big Data), o denominado *deep learning* (KARP, 2016), uma variante da *machine learning* que utiliza múltiplas camadas de redes neuronais e que tem vindo a revolucionar certas áreas da atividade humana, assumindo particular relevância no âmbito da medicina, ao possibilitar o processamento e análise de imagens e vídeos com vista à obtenção de um diagnóstico (Machado, 2019).

Em suma, será correto afirmar-se que a IA se encontra presente nos mais diversos setores da economia e da sociedade (Castro, 2016), ainda que nem sempre tal dimensão da IA seja totalmente percetível, atenta a forma quase invisível como muitas vezes opera[190]. Aspetos absolutamente centrais da vida humana, como a alimentação, a acessibilidade, a educação, a segurança, o entretenimento, os transportes ou a saúde, foram profundamente impactados pela IA, daí resultando um evidente acréscimo da qualidade de vida de cada um de nós.

2. UTILIZAÇÃO DA IA NA ÁREA DA SAÚDE

Como sucede em quase todos os domínios da atividade, também na saúde se prevê que a IA assuma um papel fundamental, possivelmente revolucionário. Segundo a Food and Drug Administration (FDA), os algoritmos de IA têm um enorme potencial na área da saúde (FDA, 2018), já que esta área se apresenta como muito favorável à aplicação de IA, atenta a transformação digital que neste setor se verifica[191] e que

[190] Circunstância que poderá explicar as conclusões vertidas no relatório da Boston Consulting Group, "Consumer Sentiment Survey 2023", nos termos do qual apenas 19% dos portugueses inquiridos admitiu já ter experimentado a tecnologia, mas não ter voltado a usar e 38% assegurou nunca ter usado ferramentas de inteligência artificial. Relatório citado em https://business-it.pt/2023/12/12/estudo-revela-que-23-dos-portugueses-utilizam-ferramentas-de-ia-semanalmente/#google_vignette.

[191] Veja-se, por exemplo, o desenvolvimento da conectividade móvel e a ampla adoção de dispositivos portáteis ofereceram aos clínicos e investigadores em saúde pública uma visão mais aprofundada sobre os dados fisiológicos dos indivíduos, facilitando a aplicação de medidas terapêuticas e preventivas mais eficazes.

possibilita inúmeras possibilidades de aplicações práticas da IA neste contexto (NOOR BAKHSH-SABET et. al.; 2019).

A IA na saúde divide-se em duas dimensões principais: a virtual e a física. A vertente virtual respeita ao uso de tecnologias informáticas, como o *deep learning*, para gerir informações e controlar sistemas de saúde, englobando registos de saúde eletrónicos e ferramentas que apoiam os médicos na tomada de decisões terapêuticas. Por outro lado, a vertente física da IA na saúde traduz-se na utilização de robôs capazes de prestar assistência a pacientes idosos ou apoiar médicos em procedimentos cirúrgicos.

No âmbito deste trabalho pretende-se destacar o papel que o *machine learning* tem desempenhado na prestação de cuidados de saúde à população, designadamente no âmbito dos processos de assistência e análises avançadas de big-data, quer no que respeita à realização de diagnósticos e prognósticos, na otimização de tratamentos e antecipação de resultados, no desenvolvimento de terapêuticas e na saúde pública, mas também no que concerne à redução de custos ou à diminuição de tempos de espera. Com a crescente disponibilização de dados na área da saúde e o avanço acelerado das técnicas de análise de big data, torna-se possível descobrir informações relevantes que não seriam facilmente identificadas pelos profissionais de saúde, contribuindo para uma tomada de decisões clínicas mais informada e de maior qualidade. Veja-se o caso do programa informático "OsteoDetect", um *software* de IA aprovado pela FDA em 2018 para auxiliar os profissionais de saúde na deteção de fraturas do punho, especificamente em imagens radiográficas e que utiliza algoritmos de *machine learning* para analisar radiografias e identificar características que indicam a presença de fraturas, possibilitando o diagnóstico de fraturas de uma forma mais rápida e precisa[192]. Outro exemplo a este título é o "IDx-DR", também aprovado pela FDA em 2018 e projetado para a deteção de retinopatia diabética, sendo um dos primeiros sistemas de IA aprovados que pode tomar decisões diagnósticas sem a necessidade de intervenção ou validação de um especialista em saúde ocular[193].

Não podem subsistir dúvidas, por conseguinte, quanto ao impacto positivo que os sistemas de IA estão já a ter nos cuidados de saúde da população em redor do mundo, esperando-se que num futuro breve possam assumir ainda uma maior relevância na prestação de cuidados de saúde, tornando-os melhores e mais eficientes, nomeadamente através de um diagnóstico mais rápido e preciso que é possibilitado em resultado de uma análise inteligente de milhões de registos clínicos que, ao identificarem padrões de doenças em estágios iniciais, aumentam as probabilidades de sucesso no tratamento.

[192] Citado em https://www.fda.gov/news-events/press-announcements/fda-permits-marketing-artificial-intelligence-algorithm-aiding-providers-detecting-wrist-fractures.
[193] Citado em https://www.healthvisors.com/en/idx-dr/.

3. ÉTICA E INTELIGÊNCIA ARTIFICIAL

Com o crescente protagonismo da IA na sociedade, ao promover melhorias na qualidade de vida das populações e a otimizar a eficiência e eficácia das instituições governamentais, através do aumento da sua capacidade de resposta às necessidades sociais, tem-se tornado mais evidente a conscientização sobre os riscos associados à sua implementação. Como referido no Livro Branco da IA do Conselho Nacional de Ética para as Ciências da Vida (CNECV) (Nunes et. al., 2024, p. 57), a IA apresenta: "*benefícios que protagoniza para as sociedades e os cidadãos são meritórios, devendo ser identificados e implementados. Impõe-se, concomitantemente, uma ponderação cuidada relativamente aos eventuais riscos subjacentes, procurando discernir, na miríade de possibilidades que a tecnologia oferece, os caminhos que melhor prossigam os valores e princípios éticos em que nos revemos.*"

A IA é uma tecnologia concebida por seres humanos para emular, aperfeiçoar ou até substituir a inteligência humana que frequentemente depende de vastos volumes de dados variados para gerar conclusões rigorosas. Projetos mal concebidos, baseados em dados defeituosos, inadequados ou enviesados, podem acarretar consequências não intencionais e, em muitos casos, prejudiciais para aqueles que deveriam obter benefícios com a sua utilização, levantando dúvidas concernentes à responsabilização pelas consequências das decisões baseadas em IA. Para além disso, o progresso acelerado dos sistemas algorítmicos levanta a questão de, em algumas situações, não ser claro o raciocínio que levou às conclusões vertidas por um sistema de IA, tornando-nos essencialmente dependentes de tecnologias cujas decisões não conseguimos explicar, o que tem impactos diretos na sociedade, como a perda de confiança na adoção de sistemas de IA. Depois, atendendo a que a utilização de IA envolve a análise de conjuntos de dados que contêm informações pessoalmente identificáveis, é extremamente importante garantir que tais dados não sejam distorcidos em função de raça, género ou etnia. Ao exposto acrescem ainda os problemas relacionados com a privacidade e o controlo do acesso à informação constante dos dados utilizados, bem como do dever de sigilo e da educação deontológica de todos os profissionais.

Consequentemente, revela-se fundamental assegurar a utilização ética e responsável da Inteligência Artificial, o que se alcança desde logo pela promoção de princípios que priorizem o respeito pelos direitos humanos, a participação ativa e a responsabilização pelas escolhas e decisões tomadas.

Os seres humanos devem, por conseguinte, ser colocados no centro da inovação tecnológica, para que o desenvolvimento e a implementação da IA respeitem os direitos fundamentais das pessoas, os quais, no entender de Jorge Miranda "*(…) podem ser entendidos prima facie como direitos inerentes à própria noção de pessoa, como direitos básicos de pessoa, como os direitos que constituem*

a base jurídica da vida humana no seu nível atual de dignidade" (Miranda, 2000, p.10).

Um quadro ético para a IA torna-se indispensável, pois identifica os riscos e os benefícios das ferramentas de IA, ao mesmo tempo que estabelece as normas para o seu uso responsável. A construção de um sistema de princípios morais e técnicas para a utilização responsável da IA exige que a indústria e as partes envolvidas ponderem questões sociais relevantes e, em última análise, reflitam sobre a essência da condição humana (Caldeira, 2021).

O termo "ética" resulta do grego "ethos", traduzindo os princípios morais pelos quais um indivíduo rege a sua conduta pessoal ou profissional[194]. Nestes termos, o *ethos* constituiu o ponto de partida para a criação de princípios que devem orientar a utilização da IA. A ética na IA corresponde, assim, a um conjunto de princípios morais e diretrizes, assentes em valores pessoais, princípios, contextos culturais, tradições e experiências de vida, que orientam o desenvolvimento e a implementação responsável desta tecnologia.

À medida que a IA se aplica cada vez mais a produtos e serviços, a ética tem assumido uma dimensão cada vez mais relevante e quer as empresas, por intermédio de códigos éticos, assim como organizações nacionais ou internacionais, através dos Livros Brancos, têm procurado estabelecer normas éticas específicos para a aplicação da IA, procurando responder a questões concretas com algumas propostas e/ou estratégias, contribuindo para a resolução de problemas emergentes colocados neste contexto.

Em suma, a utilização da IA não traz apenas benefícios e vantagens, acarretando igualmente grandes riscos e desafios que importa analisar e que impõem a criação de um quadro ético e legal robusto que discipline a aplicação da IA na área da saúde. Conforme exposto na Comunicação da Comissão Europeia de 25/04/2018, "*(…) algumas aplicações de IA podem suscitar novas questões éticas e jurídicas ligadas, por exemplo, à responsabilidade ou a decisões potencialmente tendenciosas. A UE deve, portanto, assegurar que a IA é desenvolvida e aplicada num quadro adequado, que favoreça a inovação e respeite os valores da União e os direitos fundamentais, bem como princípios éticos tais como a responsabilização e a transparência.*" (Comissão Europeia, 2018).

4. DESAFIOS ASSOCIADOS À UTILIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA SAÚDE

Como acima exposto, a implementação massiva de tecnologias de IA na área da saúde pode apresentar riscos consideráveis para os indivíduos, empresas e governos, colocando-se em evidência no âmbito do presente estudo os desafios éticos e legais, os quais se encontram intrinsecamente relacionados, pois enquanto a ética fornece princípios orientadores para o uso da IA, o direito promove a materialização de tais valores em normas vinculativas que regulam a utilização da IA. Nestes termos,

[194] Porto Editora – ética no Dicionário infopédia da Língua Portuguesa [em linha]. Porto: Porto Editora. Disponível em https://www.infopedia.pt/dicionarios/lingua-portuguesa/ética.

tanto os desafios éticos como os jurídicos associados ao uso da IA na área da saúde abordam questões fundamentais sobre a responsabilidade, os direitos e a proteção de indivíduos e da sociedade.

Os desafios éticos e jurídicos associados à IA são de natureza intrincada e multidisciplinar, constituindo um tema emergente e em constante evolução que ocupa uma posição central na agenda política europeia. Torna-se imperativo adotar um modelo holístico que considere as questões éticas desde as fases iniciais de conceção de qualquer solução tecnológica, abordando-as de forma repetida e contínua. Este modelo deve também assegurar um envolvimento abrangente de todas as partes interessadas, promovendo a inclusão, a equidade no acesso e uma aplicação mais justa e responsável da IA no domínio da saúde (Dantas et. al., 2024).

Muitas dúvidas e questões se colocam a este respeito: deverá o médico comunicar ao paciente que o diagnóstico foi elaborado com o auxílio de um sistema de apoio à decisão baseado em inteligência artificial? Como assegurar que as orientações clínicas geradas por essas ferramentas sejam fiáveis e livres de erros significativos? Quem deve ser responsabilizado em caso de erro ou prejuízo causado pela IA? Os desenvolvedores, os profissionais de saúde que utilizam a tecnologia ou as instituições de saúde que a implementam? Será o médico obrigado a seguir as sugestões da IA, tanto no diagnóstico como na escolha do tratamento? Em que circunstâncias o médico poderá divergir das recomendações da IA? Como assegurar a proteção dos dados de saúde e da privacidade dos utentes contra acessos indevidos ou utilizações impróprias, tendo em consideração a grande quantidade de dados que são disponibilizados, analisados e processados por sistemas de IA? Muitos são os desafios éticos que se colocam à utilização da IA na área da saúde, como os que constam do livro branco do CNECV para a IA.

Optou-se, no contexto do presente estudo, por destacar três desafios ético-jurídicos respeitantes à implementação da IA na área da saúde: a questão da opacidade, isto é, de falta de explicabilidade de algumas das decisões que são tomadas pelos sistemas de IA; o impacto do enviesamento desta tecnologia, em resultado da análise de dados distorcidos e a necessidade de normas claras e específicas que garantam a utilização ética da IA.

4.1. OPACIDADE DOS SISTEMAS

A questão da opacidade está relacionada com a falta de transparência de alguns dos critérios utilizados pelos sistemas de IA para, a partir da análise de um certo conjunto de dados, tomar determinadas decisões, o que por sua vez se traduz em falta de explicabilidade de tais decisões e que pode comprometer o uso da IA. Este problema é conhecido por efeito *black box* da IA (Kosinski, 2024) e que é agravado pelo surgimento dos sistemas de *deep learning*, os quais, em face do respetivo modo de funcionamento, são caracterizados por uma maior opacidade, sendo por vezes difícil, até mesmo para o programador do sistema, compreender e justificar os

processos de raciocínio que levaram à decisão tomada pela IA. Tal circunstância é especialmente preocupante na área da medicina, onde as decisões tomadas pelos sistemas de IA podem ter um impacto significativo na saúde e no bem-estar físico e psicológico dos pacientes. A ausência de explicabilidade nos sistemas de IA constitui um desafio para os próprios médicos, que podem encontrar dificuldades em interpretar, por exemplo, os diagnósticos produzidos pela máquina. Consequentemente, esses diagnósticos tornam-se igualmente difíceis de compreender para o cidadão comum, especialmente quando os critérios aplicados são desconhecidos pelos especialistas da área.

Assim, no contexto da prestação de cuidados de saúde, a falta de transparência das decisões tomadas pela IA assume especial relevância, por exemplo, no que respeita à exigência do consentimento informado, quer para a realização do ato médico, quer para a recolha de dados pessoais. Isto é, os pacientes devem estar plenamente informados quanto ao uso de IA no seu diagnóstico ou tratamento, a fim de aceitarem os termos de tal utilização. Por outro lado, a opacidade associada aos sistemas de IA poderá ainda levantar problemas relativamente à imputação dos danos causados com a sua utilização, importando perceber quem deve ser responsabilizado por tais prejuízos, se os programadores, os fornecedores de *hardware*, se o hospital ou o médico que realizou o diagnóstico ou aplicou determinada terapêutica (Vayena et. al., 2018).

Afigura-se imprescindível, por conseguinte, garantir que os processos utilizados e os resultados alcançados pelos sistemas de IA sejam explicáveis e compreensíveis.

Nestes termos não surpreende que no contexto da saúde a falta de transparência dos critérios decisórios e dos próprios erros compromete o desenvolvimento da IA a longo prazo, em face da falta de confiança que daí decorre, quer para os profissionais de saúde como para os próprios pacientes (Magrani e Silva, 2023). A opacidade está diretamente relacionada, portanto, com a confiança dos profissionais de saúde e dos doentes nos sistemas de AI, sendo essencial dispor de evidências sólidas e de uma validação rigorosa dos algoritmos de IA destinados a fins médicos, garantindo que possam gerar resultados confiáveis e aplicáveis na prática clínica. Para integrar a IA de forma eficaz na prestação de cuidados de saúde, é indispensável que sejam realizados estudos científicos detalhados, com resultados publicados em revistas submetidas a revisão por pares. Além disso, esses resultados devem ser posteriormente testados e confirmados no contexto do clínico real.

4.2. DISTORÇÃO DOS DADOS

Um dos desafios mais comuns quanto à aplicação da IA no âmbito da prestação de cuidados de saúde é o relacionado com o enviesamento dos dados utilizados para treinar os algoritmos, atendendo a que tais dados podem não estar completos, não ser representativos da população real ou incluir outras distorções relevantes devido aos parâmetros definidos para a recolha de dados[195], originando atrasos no

[195] Como os algoritmos refletem o sistema de valores e crenças dos seus criadores, a própria

tratamento ou decisões clínicas erradas, ao mesmo tempo que levantam problemas de discriminação, contribuindo para o incremento de preconceitos sistémicos.

Estudos realizados mostram que os sistemas de IA projetados para sugerir decisões, conhecidos como "recommender systems", embora sigam processos considerados objetivos, podem apresentar sérios problemas de tendenciosidade. Isso acontece porque, mesmo que o algoritmo em si seja neutro, os dados utilizados no seu treino muitas vezes incorporam e reproduzem preconceitos já presentes na sociedade (Vayena et. al, 2018).

Nestes termos, é provável que muitos dos conjuntos de dados utilizados para treinar um determinado algoritmo apresentem algum grau de tendenciosidade, especialmente em relação a características como idade, género, raça ou condições económicas e sociais. Tal distorção pode ter origem em vários motivos, incluindo pela própria circunstância dos registos médicos utilizados terem sido gerados apenas para efeitos da realização de determinado tratamento ou para finalidades de faturação. Atente-se, por exemplo, à situação em que os dados utilizados para treinar algoritmos de deteção de cancro de pele respeitam a predominantemente a pessoas de cor branca, o que pode motivar piores resultados no tratamento de cancro de pele nas pessoas negras (Kleinberg et al., 2018). Ou à circunstância da maior parte dos dados sobre cancro respeitar a doentes com mais de 60 anos de idade quando, nos últimos anos, assiste-se a uma tendência de crescente número de cancros em doentes mais jovens, o que pode diminuir a eficiência da terapêutica aplicada. Verifique-se ainda o caso em que o algoritmo utiliza os custos de saúde como modelo para as necessidades de saúde. Autores (Obermeyer et al., 2019) encontraram evidências de distorção racial num algoritmo utilizado na prestação de cuidados de saúde, motivando que pacientes negros classificados pelo algoritmo com o mesmo nível de risco do que pacientes brancos estejam, na verdade, mais doentes. Ao serem considerados os custos gastos com saúde como referência para as necessidades de prestação de cuidados de saúde, constatou-se que, como se gasta menos dinheiro com pacientes negros que apresentam o mesmo nível de necessidade, o algoritmo conclui erroneamente que estes são mais saudáveis do que pacientes brancos igualmente doentes, comprometendo o tratamento daqueles.

Em suma, a problemática respeitante ao enviesamento dos dados empregues nos sistemas de IA é deveras complexa, levantando dúvidas quanto à exatidão e eficiência das ferramentas de IA, ao mesmo tempo que coloca questões éticas e jurídicas quer ao nível da discriminação e do preconceito como no plano da responsabilidade pelos danos causados em resultado da utilização de dados distorcidos.

---

seleção dos dados de treino pode refletir os enviesamentos dos programadores, o que pode criar uma discriminação sistemática por parte do sistema. Vide Lévy, Pierre (2022). Inteligência Artificial produz "monstruosidades éticas". Revista Fórum. Disponível em https://revistaforum.com.br/ciencia-e-tecnologia/2022/12/27/inteligncia-artificial-produz-monstruosidades-eticas-diz-pierre-levy-129333.html

4.3. NECESSIDADE DE MAIOR REGULAMENTAÇÃO ÉTICO- JURÍDICA

Para se lidar com os desafios acima mencionados, assim como outros, resulta fundamentalmente a existência de legislações e regulamentações sólidas que traduzam, de forma objetiva e precisa, os princípios éticos orientadores do desenvolvimento, da avaliação clínica e da aplicação das tecnologias de IA no setor da saúde.

Urge, por conseguinte, promover-se a criação de uma moldura ética robusta que garanta a segurança, a ética e a transparência no uso da IA e que, ao mesmo tempo, fomenta e promove a inovação. Como já abordado neste estudo, a **moldura ética da IA aplicada à área da saúde** traduz-se no conjunto de princípios, diretrizes e práticas que orientam o desenvolvimento, a implementação e o uso responsável das tecnologias de IA em contextos relacionados com a prestação de cuidados de saúde.

Como se verá mais à frente neste estudo, são vários e diversos os princípios e valores constantes de instrumentos quer de direito internacional, como de direito nacional, que estabelecem as diretrizes éticas do desenvolvimento e implementação da IA. Contudo, dois grandes problemas se colocam a este título. Por um lado, os princípios e valores são normalmente dotados de um amplo grau de abstração e, consequentemente, carecem de ser concretizados, a fim de se poderem aplicar a situações concretas. Por outro lado, a maior parte dos diplomas atrás referidos, que proclamam os princípios e valores éticos a observar relativamente à utilização da IA, não possuem força vinculativa, isto é, não obrigam os EM a estabelecer disposições jurídicas que concretizem tais princípios e valores. Por conseguinte, a criação de tal moldura ética para a utilização responsável da IA na área da saúde está subordinada à aprovação e vigência de normas jurídicas que concretizem os princípios e valores proclamados a este respeito. Um exemplo pragmático do exposto é o facto de ainda inexistir um regime de responsabilização para os danos provocados pela utilização de sistemas de IA.

Nestes termos, se da análise dos princípios e valores que se propõem a construir uma moldura ética relativa à utilização da IA na área da saúde resulta a conclusão que a maior parte deles não apresenta força vinculativa e, dada a sua inerente abstração e carácter genérico, revestem dificuldades de aplicação às situações concretas, a verdade é que do exame das normas jurídicas (com força de lei) relativas ao uso de IA decorre a conclusão de que as normas existentes se revelam como pouco claras e precisas para se aplicarem a situações específicas e, assim, garantirem uma utilização ética da IA na área da saúde (Elias et. al., 2023).

As duas conclusões acima referidas refletem uma realidade que gera preocupação em diversos níveis e que, entre outros motivos, encontra justificação no rápido desenvolvimento e a implementação de sistemas de IA na área da saúde, muitas vezes ultrapassando a capacidade das estruturas regulatórias de

acompanhar esse progresso. Também a diversidade dos sistemas de IA aplicados à saúde, seja para efeitos de diagnóstico, de tratamentos personalizados, de gestão de dados de pacientes ou de pesquisa científica, compromete a ausência de um quadro regulatório forte, dado que cada uma das aplicações de IA atrás referidas apresenta desafios únicos que requerem abordagens regulatórias diferenciadas (Melo et. al). Este cenário cria um vazio normativo que pode comprometer a segurança, a eficácia e a equidade na aplicação dessas tecnologias, por intermédio da ocorrência de violações de privacidade, discriminação algorítmica e desigualdades no acesso a tratamentos de saúde, ao mesmo tempo que motiva desconfiança por parte dos profissionais de saúde e do público. De todo o modo e a fim de se fundamentar conveniente a conclusão acima expressa, cumpre aferir e analisar quais as normas legais atualmente aplicáveis à medicina assistida por IA.

5. O ATUAL QUADRO ÉTICO-NORMATIVO DA INTELIGÊNCIA ARTIFICAL

5.1. CONTEXTO INTERNACIONAL

A utilização da IA, particularmente no âmbito da saúde, dispõe hodiernamente de alguns mecanismos de regulação ético-normativa a nível internacional, mormente no âmbito europeu, pese embora nem todos possuam a mesma força vinculativa.

De entre aqueles que não apresentam vinculação obrigatória para os Estados, cumpre destacar dois instrumentos de alcance mundial, a Recomendação da UNESCO sobre a ética da IA[196] e o Guia da Organização Mundial de Saúde sobre Ética e Governação da IA para a Saúde[197], os quais, não obstante não se imporem de forma obrigatória aos seus destinatários, constituem uma importante fonte dos valores éticos a observar no âmbito da aplicação da IA. Ainda no que concerne aos instrumentos de regulação de IA não vinculativos, mas de alcance comunitário, cumpre destacar o já aqui abordado Guia de Orientações Éticas para uma IA de Confiança do Grupo de Peritos de Alto Nível sobre a IA.

Já no que respeita a instrumentos de regulação ético-normativa vinculativa, abordar-se-á o Regulamento da Inteligência Artificial da União Europeia (AI Act)[198], o qual, tendo entrado em vigor em 01 de agosto de 2024, será diretamente aplicável na ordem jurídica dos Estados Membros (EM) que integram a UE a 2 de agosto de 2026, configurando o pilar da regulamentação de IA para todos os EM.

---

[196] UNESCO, Recomendação sobre a Ética da IA, 2021, Disponível em https://unesdoc.unesco.org/ark:/48223/pf0000381137_por

[197] World Health Organization, Ethics and governance of artificial intelligence for health: WHO guidance, 2021. Disponível em https://iris.who.int/bitstream/handle/10665/341996/9789240029200-eng.pdf?sequence=1

[198] Regulamento (UE) 2024/1689 DO Parlamento Europeu e do Conselho, de 13 de junho de 2024, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L_202401689.

5.1.1. RECOMENDAÇÃO DA UNESCO SOBRE A ÉTICA DA IA

A Recomendação da UNESCO sobre a Ética da IA, adotada em novembro de 2021, é um marco internacional no campo da regulamentação da IA. Este documento, ao reconhecer que os sistemas de IA levantam novos problemas éticos nos mais variados campos da vida humana, incluindo na saúde, procura estabelecer princípios e valores éticos para orientar o desenvolvimento e a aplicação de tecnologias de IA, com o objetivo de assegurar que sejam utilizadas de forma responsável e em benefício da humanidade.

Nestes termos, a Recomendação em análise fornece quatro valores e dez princípios fundamentais para a aplicação da IA.

No que concerne aos valores a observar pelos Estados-Membros na implementação e desenvolvimento das tecnologias de IA, são eles: (*i*) respeito, proteção e promoção dos direitos humanos e liberdades fundamentais e dignidade humana; (*ii*) promoção do ambiente e dos ecossistemas; (*iii*) garantia de diversidade e inclusão e (*iv*) viver em sociedades pacíficas, justas e interligadas.

Já quanto aos princípios a cumprir a este título, são proclamados os seguintes: (*i*) proporcionalidade e não causar dano; (*ii*) segurança e proteção; (*iii*) justiça (equidade) e não-discriminação; (*iv*) sustentabilidade; (*v*) direito à privacidade e proteção de dados; (*vi*) supervisão humana; (*vii*) transparência e explicabilidade; (*viii*) responsabilidade e responsabilização; (*ix*) consciência e literacia e (x) respeito pelo direito internacional e as soberanias nacionais com abordagem participativa e multilateral.

5.1.2. GUIA DA ORGANIZAÇÃO MUNDIAL DA SAÚDE SOBRE ÉTICA E GOVERNAÇÃO DA IA PARA A SAÚDE

No que respeita em específico ao tema do presente estudo, cumpre destacar o Guia da Organização Mundial de Saúde sobre Ética e Governação da IA para a Saúde, que constitui um marco incontornável na orientação do uso responsável e ético da inteligência artificial (IA) no setor da saúde. Publicado em 2021, este guia visa estabelecer princípios e boas práticas para o desenvolvimento, implementação e uso da IA na saúde, garantindo que essas tecnologias melhorem os sistemas de saúde de forma justa e sustentável. Este enfatiza a necessidade de proteger os direitos humanos, promover a equidade e garantir a segurança no uso dessas ferramentas, colocando o foco na proteção dos direitos humanos, na promoção da equidade e na garantia da segurança no uso dessas ferramentas.

Neste contexto o guia em apreço propõe princípios éticos que devem presidir ao desenvolvimento e à aplicação das tecnologias baseadas em IA na saúde: (*i*) o princípio da autonomia exige que a utilização de sistemas ou tecnologias de IA não comprometa nem reduza a capacidade de decisão humana. A supervisão humana deve ser constante, garantindo que as decisões possam ser ajustadas quando necessário, bem como assegurando que o consentimento informado seja

plenamente respeitado. De seguida, (*ii*) de acordo com o princípio da não-maleficência, é imprescindível garantir que as tecnologias de IA sejam seguras, precisas e eficazes antes de serem introduzidas no mercado; (*iii*) o princípio da transparência implica a disponibilização e documentação de informações suficientes durante o desenvolvimento das tecnologias de IA, bem como após a sua aprovação e implementação. Estas tecnologias devem ser capazes de fornecer explicações compreensíveis aos diferentes públicos. Posteriormente, (*iv*) o princípio da responsabilidade deve ser garantido através da supervisão humana constante. Esta supervisão inclui a avaliação, tanto por profissionais de saúde como por pacientes, do desempenho das tecnologias de IA. Nos casos em que decisões tomadas por IA resultem em danos, é essencial identificar claramente a responsabilidade de cada parte envolvida, incluindo fabricantes e utilizadores clínicos. Adiante, (*v*) o princípio da inclusão implica que as tecnologias de IA utilizadas nos cuidados de saúde sejam concebidas para garantir o acesso equitativo e apropriado a todos os indivíduos, independentemente de fatores como idade, género, rendimento ou capacidade. É crucial evitar a utilização de dados enviesados, assegurando uma representatividade abrangente. Por último, (*vi*) a introdução de tecnologias de IA nos sistemas de saúde deve estar condicionada à sua plena integração e capacidade de sustentação. É necessário identificar as reais necessidades do contexto em que serão utilizadas e garantir que se adequam aos requisitos locais.

5.1.3. GUIA DE ORIENTAÇÕES ÉTICAS PARA UMA IA DE CONFIANÇA

Para enfrentar os desafios expostos no capítulo anterior, assim como outros, a Comissão Europeia criou, em 2018, o Grupo Independente de Peritos de Alto Nível em IA, para estabelecer requisitos gerais para uma IA confiável na Europa. Este Grupo publicou um guia que fornece orientações e perguntas para incentivar o desenvolvimento da IA no sentido de uma maior fiabilidade. Este guia constitui um documento de referência para assegurar que os sistemas de IA sejam desenvolvidos e implementados de forma ética, confiável e alinhada com os valores europeus. Publicado em 2019, este guia identifica princípios, requisitos e medidas operacionais para promover uma IA que respeite os direitos fundamentais, a dignidade humana e o bem-estar social e posiciona a UE como líder na promoção de uma IA ética e confiável, servindo como modelo para regulamentação e práticas de IA, inspirando governos, organizações e empresas a adotar abordagens responsáveis no desenvolvimento de tecnologias baseadas em IA.

Com base no princípio de que a IA deve ser legal, ética e robusta, este Guia define sete critérios essenciais que a IA deve atender, para ser de confiança: (*i*) os sistemas de IA devem permitir a tomada de decisões informadas e devem estar sujeitos à supervisão humana, por intermédio de mecanismos de governação de intervenção humana; (*ii*) os sistemas de IA devem ser resilientes e seguros, precisos,

fiáveis e reprodutivos, dado ser a única forma de garantir que quaisquer danos acidentais possam ser minimizados e prevenidos; (*iii*) deve ser assegurado o respeito pela privacidade e pela proteção de dados pessoais, assim como devem existir mecanismos de gestão que considerem a qualidade e a integridade desses dados; (*iv*) os dados, o sistema e os modelos de negócio da IA devem ser transparentes e explicáveis. É essencial que as pessoas sejam informadas de que estão a interagir com um sistema de IA e tenham conhecimento tanto das suas capacidades como das suas limitações; (*v*) devem ser evitadas distorções injustificadas, uma vez que podem originar diversas consequências negativas, incluindo a exclusão de grupos vulneráveis e o agravamento de preconceitos e práticas discriminatórias; (*vi*) é necessário garantir que os sistemas de IA sejam sustentáveis e respeitadores do ambiente; (*vii*) é fundamental estabelecer mecanismos que assegurem tanto a atribuição de responsabilidade quanto a responsabilização pelos sistemas de IA e pelos seus resultados.

5.1.4. O REGULAMENTO IA DA UNIÃO EUROPEIA (AI ACT)

Apresentando-se como o principal instrumento normativo no âmbito da União Europeia, o AI ACT constituiu o primeiro esforço legislativo abrangente a nível mundial para regular a inteligência artificial. Conforme decorre do seu artigo 1.º, o Regulamento em apreço propõe-se a alcançar duas grandes finalidades: controlar os riscos associados à IA e aumentar a confiança na IA. Isto é, ao mesmo tempo que pretende garantir o desenvolvimento e a inovação da IA na Europa, igualmente pretende defender os direitos dos cidadãos.

Nestes termos, será correto afirmar-se que por intermédio do AI ACT a UE procurou criar um quadro jurídico harmonizado para regular o desenvolvimento, a comercialização e a utilização éticas, seguras e transparentes de sistemas de IA em todos os Estados-Membros da UE (Nunes et. al., 2024).

Para os efeitos acima referidos e de acordo com o n.º 2 do artigo 1.º do Regulamento, o AI Act estabelece regras harmonizadas para a colocação no mercado e em serviço de sistemas de IA, proibições de certa IA (quando os sistemas de IA colidem com princípios éticos universais ou com direitos humanos fundamentais), regras de transparência harmonizadas para interação e, ainda, regras de monitorização do mercado e vigilância.

A abordagem prosseguida pelo AI ACT, alcançar os objetivos propostos é alicerçada na análise de risco, segundo a qual os sistemas de IA se encontram sujeitos a diferentes obrigações, consoante o risco que a sua utilização representa. Neste contexto, são identificados três grupos de sistemas de IA.

Em primeiro lugar estão os sistemas de AI cuja utilização é proibida e que, como tal, não podem ser comercializados (artigo 5º). Coloca-se em evidência, no âmbito do presente estudo, os sistemas que manipulem o utilizador, através de técnicas subliminares (artigo 5.º n.º 1 al. a)), distorcendo a sua capacidade de tomar uma decisão informada. No âmbito do uso dos sistemas de IA, que realizem

diagnósticos médicos, resulta crucial estabelecer um equilíbrio entre fornecer um resultado útil e informativo tanto para o utilizador como para o próprio médico, sem que esse resultado seja enviesado ou influencie indevidamente as decisões dos profissionais. A proibição de sistemas que manipulem a capacidade do utilizador de tomar uma decisão fundamentada será particularmente relevante neste domínio, para assegurar a validade do consentimento informado, garantindo que o paciente preserve a sua autonomia para tomar decisões conscientes e livres acerca de qualquer tratamento que lhe seja sugerido pelo sistema de IA. Mais se destaca a proibição de sistemas de categorização biométrica, que classifiquem os indivíduos com base em dados pessoais como a raça, crenças religiosas ou vida sexual (artigo 5.º, nº 1, al. g)), uma vez que a recolha de dados de saúde pode levar a inferências feitas pelos sistemas de IA sobre informações pessoais, para as quais os pacientes não concederam o seu consentimento.

Posteriormente, encontram-se os sistemas de alto risco (artigo 6.º), em que os produtores e fornecedores destes sistemas se encontram sujeitos a uma maior exigência, sendo estipuladas obrigações agravadas, atendendo ao perigo que representam para os seus utilizadores. Entre tais deveres adicionais encontram-se o estabelecimento de um sistema de gestão de riscos (artigo 9º), a implementação de um mecanismo de gestão de dados (artigo 10º), a manutenção de documentação técnica (artigo 11º) e registos (artigo 12º), assim como a exigência de transparência, fornecimento de informações (artigo 13º) e supervisão humana (artigo 14º), além da necessidade de garantir a precisão, robustez e segurança cibernética do sistema (artigo 15º). Os sistemas de IA utilizados no setor da saúde são, na sua maioria, considerados como sistemas de alto risco (artigo 6º n.ºs 2 e 3) e, como tal, a utilização de um sistema de IA no setor da saúde estará sujeita a obrigações mais exigentes, como seria expectável, dada a natureza sensível dos dados, e da situação mais vulnerável em que, por regra, os utilizadores se encontram.

Finalmente, estão os sistemas sujeitos a obrigações adicionais de transparência (artigo 50º), exigindo-se, em certos casos, a informação ao utilizador de que o mesmo se encontra a interagir com um sistema de IA, conforme determinado no seu n.º 1.

Em síntese, o AI Act representa um passo importante para o estabelecimento de um ecossistema digital ético e juridicamente responsável na EU, podendo servir de modelo para regulamentações futuras em outras jurisdições globais (NUNES et. al., 2024). Não obstante, cumpre afirmar que o Regulamento não considera a totalidade das questões éticas decorrentes da aplicação da IA ao setor da saúde, como a privacidade dos dados de saúde, o consentimento informado, a distorção dos dados utilizados em diagnósticos, a responsabilidade em casos de erro médico ou a explicabilidade dos algoritmos utilizados em certos sistemas de IA. Importa, por conseguinte, que estas questões éticas e jurídicas obtenham uma regulação mais clara e específica.

5.2. CONTEXTO NACIONAL

5.2.1. CARTA PORTUGUESA DE DIREITOS HUMANOS NA ERA DIGITAL

De entre os instrumentos nacionais, um dos que assume maior relevo neste contexto é a Carta Portuguesa de Direitos Humanos na Era Digital, aprovada pela Lei n.º 27/2021, de 17 de maio[199].

Esta Carta, adotada em 2020, é um documento que estabelece princípios fundamentais para a proteção dos direitos humanos no contexto da digitalização e das tecnologias emergentes, incluindo a IA. A sua relação com a regulação da IA é percetível, pois ambos procuram garantir a utilização responsável e ética dessas tecnologias, assegurando a proteção dos direitos individuais e coletivos.

O artigo 9.º desta Lei, sob a epígrafe "Uso da inteligência artificial e de robôs", é categórico ao determinar que a utilização da IA deve ser centrada no respeito pelos direitos fundamentais, como forma de se assegurar o cumprimento de alguns dos princípios éticos já apontados neste estudo, como a explicabilidade, autonomia, consentimento informado, transparência, segurança e responsabilidade e a negação da discriminação e do preconceito.

Porém e à semelhança dos restantes diplomas já aqui abordados, a exposição dos critérios a serem tidos em consideração para a utilização de sistemas de IA é efetuada de forma vaga e genérica, não sendo determinado, de uma forma clara e precisa, como os princípios éticos em causa deverão ser concretizados em situações concretas. Isto é, não obstante esta Lei estabelecer o esboço dos princípios e dos valores éticos a serem prosseguidos com o uso da IA, não oferece os procedimentos que na prática deverão ser observados para garantia de tais princípios e valores.

5.2.2. REGIME JURÍDICO DA SEGURANÇA DO CIBERESPAÇO

O Regime Jurídico da Segurança do Ciberespaço, aprovado pelo DL n.º 65/2021, de 30 de julho, tem como objetivo regulamentar a segurança das redes e sistemas de informação, assegurando a proteção contra riscos cibernéticos e promovendo um ambiente digital confiável e resiliente.

Este diploma legal relaciona-se com a IA na medida em que os sistemas de IA estão profundamente integrados no ciberespaço e dependem de infraestruturas digitais seguras para funcionar de forma eficaz e ética. Ou seja, o regime jurídico em apreço procura estabelecer a segurança das redes e dos sistemas de informação que sustentam o uso de tecnologias como a IA, para que o seu desenvolvimento e utilização decorra num ambiente de confiança e protegido de ameaças.

[199] Disponível em https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3446A0001&nid=3446&tabela=lei_velhas&pagina=1&ficha=1&so_miolo=&nversao=1

6. PROPOSTAS PARA UMA UTILIZAÇÃO ÉTICAMENTE RESPONSÁVEL DA IA NA ÁREA DA SAÚDE

As ferramentas de IA não apenas contribuem para melhorar os resultados clínicos, mas também operam dentro de um conjunto de princípios éticos e legais. Em face do exposto até ao momento, será correto desde já se afirmar que, para se assegurar uma efetiva utilização ética dos sistemas de IA na saúde, é fundamental adaptar os princípios e valores éticos já existentes no domínio da IA à realidade da área da saúde, garantindo-se por esta via que o seu uso esteja alinhado com a diversidade das necessidades e contextos que se verificam na saúde. Da análise dos instrumentos legais acima referidos, nomeadamente do IA Act e da Lei n.º 27/2021, de 17 de maio, decorre a conclusão de que pese embora as orientações éticas neles contidas constituam um recurso importante para a criação de uma moldura ética relativa à utilização da IA, a verdade é que, na sua maioria, os princípios e valores por eles enunciados são genéricos a todos os domínios da I.A e da sociedade, sendo evidente que a sua concretização na área da prestação de cuidados de saúde reclama um enquadramento e soluções adaptadas. Acresce ainda, neste âmbito, a exigência de uma regulamentação jurídica devidamente adaptada à realidade do setor da saúde que concretize os princípios e valores éticos existentes: documentos como o Guia da Organização Mundial de Saúde sobre Ética e Governação da IA para a Saúde carecem que os princípios éticos aí proclamados sejam objeto de uma regulamentação jurídica que abranja situações claras e específicas. Em suma, é absolutamente fundamental a existência de legislação nacional e internacional em conformidade com a realidade do setor da saúde e que seja atualizada a um ritmo mais rápido, para que questões ético-jurídicas, como a responsabilidade decorrente de danos causados pela utilização de sistemas de AI, obtenham uma solução adequada.

Em segundo lugar e apesar de ser prudente a adoção de sistemas de IA que levantem menos questões éticas, não parece viável a ideia de restringir a utilização de IA a tarefas que requeiram menos conhecimento profissional e experiência, no sentido de evitar problemas éticos (como a IA ser apenas usada para situações, por exemplo, de transporte de comida e medicamentos dentro dos hospitais (Lima e Paiva, 2023), já que a constatação dos amplos benefícios que a IA pode introduzir na prestação de cuidados de saúde aponta noutro sentido. A adoção de sistema de IA na área da saúde exigirá sempre uma avaliação cuidada dos riscos associados em confronto com as vantagens que pode oferecer, como, aliás, já resulta do artigo 28.º do AI Act, o qual estabelece a exigência de um relatório de avaliação dos riscos que o sistema pode apresentar para os direitos humanos. A avaliação destes riscos é particularmente importante, no setor da saúde, dada a potencial ameaça para a integridade física e psicológica dos utentes (Fernandes e Goldim, 2023). Se se concluir por uma excessiva gravidade dos riscos associados, será dificilmente justificável a

utilização destes sistemas num setor que impacta aspetos sensíveis da vida das pessoas. Neste contexto, um dos aspetos que tem registado maior progresso na regulação ética da IA é a implementação das chamadas "regulatory sandboxes", ou "modelos de regulação em ambiente controlado". Esta abordagem permite identificar potenciais riscos durante a fase de desenvolvimento, mesmo com requisitos mínimos, proporcionando uma forma flexível de lidar com os desafios que surgem ao longo do processo. A UE tem vindo a adotar este modelo, que se caracteriza por ser uma forma avançada de regulação responsiva, onde reguladores e entidades reguladas colaboram ativamente para alcançar um objetivo específico e previamente definido (Nunes, 2021).

Em terceiro lugar, é fundamental que as preocupações éticas com a utilização da IA sejam tidas em consideração logo a partir do momento do desenvolvimento destes sistemas, sendo privilegiados os sistemas que desde a sua conceção traduzam as preocupações éticas levantadas neste estudo, entre outras. A título exemplificativo, deverão apenas ser desenvolvidos e implementados sistemas de IA na área da saúde que não sejam caracterizados pela opacidade, em que se desconhece o processo que conduz a uma determinada decisão, a fim de se garantir um maior grau de transparência e explicabilidade dos sistemas. Resulta absolutamente imprescindível que quer os pacientes como os profissionais de saúde tenham confiança nos sistemas de IA e isso apenas sucederá se estes forem explicáveis e transparentes. Para promover a confiança entre os profissionais de saúde, uma possível abordagem é disponibilizar documentação que explique o desempenho, o uso e a forma como dado sistema de IA foi integrada em práticas de cuidados noutras organizações de saúde. Apesar de não ser necessário que os profissionais entendam os detalhes técnicos mais complexos, é essencial que compreendam como os modelos chegaram a previsões específicas. Uma das soluções a adotar neste âmbito será a inclusão de profissionais médicos no desenvolvimento dos sistemas de IA. A cooperação entre várias áreas da ciência possibilita, por um lado, que os sistemas de IA sejam compreensíveis para os profissionais de saúde e, por outro lado, facilita a perceção das ramificações éticas de dado sistema de IA para os seus produtores e programadores (Vayena et. al, 2018). Resulta igualmente fundamental a este título que os programadores, os profissionais de saúde e os pacientes disponham de formação adequada para identificar e atenuar potenciais problemas éticos, como o enviesamento dos dados. Uma devida formação ética dos programadores de ferramentas de IA na área da saúde fará com que estes tenham uma maior consciencialização e incorporação das preocupações éticas desde o *design* e conceção dos sistemas AI. Tal exigência fará com que as empresas desenvolvam sistemas de IA, colocando a ética dos mesmos como uma prioridade. (Gonçalves-Sá e Pinheiro, 2023). Por outro lado, deve ser dada preferência a sistemas de IA cujos produtores tenham implementado um código de conduta. Este mecanismo de autorregulação, orientado para a definição de padrões éticos pela própria organização, garante que os sistemas são concebidos em conformidade com os princípios éticos de elevado rigor. Um

exemplo paradigmático é a "Parceria em IA para Beneficiar as Pessoas e a Sociedade", criada inicialmente pelas grandes empresas tecnológicas (Microsoft, Google, Amazon, Facebook, IBM) com o objetivo de estabelecer melhores práticas alinhadas com os princípios éticos.

Por fim, cumpre salientar que a criação de uma adequada moldura ética para a utilização da IA na área da saúde estará sempre subordinada ao cumprimento de um imperativo fundamental: a IA deverá ter em consideração o ser humano e o respeito pelos seus direitos fundamentais, como critério mais importante que preside ao seu desenvolvimento e aplicação.

CONSIDERAÇÕES FINAIS

A crescente aplicação da inteligência artificial na área da saúde traz consigo uma série de oportunidades e benefícios para o ser humano, assim como desafios éticos e jurídicos que não podem ser ignorados. Embora a IA tenha o potencial de melhorar significativamente os cuidados de saúde, a sua implementação exige uma atenção cuidadosa aos princípios éticos fundamentais, como a transparência, a explicabilidade, a responsabilização e a proteção dos direitos dos indivíduos. A opacidade das decisões algorítmicas, o enviesamento dos dados e a falta de regulação clara e específica relativamente ao uso da IA no setor da saúde são questões críticas que necessitam de soluções claras e adaptadas à realidade deste domínio sensível.

A opacidade dos sistemas de IA, isto é, a tomada de decisões sem uma explicação clara sobre o processo que conduziu a essas conclusões, mina a confiança dos profissionais de saúde e dos pacientes, tornando a responsabilização de eventuais erros mais complexa. Daí a necessidade de princípios éticos que possibilitem o desenvolvimento de sistemas de AI transparentes e explicáveis.

Além disso, quando os sistemas de IA são "alimentados" por dados enviesados, esses sistemas correm o risco de perpetuar desigualdades existentes no acesso e na qualidade dos cuidados de saúde, afetando particularmente grupos vulneráveis. Nestes termos, uma moldura ética deve promover a equidade no acesso aos cuidados, assegurando que os dados utilizados na formação da IA sejam representativos e livres de viés discriminatório.

Por fim, a ausência de regulamentações específicas e adaptadas ao contexto da saúde para a utilização da IA agrava os riscos éticos e jurídicos envolvidos. Embora regulamentações como o AI Act da União Europeia representem um passo importante para o desenvolvimento da IA em diversos setores, a sua aplicabilidade no campo da saúde reveste uma natureza genérica e abstrata. A criação de normas claras, que integrem as preocupações éticas e jurídicas, é

fundamental para garantir uma utilização responsável da IA, respeitando os direitos humanos e promovendo a segurança dos pacientes.

A criação de uma moldura ética robusta para a utilização da IA na saúde é imprescindível, e isso passa pela adaptação dos princípios gerais de ética da IA às necessidades e particularidades do setor. Por sua vez, a disciplina jurídica relativa à aplicação da IA à área da saúde deve abranger situações concretas, colocando-se ênfase em normas que garantam a proteção dos dados dos pacientes e a minimização de riscos à sua integridade física e psicológica. Além disso, é fundamental promover a educação ética para todos os envolvidos, desde programadores até profissionais de saúde, conferindo confiança a todos os intervenientes envolvidos e assegurando que a implementação de sistemas de IA seja feita de forma responsável e alinhada com os valores humanos essenciais.

A IA, como qualquer outra tecnologia, deve ser uma ferramenta ao serviço do ser humano, respeitando os direitos fundamentais e sempre voltada para a promoção do bem-estar social. Portanto, para que a IA tenha um impacto positivo e duradouro na saúde, é necessário um compromisso contínuo com a ética, além de uma colaboração constante entre todas as partes interessadas para garantir que as suas vantagens sejam plenamente aproveitadas sem comprometer a confiança na utilização dos sistemas de IA ou os direitos fundamentais dos cidadãos.

REFERÊNCIAS

CALDEIRA, Cristina Maria de Gouveia, O Impacto ético e Jurídico da Aplicação da Inteligência Artificial no Setor da Saúde, Cadernos do Programa de Pós-Graduação, Direito/ Universidade Federal do Rio Grande do Sul, 2021. Disponível em https://www.seer.ufrgs.br/ppgdir/article/download/121131/65761

CASTRO, D., (2016), New J. The promise of artificial intelligence: reckoning and judgment. Cambridge, MA: The MIT Press.

COMISSÃO EUROPEIA, Comunicação da Comissão: Inteligência artificial para a Europa, Bruxelas, 25/04/2018. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018DC0237&from=SV

COMISSÃO EUROPEIA, 2018, Orientações Éticas para uma AI de confiança, p. 47. Disponível em https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

DANTAS, Carina, CABRITA, Miriam, MIDÃO, Luís, COSTA, Elísio, (2024),Alguns desafios e soluções para uma Inteligência Artificial mais ética e confiável em Saúde, Revista Labor Hospitalaria. Disponível em https://www.laborhospitalaria.com/alguns-desafios-solucoes-para-uma-inteligencia-artificial-mais-etica-confiavel-saude

ELIAS, Mariele Abadia, FAVERSANI, ARRUDA, Luciana, MOREIRA, Josiane Aparecida Vieira, MASIERO, Anelise Viapiana, CUNHA, Natalia Veronez da, (2023), Artificial intelligence in health and bioethical implications: a systematic review, Revista Bioética, vol.31 Brasília.

FDA permits marketing of artificial intelligence algorithm for aiding providers in detecting wrist fractures. Food and Drug Administration, 2018. Disponível em: https://www.fda.gov/news-events/press-announcements/fda-permits-marketing-artificial-intelligence-algorithm-aiding-providers-detecting-wrist-fractures

FERNANDES, M., & GOLDIM, J. (2023). Artificial Intelligence and Decision Making in Health: Risks and Oportunities. in Multidisciplinary Perspectives on Artificial Intelligence and the Law, Springer.

GONÇALVES-Sá, J., & PINHEIRO, F. (2023). Societal Implications of Recommendation Systems: A Technical Perspective. in Multidisciplinary Perspectives on Artificial Intelligence and the Law, Springer.

HACKER, Philipp, AI Regulation in Europe: From the AI Act to Future Regulatory Challenges, (2023). Disponível em https://arxiv.org/pdf/2310.04072

KARP, A., (2016), Deep learning will be huge: and here's who will dominate it. San Francisco, CA: Bessemer Venture Partners. Disponível em https://venturebeat.com/business/deep-learning-will-be-huge-and-heres-who-will-dominate-it/

KLEINBERG, Jon, LAKKARAJU, Himabindu, LESKOVEC, Jure, LUDWIG, Jens, MULLAINATHAN, Sendhil, Human Decisions and Machine Predictions, The Quarterly Journal of Economics, Volume 133, Issue 1, February 2018. Disponível em https://academic.oup.com/qje/article-abstract/133/1/237/4095198

KOSINSKI, Matthew, What is black box artificial intelligence (AI)? (2024. Disponível em https://www.ibm.com/think/topics/black-box-ai

LÉVY, Pierre (2022). Inteligência Artificial produz "monstruosidades éticas". Revista Fórum. Disponível em https://revistaforum.com.br/ciencia-e-tecnologia/2022/12/27/inteligncia-artificial-produz-monstruosidades-eticas-diz-pierre-levy-129333.html

LIMA, P., & PAIVA, A. (2023). Autonomous and Inteligent Robots: Social, Legal and Ethical Issues. in Multidisciplinary Perspectives on Artificial Intelligence and the Law, Springer

MACHADO, L. (2019). Médico robô: responsabilidade civil por danos praticados por atos autónomos de sistemas informáticos dotados de Inteligência Artificial. in Lex Medicinae, Ano 16, nº31-32

MAGRANI, E., & SILVA, P. (2023). The Ethical and Legal Challenges of Recommender Systems Driven by Artificial Intelligence. in Multidisciplinary Perspectives on Artificial Intelligence and the Law, Springer. Disponível em https://link.springer.com/chapter/10.1007/978-3-031-41264-6_8

MELO, Ana Karolina Acris, SOUZA, Géssica C, VASCO, Amanda Corrêa, REIS, Breno Salomon, (2022), Evidência Express (EvEx), Regulação da Inteligência Artificial, Benchemarking de países selecionados.

MIRANDA, Jorge, (2000), Manual de Direito Constitucional. Tomo IV. Coimbra: Coimbra Editora, p. 10

NOORBAKHSH-SABET, N., ZAND, R., ZHANG, Y., AABEDI, V., 2019, Artificial intelligence transforms the future of health care. Am J Med. Disponível em https://pmc.ncbi.nlm.nih.gov/articles/PMC6669105/

NUNES, Lorena de Almeida, NETA, Ainah Hohenfeld Angelini, Marco Regulatório da Inteligência Artificial: Análise do AI ACT da União Europeia no Tocante à Privacidade e Proteção dos Dados Pessoais, Revista Direito UNIFACS, 2024. Disponível em https://revistas.unifacs.br/index.php/redu/article/viewFile/9279/5266

NUNES, Rui, Regulação na Saúde, Vida Económica, Porto, 2021, 4ª edição

NUNES, Rui, RICOU, Miguel, GODINHO, Inês, e NEVES, M. Patrão M, (2024) Inteligência Artificial (IA): Inquietações Sociais, Propostas Éticas e Orientações Políticas - LIVRO BRANCO, Conselho Nacional de Ética para as Ciências da Vida. Disponível em https://www.cnecv.pt/files/1715104301_c3ad59f003de091ee280b6c153182c6b_cnecv-livro-branco-ia-maio-2024.pdf

OBERMEYER, Ziad, POWERS, Brian, VOGELI, Christine, and MULLAINATHAN, Sendhil, Dissecting racial bias in an algorithm used to manage the health of populations, Revista Science, 2019. Disponível em https://www.science.org/doi/10.1126/science.aax2342

SAIAS, José, MAIA, Miguel, RATO, Luis e GONÇALVES, Teresa, Dep. de Informática, ECT, Universidade de Évora, (2018), Machine Learning: um estudo sobre conceitos, tarefas e algoritmos relacionados com predição e recomendação. Disponível em https://dspace.uevora.pt/rdpc/bitstream/10174/30174/1/apra_techReport_paper01_2018-11_v02.pdf

VAYENA, E., BLASIMME, A., & COHEN, I. (2018). Machine learning in medicine: Adressing ethical challenges. Disponível em https://pmc.ncbi.nlm.nih.gov/articles/PMC6219763/

Consentimento ético em pesquisas científicas: a influência da literacia jurídica e digital na autonomia do titular de dados

Isabelly Ribeiro Falcão Mendes [200]

Resumo

Este artigo investiga como as literacias jurídica e digital influenciam a autonomia dos titulares de dados diante do consentimento ético em pesquisas científicas. Nesse sentido, o objetivo central é compreender o impacto dessas competências na capacidade de decisão informada, tendo em conta as desigualdades no acesso ao conhecimento jurídico e digital. A pesquisa utiliza metodologia qualitativa, baseada em revisão bibliográfica e análise teórica de autores como Habermas e Freire, além de regulamentos legislativos, como o RGPD, a LGPD e a Declaração de Helsinque. Os resultados, por sua vez, indicam que a ausência de literacia jurídica e digital compromete a compreensão dos termos de consentimento, enquanto práticas como a simplificação da linguagem, o uso de recursos visuais e a implementação de políticas públicas educacionais podem promover maior acessibilidade e inclusão. Conclui-se, portanto, que essas medidas são essenciais para validar o consentimento ético e assegurar autonomia e dignidade nos processos de tratamento de dados.

Palavras-chave: consentimento, literacia, jurídica, digital, autonomia, pesquisas científicas.

[200] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Abstract
This article investigates how legal and digital literacy influence data subjects' autonomy in the context of ethical consent in scientific research. The central objective is to understand the impact of these competencies on the ability to make informed decisions, considering inequalities in access to legal and digital knowledge. The study employs a qualitative methodology, based on a literature review and theoretical analysis of authors such as Habermas and Freire, as well as legislative regulations, including the GDPR, LGPD, and the Declaration of Helsinki. The findings indicate that a lack of legal and digital literacy compromises the understanding of consent terms, while practices such as language simplification, the use of visual resources, and the implementation of educational public policies can enhance accessibility and inclusion. The study concludes that these measures are essential to validate ethical consent and ensure autonomy and dignity in data processing procedures.

Keywords: consent, literacy, legal, digital, autonomy, scientific research.

Introdução

No contexto da era digital, a utilização do conceito de consentimento ético, para fins de fornecimento de dados em pesquisas científicas, tem se tornado cada vez mais comum. Contudo, a compreensão desse consentimento não se mostra acessível, tampouco assegurada a todos os indivíduos, sobretudo, especialmente das disparidades na formação jurídica e digital.

Dito isto, esse estudo visa não apenas definir as literacias jurídica e digital, mas também investigar como ambas influenciam na autonomia do titular de dados, nomeadamente, quanto à sua capacidade de entender e tomar decisões informadas em contextos que envolvem consentimento ético em pesquisas científicas.

Decerto, os estudos acadêmicos e a própria legislação suscitam debates sobre a efetividade do consentimento ético, que é requisito e suporte para a licitude do tratamento de dados em pesquisas científicas, sobretudo, pelo fato de que se vislumbra a necessidade de garantir um consentimento livre e informado, em que o titular tenha a autonomia de decidir com base na compreensão da forma de coleta, do processamento, armazenamento e finalidade dos dados. No entanto, vislumbra-se uma lacuna em estudos voltados especificamente para a evidente interseção entre literacia jurídica e digital no consentimento consciente, livre e inequívoco.

Por essa razão, o presente ensaio visa expor conceitos, como o do consentimento ético, da autonomia do indivíduo e das literacias jurídica e digital, relacionando tais concepções entre si no âmbito das pesquisas científicas. Além disso, pretende construir subsídios para a formulação de diretrizes mais inclusivas, no âmbito do tratamento de dados para fins científicos, principalmente no que diz respeito à elaboração de termos de consentimento, a fim de que esses sejam mais acessíveis e compreensíveis aos indivíduos com diferentes níveis de literacia digital e jurídica.

Nesse sentido, o impasse levantado como o cerne do problema é o seguinte: Como as literacias digital e jurídica influenciam a autonomia do titular de dados e comprometem a efetividade do consentimento ético em pesquisas científicas?

Com isso, as hipóteses para o problema supracitado incluem as ideias de que a) a baixa literacia digital e jurídica compromete a autonomia e dificulta a compreensão do consentimento ético. (b) um maior letramento legal e digital favorece a compreensão do consentimento ético, permitindo decisões mais informadas e autônomas; (c) a adoção de linguagem simples e recursos visuais facilita a compreensão do consentimento, reforçando sua validade e a autonomia do titular.

Sendo assim, o objetivo central do presente artigo se pauta na análise e compreensão das literacias digital e jurídica e a influência na autonomia dos titulares de dados no âmbito das pesquisas científicas, sobretudo, no que diz respeito ao fornecimento do devido consentimento ético. Ainda, em outras palavras, analisar e compreender como esses letramentos impactam a capacidade dos indivíduos de

tomar decisões informadas, considerando os desafios relacionados à disparidade no acesso ao conhecimento digital e jurídico, além de propor soluções para tornar o consentimento ético mais acessível, compreensível e efetivo.

Quanto à especificidade objetiva, pretende-se, então, **definir** os conceitos de literacia digital, literacia jurídica, consentimento ético e autonomia, contextualizando-os no âmbito das pesquisas científicas, **explorar** a relação desses conceitos entre si no âmbito das pesquisas científicas, sobretudo, no que se refere às questões de desigualdade no acesso à educação digital e jurídica, **fornecer** subsídios para a formulação de diretrizes mais inclusivas, visando promover maior autonomia dos titulares e fortalecer a validade do consentimento ético em pesquisas científicas.

Isto posto, a metodologia a ser empregada nesta investigação é de natureza qualitativa, escolhida por sua adequação à análise e exposição de conceitos e à formulação de interpretações críticas, pelo que tal método permite o aprofundamento na compreensão teórica sobre o consentimento ético e a autonomia do titular no contexto das pesquisas científicas.

Ainda, o estudo será embasado em revisão de textos e documentos, incluindo livros, artigos acadêmicos, legislações relevantes e pesquisas já realizadas, com o objetivo de mapear as lacunas existentes na literatura e fundamentar os resultados esperados.

Vale destacar que a pesquisa também adota uma abordagem exploratória, voltada para investigar novas perspectivas e fornecer subsídios para a construção de diretrizes inclusivas no campo do consentimento ético, bem como uma abordagem dogmática, na medida em que interpreta normas jurídicas aplicáveis, como as que regem o tratamento de dados pessoais e a proteção da autonomia dos titulares.

O roteiro da pesquisa inclui, portanto, a leitura aprofundada e crítica de material teórico-bibliográfico. Com efeitos, os resultados alcançados com a pesquisa aqui tecida e estruturada, projetam evidências acerca da influência da literacia digital e jurídica na compreensão dos termos de consentimento ético em pesquisas científicas, dado que a ausência do discernimento compromete a autonomia dos titulares dos dados e os levam a consentir sem, de facto, perceber os seus riscos e as suas implicações. Mais, destacam maneiras de tornar os termos de consentimento mais acessíveis e compreensíveis.

Por fim, concluir que as literacias digital e jurídica são essenciais para que os indivíduos sejam capazes de fornecer consentimento ético informado e autônomo, considerando que sem esses letramentos, os titulares de dados podem ser forçados a tomar decisões sem uma compreensão completa das implicações no âmbito das pesquisas científicas.

2. Consentimento Ético e Literacia Jurídica e Digital: Fundamentos e Relações

Nesta primeira seção, apresentar-se-á os conceitos de consentimento ético, literacia jurídica e digital, analisando suas interseções e o impacto das desigualdades educacionais e tecnológicas nesse contexto.

Desse modo, deve-se considerar o consentimento ético como um eixo nas interações humanas, que perpassa diversos âmbitos desde pesquisas acadêmicas até coleta de dados e práticas comerciais, impondo que indivíduos sejam plenamente informados e capazes de tomar decisões conscientes e voluntárias.

Em seguida, temos a literacia jurídica que, por sua vez, abrange o conhecimento básico das leis e direitos que regulam a vida social, possibilitando que os cidadãos entendam seus deveres e assegurem seus interesses legais. Enquanto a literacia digital refere-se a capacidade de utilizar tecnologias de maneira crítica e informada, abarcando desde o uso de dispositivos eletrônicos até a compreensão das inferências da privacidade e segurança online.

Portanto, no momento em que se interliga tais conceitos e fundamentos, conclui-se que não é possível obter o consentimento ético de forma adequada sem que os indivíduos possuam um mínimo de literacia jurídica e digital. Isso porque, as disparidades educacionais e tecnológicas ampliam a problemática, criando obstáculos para que parcelas da população compreendam plenamente as condições às quais estão sendo submetidas. À luz disso, a análise de tais interseções torna-se essencial na promoção de uma sociedade mais justa e informada, na qual os indivíduos possam exercer e assegurar seus direitos de maneira equitativa e consciente.

2.1 Consentimento Ético: Princípios e Importância no Tratamento de Dados

Para começar, o consentimento ético deve ser visto como um instrumento fundamental para fins de assegurar que o tratamento de dados pessoais ocorra de forma transparente e respeitosa. De acordo com a definição estabelecida pelo n.º 11 do artigo 4.º do Regulamento Geral sobre a Proteção de Dados (RGPD), o consentimento do titular dos dados é entendido como sendo "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".

No mesmo sentido, numa versão mais resumida do dispositivo supramencionado, o artigo 5.º, XII da Lei Geral de Proteção de Dados (LGPD), considera o consentimento como uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Ao passar pela conceituação, faz-se necessário também reafirmar a importância do consentimento como um aspecto ético, capaz de promover a autonomia e assegurar aos participantes de pesquisas científicas a proteção de

possíveis abusos ou riscos decorrentes de atividades investigativas, assim como ressalta a Resolução nº 466/2012 do Conselho Nacional de Saúde.

Sendo certo que ao reiterar a relevância do consentimento ético na proteção dos participantes, se torna indispensável considerar também os desafios práticos para sua efetiva aplicação. A Declaração de Helsinque (2013), um marco ético internacional, corrobora tal necessidade ao estabelecer que as informações fornecidas ao titular devem ser sempre compreensíveis, claras e adequadas ao seu nível de conhecimento, garantindo que suas decisões sejam baseadas em informações reais e completas.

Além disso, é preciso levar em conta as limitações impostas por situações de vulnerabilidade ou desigualdade, que podem comprometer a autonomia no processo de consentimento. A própria Declaração de Helsinque (2013) enfatiza essa preocupação ao estabelecer o seguinte:

> 8. A pesquisa clínica é limitada por padrões éticos que promovem o respeito a todos os seres humanos e protege sua saúde e seus direitos. Algumas populações de pesquisa são vulneráveis ou necessitam de proteção especial. As necessidades particulares dos desassistidos econômica e clinicamente devem ser reconhecidas. É necessária atenção especial também para os que não podem dar ou recusar o consentimento por eles mesmos, para os que podem estar sujeitos a fornecer o consentimento sob coação, para os que não se beneficiarão pessoalmente da pesquisa e àqueles para os quais a pesquisa é associada com precaução.

Tal dispositivo citado torna evidente o facto de que o consentimento não pode ser tratado apenas como um requisito formal, mas sim como um compromisso ético de garantir que todos os indivíduos, independentemente de sua condição social ou capacidade decisória, tenham sua dignidade respeitada.

Contudo, na realidade da prática, a garantia dessa compreensão plena não é uma tarefa simples, sobretudo porque uma das principais barreiras enfrentadas pelo consentimento ético é a complexidade dos documentos utilizados na sua formalização. Desse modo, o uso excessivo de linguagem técnica e pouco acessível a extensão dos termos apresentados, frequentemente, culminam em barreiras para a maioria da população.

Nesse sentido, estudos de Ferreira (2022)[201] evidenciam que essa dificuldade pode levar a consentimentos meramente formais, nos quais o titular aceita as condições sem, de fato, compreender os riscos, benefícios ou finalidades do uso de seus dados. Demonstrando, portanto, a necessidade de tornar os processos de

[201] Ferreira, M. S. (2022). O respeito pela autonomia e o consentimento informado na investigação com seres humanos. *Revista Jurídica do Laboratório de Direito e Bioética, 2*, 1237-1272. https://www.cidp.pt/revistas/rjlb/2022/2/2022_02_1237_1272.pdf

consentimento mais acessíveis e efetivos, garantindo que a autonomia do indivíduo não seja comprometida por obstáculos informacionais.

2.2 Literacia Jurídica: Conceitos e Habilidades para o Exercício da Autonomia

Ultrapassado o conceito e compreensão da importância do consentimento ético, o presente estudo pretende tecer aqui acerca da literacia jurídica, que pode ser entendida como uma competência fundamental na sociedade contemporânea.

Através da literacia jurídica faz-se possível compreender os princípios básicos do direito, o que não é apenas uma vantagem pessoal, mas também uma necessidade para o exercício pleno da cidadania. Dito isto, não se exige que todos os cidadãos sejam especialistas em direito, mas que possam ser oportunizados a obter um conhecimento básico que lhes permita orientarem-se no sistema jurídico, assimilar os seus direitos e deveres e tomar decisões informadas em questões legais, inclusive e principalmente no âmbito das pesquisas científicas.

Segundo Giddens (2002), em *Sociologia*, literacia jurídica consiste na capacidade de um indivíduo de entender e aplicar informações legais em sua vida cotidiana, permitindo o reconhecimento de direitos e deveres. No contexto do consentimento ético, então, ela irá desempenhar um papel crucial, pois não apenas capacita os titulares de dados a interpretar os dispositivos legais, como também a avaliar criticamente os termos apresentados.

Desse modo, extrai-se que a literacia jurídica é a capacidade de compreender e aplicar princípios fundamentais do direito, incluindo entender as leis, os processos e decisões judiciais, os direitos e deveres jurídicos, bem como mecanismos de resolução de conflitos. Ademais, capacita os indivíduos para compreenderem e defenderem os seus próprios direitos, tornando-os aptos a participar ativamente no sistema jurídico e a proteger os seus interesses.

Em contrapartida, a falta de compreensão das leis pode deixar as pessoas vulneráveis à exploração e injustiça, pelo que Sarlet e Caldeira (2019) argumentam que a ausência de literacia jurídica compromete significativamente a autonomia, limitando a capacidade dos indivíduos de compreender os documentos técnicos e, consequentemente, os riscos associados ao consentimento. Inclusive, esse cenário é agravado em populações com menor acesso à educação jurídica, o que as torna mais vulneráveis à manipulação ou aceitação de condições desfavoráveis.

Além disso, o educador Paulo Freire (2018) destaca que a educação deve ser um processo que permita aos indivíduos desenvolverem uma consciência crítica sobre sua realidade, capacitando-os a participar ativamente dos processos sociais e jurídicos. Portanto, a educação jurídica se torna essencial para a construção de uma sociedade democrática, uma vez que permite que as pessoas compreendam seus direitos e deveres, incluindo aqueles relacionados à proteção de dados, sendo sua promoção essencial para assegurar que os titulares de dados possam tomar decisões informadas e livres, em consonância com os princípios da autonomia e da justiça social.

2.3 Literacia Digital: Conceitos e contextos na era digital

No mesmo sentido das definições apresentadas anteriormente, tem-se o contexto da literacia digital. Podendo ser definida como a capacidade de navegar, compreender e fazer o uso das tecnologias da informação, desempenhando, assim como a literacia jurídica, um papel crucial na efetiva autonomia do titular quanto ao consentimento ético.

Decerto, há divergências quanto ao significado de literacia digital e competência digital, no entanto, para a presente pesquisa optou-se seguir o mesmo raciocínio de Adaixo (2022), tal qual como definido pela Comissão Europeia, de modo que "a competência digital pode ser considerada como literacia digital no seu sentido mais amplo, engloba as competências digitais básicas do utilizador", justificando-se pela relação de dependência que estabelece entre competências digitais e um conjunto de ações indispensáveis para comunicar, partilhar, participar nas redes colaborativas via internet.

À esse entendimento, acrescenta-se a visão de Livingstone et al. (2007), que considera a literacia digital uma vertente social essencial, pois possibilita a participação democrática, a cidadania ativa e o desenvolvimento profissional, além de proporcionar uma vida mais plena. Essa perspectiva reforça a importância das competências digitais no contexto atual.

No entanto, a desigualdade no acesso à tecnologia continua sendo um obstáculo significativo, conforme aponta a União Internacional de Telecomunicações (UIT, 2020), com discrepâncias notáveis entre países desenvolvidos e em desenvolvimento. Essa disparidade afeta diretamente a capacidade dos indivíduos de entender os mecanismos tecnológicos envolvidos no tratamento de dados pessoais, incluindo coleta, armazenamento e compartilhamento de informações.

Dentro do campo das pesquisas científicas, a literacia digital é crucial para que os participantes compreendam e avaliem adequadamente os formulários de consentimento ético. No entanto, como observa Ferreira (2022), muitas plataformas utilizam linguagem técnica e estruturas complexas, o que dificulta a compreensão por aqueles com pouca familiaridade com a tecnologia. Essa falta de literacia digital pode resultar em decisões mal informadas ou mal interpretadas, comprometendo a validade ética do consentimento obtido.

2.4 Interseções entre Literacia Jurídica, Digital e Consentimento Ético

Na continuidade da discussão sobre consentimento ético e as implicações da literacia jurídica e entre si, especialmente em um contexto onde a compreensão dos direitos e responsabilidades se faz crucial para o exercício pleno da autonomia do indivíduo.

Durante a mesa redonda do webinar "*Pathways for Justice: Closing the Gap*[202]", que contou com a participação de Anabela Pedroso, Secretária de Estado da Justiça, Maaike de Langen, Líder de Programa da Pathfinders for Justice, Chloé Lelievre, Líder de Programa da OCDE - Justiça/Governação Pública, e Marisa Monteiro Borsboom, Presidente da Humanity of Things (moderadora).

Nesse contexto, a sra. Secretária de Estado da Justiça, Anabela Pedroso (2020) respondeu a uma questão sobre o papel da literacia jurídica nesse processo, destacando a importância dessa competência: "Do lado do cidadão, poderíamos dizer que a literacia jurídica é a pedra angular para a verdadeira democracia".

Sublinhou também que "a literacia jurídica e a literacia digital não são nada uma sem a outra, a literacia jurídica" e completou dizendo que "a literacia digital estão muito interligadas e no fundo, o que pretendemos alcançar é uma maior inclusão principalmente para perceber como posso usar os serviços digitais de forma a obter as respostas a todas as minhas questões"

Quanto à relação entre literacia jurídica, digital e consentimento ético esta é intrínseca e complementar. De acordo com Caldeira e Sarlet (2019), essas literacias oferecem aos indivíduos as ferramentas necessárias para compreender tanto os aspectos legais quanto os tecnológicos envolvidos no tratamento de dados pessoais.

Sendo certo que a ausência de uma dessas competências constitui barreiras significativas para o cumprimento do consentimento ético voltado ao tratamento de dados em pesquisas científicas e para a autonomia do titular de dados. Isto porque, indivíduos com baixo nível de literacia jurídica podem não compreender as implicações legais de suas decisões, enquanto aqueles com pouca literacia digital podem não reconhecer os riscos associados ao uso de plataformas tecnológicas.

Essa combinação de lacunas, como apontado por Sarlet e Caldeira (2019), compromete não apenas a validade do consentimento, mas também a proteção dos direitos fundamentais dos titulares de dados, nomeadamente, a autonomia e a privacidade.

Nesse contexto, a teoria da ação comunicativa de Jürgen Habermas oferece uma compreensão importante sobre como a autonomia e a comunicação se relacionam na construção de um consentimento ético legítimo. Para Habermas (1984), a autonomia é um pilar fundamental da dignidade humana, estando intrinsecamente ligada à capacidade de cada indivíduo se autodeterminar dentro de uma sociedade democrática.

Posto isto, a autonomia não se limita à liberdade individual, mas está conectada ao envolvimento ativo em processos de deliberação, nos quais as decisões são tomadas com base no consenso racional e em uma comunicação livre de coerções.

Nesse sentido, o consentimento ético só pode ser considerado legítimo quando ocorre em um ambiente onde todos têm acesso igualitário à informação, liberdade para questionar e um entendimento claro sobre os termos apresentados.

[202] "Pathways for Justice: Closing the Gap" pode ser traduzido como "Caminhos para a Justiça: Fechando a Lacuna".

Essa ideia se alinha ao disposto no artigo 8 da Declaração de Helsinque, que destaca a necessidade de proteger os indivíduos de qualquer forma de coerção, garantindo que o consentimento seja verdadeiramente livre, sem pressões ou estruturas que possam manipular a decisão, conforme defende a visão habermasiana de autonomia.

Portanto, a literacia jurídica e digital são essenciais, pois permitem que os indivíduos ultrapassem barreiras educacionais e tecnológicas que poderiam impedir uma verdadeira compreensão. Sem essas competências, a comunicação se torna desigual, prejudicando a autonomia e comprometendo a validade ética das decisões sobre o tratamento de dados pessoais, dentro de um sistema estruturado para fazer consentir inconscientemente.

Ademais, Freire (2018), em *Pedagogia da Autonomia,* defende que políticas públicas voltadas para a educação inclusiva, podendo ser incluídas a jurídica e a digital, são cruciais para reduzir as desigualdades no acesso à informação. O educador sugere que a simplificação da linguagem nos documentos de consentimento, juntamente com o uso de elementos visuais, pode facilitar o entendimento e tornar o processo mais acessível.

Dessa forma, além de garantir que o consentimento ético seja mais compreendido e respeite a autonomia dos participantes, essas iniciativas reforçam a importância da literacia digital e jurídica, assegurando que todos os cidadãos tenham as condições necessárias para tomar decisões informadas e conscientes.

3. A Relação entre Literacias Jurídica e Digital e a Efetividade do Consentimento Ético em Pesquisas Científicas

Em ordem ao que já foi discutido no presente estudo, neste capítulo, explora-se a interconexão entre as literacias jurídica e digital, destacando seus papéis nas pesquisas científicas, especialmente no que se refere ao consentimento ético.

No desenrolar da discussão será abordado como as desigualdades no acesso à educação jurídica e digital impactam a autonomia dos participantes e comprometem a validade do consentimento. A partir dessa análise, serão ponderadas estratégias e diretrizes para tornar o consentimento mais acessível e inclusivo, promovendo maior compreensão por parte dos titulares de dados e assegurando o respeito à sua dignidade e direitos.

Tendo em vista que o consentimento ético é uma prática indispensável no tratamento de dados em pesquisas científicas, pautado nos princípios de liberdade, informação e autonomia. No entanto, sua aplicação enfrenta desafios significativos, principalmente devido à desigualdade no acesso à educação jurídica e digital.

3.1 O Papel da Literacia Jurídica na Compreensão do Consentimento Ético

Com isso em mente, a literacia jurídica é um elemento central na validação do consentimento ético, uma vez que sua ausência afeta diretamente a autonomia do titular de dados, comprometendo sua capacidade de compreender os direitos e responsabilidades associados à participação em pesquisas científicas.

Sarlet e Caldeira (2019) apontam que, em muitos casos, os termos de consentimento apresentam uma linguagem técnica e jurídica complexa, dificultando a compreensão por parte do público geral.

Nesse espectro, a autonomia, como definida por Habermas (1984), não se limita à liberdade de escolha, mas exige condições que garantam igualdade de entendimento e comunicação entre as partes envolvidas. Desse modo, pode-se inferir que nas situações onde o titular de dados não entende os riscos e objetivos do tratamento, o consentimento se torna apenas uma formalidade burocrática, desvinculada de sua função ética.

Além disso, tanto a LGPD quanto o RGPD preveem que os termos de consentimento sejam apresentados de forma clara e compreensível, mas não oferecem orientações detalhadas sobre como garantir essa clareza na prática. Isso cria uma lacuna entre o que as leis estipulam e as dificuldades enfrentadas por indivíduos com menor literacia jurídica, que podem concordar com termos sem compreender de fato as implicações de suas decisões.

Embora a intenção da legislação seja garantir transparência, a linguagem jurídica complexa e a falta de diretrizes claras para promover essa compreensão acabam dificultando o entendimento genuíno por parte do cidadão. Evidenciando, assim, a necessidade de um aprimoramento na educação jurídica, pois ela desempenha um papel fundamental na desconstrução da complexidade dos documentos legais, permitindo que os indivíduos compreendam as condições de consentimento de maneira mais clara e informada.

Portanto, a capacitação jurídica e digital torna-se crucial para garantir que as pessoas possam exercer seus direitos de forma plena e consciente, principalmente se for contextualizada com base no pensamento de Freire (2018), que defende a democratização do conhecimento como um meio para alcançar a autonomia, é possível afirmar que a educação jurídica acessível e adequada à realidade de cada pessoa é essencial para que a autonomia não seja apenas uma idealização, mas sim uma prática efetiva.

Além disso, a inclusão dessas educações no cotidiano das pessoas, especialmente considerando as desigualdades sociais e educacionais, se torna imprescindível para que todos possam exercer seus direitos de forma igualitária e participar ativamente na sociedade, sem limitações impostas por uma compreensão limitada dos seus próprios direitos.

3.2 A Influência da Literacia Digital na Validade do Consentimento Ético

Dando continuidade a essa reflexão sobre a importância da literacia jurídica, cabe agora discutir um aspecto igualmente relevante para a efetividade do consentimento ético: a literacia digital. Em um contexto onde as plataformas digitais desempenham papel central na coleta e tratamento de dados, a compreensão da tecnologia e das suas implicações torna-se fundamental para garantir a validade ética do consentimento.

Assim, a literacia digital, como definida por Buckingham (2006), sendo a habilidade de compreender e utilizar informações digitais, desempenha um papel crucial em um mundo onde os dados pessoais são majoritariamente tratados em plataformas digitais. No entanto, é possível deduzir que a sua falta impede a compreensão adequada dos termos de consentimento nas plataformas digitais, comprometendo a validade ética do processo.

No âmbito das pesquisas científicas, plataformas digitais são frequentemente utilizadas para coletar consentimentos, apresentando termos que, em sua maioria, são extremamente confusos, extensos ou inacessíveis para indivíduos com baixa familiaridade tecnológica.

Conforme os estudos feitos pela União Internacional de Telecomunicações (UIT, 2020) mostram que a desigualdade no acesso à tecnologia ainda é um problema global, especialmente em países em desenvolvimento, onde o conhecimento sobre privacidade digital é limitado.

Pela mesma obra já citada, Freire (2018) enfatiza que a falta de uma educação crítica e acessível reforça desigualdades sociais, limitando a capacidade dos indivíduos de compreender e agir sobre as realidades que os cercam. Embora ele não se refira diretamente à tecnologia, deduz-se que a falta de uma base educacional sólida em áreas digitais pode ser vista como uma extensão dessa desigualdade, dificultando o entendimento de implicações importantes, como as associadas ao consentimento.

Isso se torna ainda mais crítico quando a coleta de dados ocorre por meio de sistemas automatizados que não oferecem explicações claras sobre os riscos envolvidos, o que torna imprescindível a tomada de providências estratégicas para tornar o consentimento ético mais acessível e inclusivo.

3.3 Estratégias para Tornar o Consentimento Ético Mais Acessível e Inclusivo

Para superar as barreiras criadas pela falta de literacia jurídica e digital, deve-se adotar abordagens práticas que tornem o consentimento ético mais inclusivo e compreensível para todos. Como Habermas (1984) sugere, a comunicação deve ser livre de coerções e transparente, condições que são essenciais para garantir a autonomia na tomada de decisões. Isso implica, por exemplo, em simplificar os processos e documentos relacionados ao consentimento, para que qualquer

pessoa, independentemente do seu nível de educação ou acesso à tecnologia, consiga entender.

Uma estratégia importante para alcançar esse objetivo é a simplificação da linguagem nos termos de consentimento, como dito, o RGPD e a LGPD, por exemplo, já reconhece a importância da transparência e clareza nesse processo, ao exigir que os termos de consentimento sejam apresentados de forma simples, garantindo que os titulares de dados compreendam suas escolhas. Entretanto, isso só será efetivo se forem apontados em concreto os critérios para definir essa clareza e transparência, numa real adaptação da linguagem usada nas plataformas digitais.

Além disso, o uso de recursos visuais pode aumentar significativamente a compreensão dos termos de consentimento. Ferreira (2022) destaca a eficácia de infográficos, vídeos curtos e outros elementos multimídia para tornar a informação mais acessível, especialmente para aqueles que possuem dificuldades com linguagem técnica ou com a navegação em plataformas digitais.

Incorporar esses recursos em sistemas de coleta de consentimento online não só facilita o entendimento dos termos, como também envolve os indivíduos de forma mais interativa, melhorando o engajamento com o conteúdo e com as implicações da sua decisão.

Outra abordagem crucial está nas políticas públicas que incentivem a educação em áreas jurídicas e digitais, é necessário desenvolver programas de alfabetização tanto digital quanto jurídica, por meio de campanhas educacionais e parcerias com instituições de ensino, pois bem se vê que a educação é uma ferramenta poderosa, como já apontado por Freire (2018), para transformar realidades e promover a inclusão.

Destarte, ao empoderar as pessoas com conhecimento sobre seus direitos e como navegar em ambientes digitais, é possível garantir que elas possam fazer escolhas conscientes e autônomas, respeitando os princípios éticos e de privacidade nas pesquisas científicas.

CONSIDERAÇÕES FINAIS

À luz do exposto, conclui-se que este estudo teve como objetivo compreender a influência das literacias jurídica e digital sobre a autonomia dos titulares de dados e a validade do consentimento ético em pesquisas científicas, tendo a pesquisa abordado, a partir de uma análise teórica, as interações entre esses conceitos, focando em como a falta de literacia em ambos os âmbitos compromete a capacidade dos indivíduos de tomar decisões informadas e autônomas, principalmente em um contexto digital.

Os resultados confirmaram que a compreensão dos termos de consentimento, que deve ser clara e acessível, depende diretamente do nível de literacia jurídica e digital dos indivíduos. Aqueles com maior conhecimento nessas áreas possuem melhores condições de entender os riscos e direitos envolvidos, enquanto os menos

familiarizados ficam em desvantagem, muitas vezes aceitando termos sem uma compreensão adequada.

Além disso, observou-se que a falta de literacia digital também impacta a eficácia do consentimento ético, já que grande parte dos processos de coleta de dados ocorre em plataformas digitais. Muitos indivíduos, principalmente em contextos de desigualdade social, não têm acesso ao conhecimento necessário para navegar nesses ambientes de forma crítica e consciente.

Isso se reflete nas dificuldades de entender as implicações de seu consentimento, especialmente quando os termos são apresentados em formato complexo ou sem recursos explicativos.

A pesquisa validou as hipóteses levantadas, como a de que a maior literacia jurídica e digital melhora a capacidade de decisão informada e autônoma. Ao contrário, a falta dessas habilidades resulta em uma compreensão superficial, comprometendo a validade do consentimento.

Também foi confirmada a ideia de que a adoção de recursos mais acessíveis, como linguagem simplificada e elementos visuais, pode ajudar a superar essas barreiras.

Com base nos resultados, ponderou-se a respeito de propostas para a simplificação da linguagem dos termos de consentimento, o uso de infográficos e vídeos explicativos, e a implementação de mecanismos de feedback interativo são medidas essenciais para tornar os processos de consentimento mais acessíveis.

Além disso, é crucial que políticas públicas incentivem a alfabetização jurídica e digital, promovendo uma educação que capacite os cidadãos a exercerem seus direitos de forma plena e consciente.

Em conclusão, a pesquisa enfatiza que a superação das lacunas educacionais nos âmbitos jurídico e digital é fundamental para garantir um consentimento ético verdadeiramente livre e informado em pesquisas científicas. Isso requer um esforço conjunto entre pesquisadores, instituições e formuladores de políticas públicas, com o objetivo de criar um ambiente mais justo e igualitário, em que a autonomia dos titulares de dados seja respeitada e protegida.

REFERÊNCIAS

Azevedo, J., Pedro, L., & Santos, R. (2016). Literacia(s) digital(ais): definições, perspetivas e desafios. *Revista Media & Jornalismo*, 27(1). https://impactum-journals.uc.pt/mj/article/view/2183-5462_27_1/2721

Brasil. (2012). Resolução nº 466/2012 do Conselho Nacional de Saúde. http://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf

Brasil. (2018). Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709). http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Buckingham, D. (2006). *Defining digital literacy: What do young people need to know about digital media?* Nordic Journal of Digital Literacy, 1(4), 263–276. Recuperado de https://www.researchgate.net/publication/284919482_Defining_digital_literacy_What_do_young_people_need_to_know_about_digital_media

Dias, I. (2021). *A utilização das tecnologias digitais na educação: Competências e desafios* [Dissertação de Mestrado, ISCTE - Instituto Universitário de Lisboa]. Repositório do ISCTE. https://repositorio.iscte-iul.pt/bitstream/10071/26770/1/master_isabel_dias_adaixo.pdf

Ferreira, M. S. (2022). O respeito pela autonomia e o consentimento informado na investigação com seres humanos. *Revista Jurídica do Laboratório de Direito e Bioética*, 2, 1237-1272. https://www.cidp.pt/revistas/rjlb/2022/2/2022_02_1237_1272.pdf

Freire, P. (2018). *Pedagogia da autonomia: saberes necessários à prática educativa* (3ª ed.). Paz e Terra. https://nepegeo.ufsc.br/files/2018/11/Pedagogia-da-Autonomia-Paulo-Freire.pdf

Giddens, A. (2002). Sociologia Artmed. https://damas20162.wordpress.com/wp-content/uploads/2016/08/giddens-anyhony-sociologia.pdf

Habermas, J. (1984). *The theory of communicative action* (Vol. 1). Beacon Press. Recuperado de https://teddykw2.wordpress.com/wp-content/uploads/2012/07/jurgen-habermas-theory-of-communicative-action-volume-1.pdf

Jenkins, H., Clinton, K., Purushotma, R., Robinson, A. J., & Weigel, M. (2009). *Confronting the challenges of participatory culture: Media education for the 21st century*.

MacArthur Foundation. https://www.macfound.org/media/article_pdfs/jenkins_white_paper.pdf

Livingstone, S., & Helsper, E. (2007). Gradations in digital inclusion: Children, young people and the digital divide. *New Media & Society*, 9(4), 671-696. https://doi.org/10.1177/1461444807080335

Ministério da Justiça. (2021, junho 17). *Evento online: Pathways for Justice – Closing the Gap*. https://justica.gov.pt/Noticias/Inovacao-deve-tornar-Justica-mais-simples-e-acessivel-para-o-cidadao

Sarlet, G. B. S., & Caldeira, C. (2019). *O consentimento informado e a proteção de dados pessoais de saúde na internet: Uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. Civilistica.com, 8, 1-27.*
https://civilistica.emnuvens.com.br/redc/article/download/411/345

União Europeia. (2011). *Digital Agenda Scoreboard 2011* [Relatório]. https://ec.europa.eu/digital-strategy/our-policies/digital-agenda-scoreboard

União Europeia. (2016). Regulamento Geral de Proteção de Dados (RGPD) (Regulamento [UE] 2016/679). *Jornal Oficial da União Europeia*. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679

UIT. (2020). *Measuring digital development: Facts and figures 2020*. https://www.itu.int/

World Medical Association. (2013). *Declaração de Helsinque: Princípios éticos para as pesquisas médicas envolvendo seres humanos*. https://www.wma.net/

A Inteligência Artificial e a Integridade das Decisões Clínicas: Desafios Éticos e Normativos

André Filipe da Fonseca Carreto Lopes [203]

Resumo

Este artigo científico analisa em profundidade a crescente aplicação da Inteligência Artificial (IA) no setor da saúde, destacando como as decisões clínicas são impactadas pela adoção de algoritmos cada vez mais sofisticados. O objetivo principal consiste em avaliar de que forma a IA pode melhorar a precisão e a eficiência do diagnóstico, ao mesmo tempo em que se questionam possíveis efeitos negativos, tais como a transparência dos modelos algorítmicos, a parcialidade de dados e as repercussões na autonomia do profissional de saúde e no consentimento informado.

A metodologia adotada foi predominantemente exploratória, permitindo identificar protagonistas, áreas críticas de intervenção, referenciais teóricos e normativos, bem como tendências e cenários futuros. Paralelamente, recorreu-se a uma abordagem dogmática em momentos específicos, sobretudo na análise de quadros normativos em vigor, diretivas institucionais e códigos deontológicos. Além disso, o estudo assumiu traços descritivos, ao caracterizar o estado da arte da IA na saúde, descrevendo práticas consolidadas, tecnologias emergentes e exemplos de aplicação, possibilitando assim um retrato fiel e contextualizado que fundamenta as reflexões éticas subsequentes.

Os resultados indicam que a IA tem potencial para agilizar diagnósticos, personalizar tratamentos e otimizar recursos clínicos, mas expõe igualmente riscos éticos e jurídicos, desde a manipulação indevida de dados sensíveis até à perpetuação de desigualdades sociais. Conclui-se que o quadro normativo em vigor – com destaque para o Regulamento Geral de Proteção de Dados (RGPD) e o Regulamento (UE) 2024/1689 (EU AI Act) – constitui uma base sólida, mas carece de atualização permanente e de uma abordagem preventiva que envolva literacia digital, formação contínua dos profissionais de saúde e sistemas de auditoria dos algoritmos. Estes mecanismos são cruciais para garantir a integridade das decisões clínicas e a

[203] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

preservação dos valores humanistas da medicina, mesmo num ambiente em acelerada transformação tecnológica.

Palavras-chave: IA; Decisões Clínicas; Proteção de Dados; Ética; Regulamentação

Abstract

This scientific article provides an in-depth analysis of the growing application of Artificial Intelligence (AI) in the healthcare sector, highlighting how clinical decisions are influenced by increasingly sophisticated algorithms. The primary objective is to assess how AI can enhance diagnostic accuracy and efficiency while also examining potential drawbacks, such as algorithmic opacity, data bias, and the implications for healthcare professionals' autonomy and informed consent.

Methodologically, this research adopts an exploratory approach, enabling the identification of key stakeholders, critical areas for intervention, theoretical and regulatory frameworks, as well as future trends and scenarios. In specific instances, a dogmatic approach is applied, particularly in examining existing regulatory frameworks, institutional directives, and professional codes of ethics. Additionally, the study features descriptive elements by characterizing the current state of AI in healthcare, outlining established practices, emerging technologies, and real-life applications. This detailed depiction offers a reliable and contextualized foundation for the subsequent ethical discussions.

The findings suggest that AI holds great promise for streamlining diagnostics, personalizing treatments, and optimizing clinical resources. Nevertheless, it also presents ethical and legal risks, including inappropriate handling of sensitive data and the perpetuation of social inequalities. The existing regulatory framework—especially the General Data Protection Regulation (GDPR) and Regulation (EU) 2024/1689 (EU AI Act)—provides a solid basis but requires continuous updates and a preventative approach. Such an approach should incorporate digital literacy, ongoing professional training, and algorithm auditing systems. These mechanisms are crucial for safeguarding the integrity of clinical decisions and preserving the humanistic values of medicine in a rapidly transforming technological environment.

Keywords: AI; Clinical Decisions; Data Protection; Ethics; Regulation

Introdução

A expansão progressiva das capacidades de processamento de dados, a par dos avanços na aprendizagem automática *(machine learning)* e na aprendizagem profunda *(deep learning)*, tem permitido à Inteligência Artificial (IA) assumir um papel cada vez mais relevante no setor da saúde. Atualmente, algoritmos identificam padrões em exames de imagem, diagnosticam complicações em doentes crónicos e ajudam na escolha de tratamentos personalizados (*Topol, 2019*). Esta tendência é reforçada pelo volume crescente de dados clínicos disponíveis – o chamado *Big Data* –, que alimenta os modelos e incrementa a sua precisão.

A adoção deste tipo de tecnologia não surge, porém, isenta de controvérsias. Se, por um lado, a IA revela-se promissora para agilizar processos, por outro, levanta preocupações sobre a proteção de dados sensíveis, a explicabilidade das decisões e a tendência que pode afetar grupos populacionais vulneráveis *(Abidi, 2019; Barocas et al., 2019)*. A prática médica, historicamente moldada por princípios éticos e deontológicos, vê-se confrontada com a necessidade de integrar a inovação tecnológica, sem perder de vista a dignidade e a autonomia do doente, bem como a responsabilidade do profissional de saúde.

Simultaneamente, o quadro legal europeu tem procurado acompanhar esta transformação. O Regulamento (EU) 2016/679 (RGPD) estabelece diretivas específicas para o tratamento de dados, incluindo os de saúde, e o Regulamento (EU) 2024/1689 (EU AI Act) reforça a necessidade de padrões de transparência e robustez em sistemas de IA de alto risco, como os da área médica *(Comissão Europeia, 2020; European Parliament, 2023)*. Ainda assim, a velocidade do desenvolvimento tecnológico questiona a suficiência desses normativos e abre margem para discussões acerca da responsabilização em caso de erro clínico.

O conceito de integridade das decisões clínicas surge, neste contexto, como fio condutor desta investigação. Pretende-se compreender de que forma as decisões médicas continuam a ser informadas pelos valores humanistas centrais – beneficência, não prejudicar, autonomia e justiça – quando uma parte substancial da avaliação diagnóstica e terapêutica passa a depender de algoritmos obscuros ou de difícil interpretação *(Friedman & Nissenbaum, 1996)*. Assim, este artigo propõe-se avaliar os principais desafios éticos e normativos e discutir possíveis caminhos para a adoção segura e responsável da IA em saúde.

Do ponto de vista metodológico, recorre-se a uma revisão bibliográfica e documental abrangente, integrando estudos académicos, em diferentes contextos e disposições legais nacionais e europeias. A proposta analítica abrange, de forma ligada, o enquadramento tecnológico, as implicações éticas e jurídicas, a problemática da tendência, a preservação da autonomia profissional e a relação médico-paciente, culminando na apresentação de sugestões para uma gestão ética e transparente da IA. Estrutura-se, pois, o artigo em secções que vão do

enquadramento teórico às conclusões, procurando esmiuçar a forma como a IA pode reforçar ou, pelo contrário, fragilizar a integridade das decisões clínicas. Segue-se o Desenvolvimento, onde se aprofunda a aplicação prática de algoritmos, com destaque para a recolha e tratamento de dados, as preocupações referentes à 'caixa negra' (*Black Box)* algorítmica e ao consentimento informado. Depois, apresentam-se os Resultados, com uma síntese das principais constatações empíricas e teóricas, e a Discussão, na qual se confrontam os dados obtidos com a literatura especializada, salientando as lacunas regulatórias. Por fim, na Conclusão, reflete-se sobre as implicações que a IA tem a longo prazo para a medicina, propondo-se estratégias e recomendações para preservar o caráter humanista da prática clínica.

1. Revisão Bibliográfica: Estado da Arte e Referência Teórica

1.1. Estado da Arte

1.1.1. Levantamento Crítico das Investigações Existentes

A adoção da IA em saúde tem sido alvo de inúmeros estudos *(Amaro, 2022; Freitas & Novais, 2018; Topol, 2019*), que evidenciam sobretudo a capacidade de algoritmos de *machine learning* para processar grandes volumes de dados clínicos, detetando padrões e prevendo complicações. Se, por um lado, isso agiliza e otimiza o diagnóstico, por outro, alguns autores (*Obermeyer et al. 2019 e Barocas et al. 2019)* alertam para o risco de preconceito nos algoritmos, alimentado por bases de dados historicamente tendenciosas. Esse preconceito pode prejudicar grupos vulneráveis, aumentando desigualdades já existentes.

No campo prático, as aplicações radiológicas *(Benke & Benke, 2018; Amaro, 2022)* e de triagem hospitalar *(Dias, 2020; Obermeyer et al., 2019)* são apontadas como paradigmas que ilustram bem as vantagens e, simultaneamente, os problemas da IA na saúde. Em paralelo, do ponto de vista legal, *Pereira (2015) e Dias (2020)* discutem detalhadamente o desafio de atribuir responsabilidade civil, especialmente nos cenários em que o erro clínico tem origem numa recomendação algorítmica imperfeita ou mal aplicada.

1.1.2. Identificação de Lacunas e Caminhos Futuros

A revisão da bibliografia demonstra uma evolução significativa da IA na medicina, mas realça também aspetos carentes de investigação. A representatividade dos dados continua a ser um problema central, na medida em que a maioria dos conjuntos de treino não reflete a diversidade de perfis de doentes e respetivas condições de saúde *(Obermeyer et al., 2019)*. Acresce que a "caixa negra" algorítmica *(Raji et al., 2020)* dificulta a explicabilidade, condicionando o consentimento informado e a autonomia tanto do médico quanto do doente.

Como possíveis caminhos de progresso, diversos autores *(Freitas & Novais, 2018; Raji et al., 2020; Pedro et al., 2023)* sugerem:

- Maior investimento em metodologias de *Explainable AI,* de modo a tornar inteligíveis as decisões algorítmicas;
- Auditorias independentes para detetar preconceitos e avaliar a robustez dos sistemas;
- Formação contínua dos profissionais de saúde, não só na vertente técnica, mas também na vertente ética e legal, para que saibam questionar e utilizar criticamente as recomendações dos algoritmos.

1.1.3. Análise Crítica para a Formulação de Problemas, Objetivos e Metodologia

As lacunas acima apontadas justificam a problemática central deste artigo: compreender como a IA pode, efetivamente, contribuir para decisões clínicas mais integras e humanas, sem que a autonomia e a dignidade do paciente fiquem em risco. A metodologia exploratória e dogmática escolhida (analisando diplomas como o *RGPD* e o *EU AI Act)* também encontra fundamento nas reflexões da literatura, que insiste na necessidade de enquadrar juridicamente a utilização da IA, impondo limites claros e atribuindo responsabilidades *(Dias, 2020; Pereira, 2015)*.

1.1.4. Articulação entre Teoria e Prática, Base Conceitual

A teoria e a prática articulam-se, sobretudo, nos casos de sucesso e nas aplicações já implementadas *(Amaro, 2022; Dias, 2020)*. A bioética clarifica os limites do uso da IA ao enfatizar a beneficência e a justiça, enquanto a regulamentação europeia *(RGPD, EU AI Act)* fornece pilares para a proteção de dados sensíveis. A gestão de sistemas de saúde demonstra como a IA pode otimizar recursos, mas alerta para a necessidade de políticas internas e de formação para garantir que as propostas algorítmicas são devidamente interpretadas e validadas *(Freitas & Novais, 2018)*. Desta forma, os pressupostos científicos transpostos para o ambiente clínico contribuem para a consolidação de práticas que não descuram a dimensão ética e legal, preservando a essência humanista da medicina. A IA é entendida não apenas como uma ferramenta tecnológica, mas como um fenómeno multidimensional que afeta relações profissionais, decisões clínicas e direitos fundamentais, incluindo a privacidade e a não-discriminação.

2. Enquadramento Tecnológico e Operacional da IA em Saúde

2.1. Big Data e Aprendizagem Automática

A expansão da capacidade de armazenamento e análise de dados impulsionou radicalmente a adoção de sistemas de *machine learning* na saúde. Algoritmos capazes de processar milhões de registos clínicos (resultados de exames, registos médicos eletrónicos, dados demográficos) tornam-se aptos a identificar correlações subtis e padrões indicativos que o clínico, por mais experiente que seja, dificilmente conseguiria apreender na sua totalidade *(Amaro, 2022)*. O desenvolvimento do

deep learning, por sua vez, reforçou esta tendência, ao permitir a implementação de redes neuronais com múltiplas camadas, capazes de lidar com volumes maciços de informação *(Freitas e Novais, 2018)*.

O conceito de *Big Data* em saúde compreende, portanto, a recolha massiva de informações de múltiplas fontes, incluindo imagens radiológicas, dados laboratoriais, monitorização de sinais vitais em tempo real e até elementos de estilo de vida captados por dispositivos *wearables (OMS, 2021)*. A IA, ao alimentar-se destes dados, sustenta sistemas de apoio à decisão que se apresentam como capazes de prever o risco de determinadas complicações ou de recomendar intervenções específicas com base no perfil individual do paciente *(Lovis, 2019)*.

2.2. Arquitetura de Sistemas e Infraestruturas Digitais

A implementação de IA requer infraestrutura robusta, o que implica redes hospitalares seguras, sistemas de armazenamento (em *cloud* ou servidores locais) com protocolos de encriptação e plataformas de interoperabilidade para o intercâmbio de dados entre diferentes unidades de saúde *(ENISA, 2016)*. Esta vertente técnica, apesar de muitas vezes subestimada, é crucial para garantir que a informação flua de modo confiável e que os algoritmos possam ser treinados com dados fidedignos e continuamente atualizados *(Johnson et al., 2016)*.

2.3. 'Caixa Negra' Algorítmica: O Desafio da Explicabilidade

Ao mesmo tempo que o *deep learning* eleva a precisão de determinados diagnósticos, acentua a questão da falta de clareza: como compreender as relações internas que o algoritmo estabelece entre as variáveis? *(Raji et al., 2020)* Em muitas redes neuronais, a quantidade de parâmetros é de tal ordem que inviabiliza a explicação convencional do tipo "o algoritmo concluiu X por causa de Y". Surge, então, a necessidade por abordagens de *explainable* AI *(XAI)*, que possam oferecer, aos profissionais de saúde, justificativas minimamente inteligíveis para cada recomendação *(Leslie, 2019)*.

3. Implicações Éticas: Autonomia, Beneficência, Justiça e Proteção

3.1. Autonomia Profissional e Participação do Paciente

Uma das preocupações mais citadas na literatura é o risco de perda de autonomia do médico, que pode sentir-se coagido a aceitar passivamente a sugestão do algoritmo *(Dias, 2020)*. De igual modo, o paciente, ao defrontar-se com a autoridade técnica de um sistema considerado altamente preciso, pode ver limitada a sua capacidade de questionar ou recusar intervenções *(Pereira, 2015)*. Este cenário contraria o princípio ético da autonomia e o próprio conceito de consentimento informado, pelo qual o paciente deve exercer um papel ativo na decisão terapêutica *(Associação Médica Mundial, 2013)*.

A autonomia profissional, por outro lado, não significa recusar a inovação. O equilíbrio desejável consiste em integrar a IA como um auxílio ao raciocínio clínico, sem substituir a prudência e a experiência do médico, e assegurando ao paciente uma visão clara sobre as razões que motivam as recomendações *(Topol, 2019)*.

3.2. Beneficência e Proteção: Riscos de Erro e Dependência

A beneficência aponta para a obrigação de promover o bem-estar do paciente, e a IA, ao aumentar a precisão diagnóstica, tende a alinhar-se com este princípio *(Benke e Benke, 2018)*. A rapidez na deteção de tumores, por exemplo, pode salvar vidas ou permitir intervenções menos invasivas. Todavia, a proteção exige cautela: qualquer erro algorítmico pode ter consequências graves, especialmente quando o médico segue, sem validação, o resultado do sistema. Em última análise, a decisão deve resultar do estudo conjunto dos dados pelo profissional e pelo próprio doente, respeitando a individualidade de cada caso clínico *(Gordete, 2024)*.

3.3. Justiça: Parcialidade e Desigualdades

O princípio da justiça requer uma distribuição equitativa dos recursos de saúde e a ausência de discriminação. No entanto, algoritmos treinados em conjuntos de dados historicamente tendenciosos podem reforçar preconceitos, ao atribuir menor prioridade ou subvalorizar sintomas de certos grupos populacionais, seja por razão de etnia, género ou situação socioeconómica *(Barocas et al., 2019; Obermeyer et al., 2019)*. Quando o Estado, ou as entidades hospitalares, confiam nestes algoritmos para alocar serviços ou avaliar riscos, corre-se o perigo de aprofundar desigualdades já existentes. Torna-se fundamental, pois, introduzir metodologias de auditoria e correção de tendências que assegurem a imparcialidade.

4. Quadro Normativo e Proteção de Dados

4.1. Regulamento Geral sobre a Proteção de Dados (RGPD)

O RGPD (União Europeia, 2016) constitui a base do regime jurídico que protege a privacidade e a autodeterminação informativa na UE. Ao classificar dados de saúde como dados sensíveis, impõe deveres rigorosos de consentimento e proteção, reforçando princípios como a minimização de dados e a limitação de finalidades. Num ambiente algorítmico, isto implica assegurar que a recolha e o processamento de informação pessoal se baseiam em autorizações adequadas e que não se ultrapassam finalidades não consentidas *(Gordete, 2024)*.

4.2. Regulamento (UE) 2024/1689 (EU AI Act)

Com o intuito de responder ao rápido progresso da IA, a UE promulgou o EU AI Act *(European Parliament, 2023)*, que classifica diferentes aplicações de IA de acordo com o grau de risco. As aplicações de IA na saúde são consideradas de alto risco, exigindo padrões reforçados de transparência, robustez e supervisão humana. Embora ainda em processo de implementação, esta legislação sinaliza um

compromisso com a segurança e a explicabilidade, prevendo sanções severas para práticas que violem princípios fundamentais de proteção de dados e direitos fundamentais *(Comissão Europeia, 2020)*.

4.3. Responsabilização em Caso de Erro Clínico Algorítmico

Uma questão fulcral consiste em definir quem assume a responsabilidade caso um paciente sofra danos devido a um erro do algoritmo ou à utilização imprudente do mesmo *(Dias, 2020)*. Se, por um lado, o médico continua a ser legalmente responsável pela decisão final, por outro, existe a influência objetiva do algoritmo no raciocínio clínico. A jurisprudência encontra-se ainda em fase inicial, mas antevê-se a necessidade de regimes específicos que estabeleçam partilha de culpas ou, pelo menos, a obrigação de manter rastreamento (*logs*) que permitam apurar onde o erro se originou *(Pereira, 2015)*.

5. Literacia Digital e Formação Contínua

5.1. Desafios de Capacitação para Profissionais de Saúde

A literacia digital surge como fator determinante para uma adoção equilibrada da IA. Sem formação adequada em análise de dados, estatística e princípios básicos de *machine learning*, o profissional de saúde pode cair na armadilha de considerar a recomendação do algoritmo como inquestionável *(Pedro et al., 2023)*. Programas de formação e workshops específicos, promovidos por universidades, ordens profissionais e centros de investigação, tornam-se assim essenciais para desenvolver o senso crítico e a compreensão das limitações técnicas de cada sistema algorítmico *(Ianni et al., 2020)*.

5.2. O Papel das Instituições e dos Organismos Deontológicos

Para além da qualificação individual, é crucial que as instituições de saúde elaborem políticas internas de gestão de IA, nomeando equipas responsáveis pela revisão ética e técnica dos modelos. Igualmente, os organismos deontológicos podem estabelecer orientações que regulem a interação entre o médico e a IA, definindo a margem de autonomia do profissional e as boas práticas de consentimento informado *(Freitas e Novais, 2018)*. Sem essas diretrizes, arrisca-se a fragmentação de abordagens e a eventual disseminação de sistemas desajustados ou perigosos.

6. Exemplos de Aplicação Prática e Estudos de Caso

6.1. Radiologia e Diagnóstico de Imagem

Na radiologia, algoritmos de *deep learning* demonstram capacidades notáveis de detetar microcalcificações em mamografias ou nódulos pulmonares em estados iniciais, aumentando a taxa de deteção de cancro *(Amaro, 2022)*. Em múltiplos

hospitais, sistemas de IA complementam a análise do radiologista, reduzindo a variabilidade entre avaliadores e acelerando o fluxo de trabalho. Contudo, permanece a dependência face à qualidade dos dados de aprendizagem: se certas populações estiverem sub-representadas, o sistema pode errar mais em grupos específicos, configurando um risco de injustiça *(Barocas et al., 2019)*.

6.2. Triagem em Serviços de Urgência

Outra área de aplicação é a triagem automatizada: algoritmos que, ao analisar sintomas, sinais vitais e histórico clínico, atribuem prioridades de atendimento. Em situações de grande afluência, esta automatização pode minimizar tempos de espera e otimizar recursos. No entanto, casos reportados de preconceito sugerem que certos grupos (ex., idosos ou minorias étnicas) podem ser desvalorizados, revelando a necessidade de calibrar permanentemente os modelos *(Obermeyer et al., 2019)*.

6.3. Telemedicina e Monitorização Remota

Com a chegada da telemedicina, a IA ganha relevo na monitorização domiciliária de pacientes crónicos, processando sinais vitais em tempo real e alertando o médico quando ocorrem desvios críticos *(OMS, 2021)*. Este modelo diminui reinternamentos e melhora o conforto do doente, mas exige elevada segurança de dados e protocolos de consentimento claros, visto que parte dos dados pode ser processada por terceiros *(Johnson et al., 2016)*.

7. Resultados da Análise

Com base na vasta literatura consultada e nos exemplos práticos relatados, emergem múltiplas constatações:

- Otimização da tomada de decisão: A IA desempenha um papel relevante no apoio diagnóstico e na personalização terapêutica, reduzindo frequentemente o tempo de resposta e a probabilidade de erro.
- Risco de falta de clareza e preconceito: A explicabilidade limitada dos sistemas e a presença de dados não representativos continuam a pôr em causa a confiança na IA, requerendo sistemas de auditoria e validação constantes.
- Quadro legal em evolução: RGPD e EU AI Act fornecem diretrizes fundamentais, mas a sua concretização prática depende de regulamentações técnicas adicionais e de monitorização ativa por parte das autoridades competentes.
- Formação e cultura organizacional: A literacia digital do corpo clínico e dos gestores de saúde aparece como eixo crucial para uma adoção ética e responsável, assegurando que os algoritmos servem de complemento e não de substituto ao raciocínio clínico.

- Integração humanista: A IA pode libertar os profissionais de tarefas repetitivas, mas não deve suplantar a dimensão relacional e empática do cuidado, na qual reside a essência da prática médica.
- Responsabilização partilhada e rastreabilidade: Em caso de erros ou danos decorrentes da utilização de algoritmos, torna-se essencial determinar a parcela de responsabilidade de cada interveniente – desde o programador até à instituição de saúde e ao próprio profissional –, garantindo registos de decisão e mecanismos de auditoria que facilitem a investigação e corrijam eventuais falhas.
- Transparência e explicabilidade como fator de confiança: A adoção de metodologias de *explainable AI* e de práticas de auditoria independente permite ao clínico – e ao próprio paciente – compreender de forma acessível as sugestões geradas pelo sistema. Este reforço na transparência é fundamental para assegurar a confiança e salvaguardar a autonomia decisória na prática clínica.

8. Discussão

A aplicação da Inteligência Artificial (IA) em saúde, como se verificou ao longo deste artigo, traz oportunidades promissoras para agilizar o diagnóstico, orientar a escolha de tratamentos e até permitir a monitorização remota de pacientes. Ao processar grandes quantidades de dados clínicos, algoritmos de *machine learning* e *deep learning* detetam padrões e correlações que podem escapar ao escrutínio humano, sobretudo em contextos de elevada complexidade e volume de informação *(Amaro, 2022; Benke & Benke, 2018)*. Assim, há uma expetativa de que a IA seja capaz de reduzir erros, acelerar tomadas de decisão e otimizar a alocação de recursos, enquanto promove uma medicina mais personalizada *(Topol, 2019)*.

No entanto, a adoção desses algoritmos no dia a dia clínico desperta também importantes preocupações éticas, jurídicas e sociais. A denominada 'caixa negra' algorítmica, por exemplo, representa uma das maiores incertezas, pois dificulta que os profissionais de saúde compreendam em detalhe as razões pelas quais o sistema emite uma determinada recomendação *(Raji et al., 2020)*. Na prática clínica, a capacidade de justificar claramente as intervenções é fundamental para manter a relação de confiança com o doente e para assegurar um consentimento informado efetivo *(Dias, 2020)*. Quando o algoritmo surge como uma entidade que sabe mais mas não consegue explicar como chegou a determinada conclusão, pode emergir um desfasamento entre a segurança aparente da máquina e a insegurança real do médico perante a pouca clareza do processo.

Este problema correlaciona-se, por outro lado, com a autonomia profissional e com a dignidade do paciente. Se o médico se vir pressionado a seguir a orientação do algoritmo mesmo quando a julga incompleta ou inadequada, poderá perder

parte do seu sentido de responsabilidade e de julgamento clínico *(Pereira, 2015)*. Num cenário extremo, a IA converter-se-ia em quem decide, enquanto o médico se tornaria um mero executor de instruções, o que não só contraria os princípios éticos clássicos (autonomia, beneficência, salvaguarda contra danos e justiça), mas também pode gerar riscos adicionais de erro, caso o algoritmo tenha sido treinado com dados pouco representativos ou viciados *(Barocas et al., 2019)*. Por conseguinte, a literacia digital dos profissionais de saúde ergue-se como fator determinante para harmonizar a adoção da IA com a salvaguarda da autonomia e da responsabilidade clínica *(Pedro et al., 2023)*.

Outra dimensão sensível nesta discussão é a transparência do algorítmico, que ameaça diretamente o princípio de justiça na prestação de cuidados. Alguns estudos evidenciam que algoritmos treinados sobre dados historicamente desequilibrados reproduzem ou intensificam disparidades, penalizando subgrupos populacionais *(Obermeyer et al., 2019)*. Quando aplicado à saúde, tal distorção pode resultar, por exemplo, na desvalorização de sintomas em grupos minoritários ou na sobrevalorização do risco para determinados perfis, conduzindo a decisões clínicas desproporcionadas ou discriminatórias. Fica claro, pois, a necessidade de recolha de dados mais abrangente e representativa, de metodologias de correção estatística e de auditorias independentes, de modo a garantir que o progresso tecnológico não amplifica injustiças sociais.

O Regulamento Geral sobre a Proteção de Dados (RGPD) (União Europeia, 2016) e o Regulamento (EU) 2024/1689 (EU AI Act) tentam responder a estes dilemas, impondo obrigações de transparência, robustez e supervisão humana a sistemas de IA considerados de alto risco, como é o caso da saúde *(Comissão Europeia, 2020; European Parliament, 2023)*. O RGPD protege a privacidade dos dados clínicos e pela autonomia do titular, enquanto o EU AI Act exige documentar o desenvolvimento e o funcionamento de algoritmos, assim como introduzir mecanismos de rastreabilidade e responsabilização. Contudo, a efetividade de tais diplomas depende de vários fatores, nomeadamente, a capacidade dos Estados-Membros para fiscalizar e sancionar violações, a adequação das empresas fornecedoras às regras impostas e a clareza das diretrizes técnicas que concretizam os princípios gerais (Dias, 2020).

Além disso, a literacia digital e a formação profissional contínua surgem como eixo transversal para gerir as complexidades da IA em saúde. Os médicos e enfermeiros necessitam não apenas de manusear a tecnologia, mas também de compreender as suas limitações e os possíveis erros sistemáticos, exercendo uma visão crítica sobre os resultados apresentados *(Gordete, 2024)*. Igualmente, o paciente deve saber que parte do seu cuidado é suportada por algoritmos, mantendo o direito de questionar e recusar, sempre que entenda que a solução algorítmica não atende ao seu contexto ou necessidades *(OMS, 2021)*.

Há também que referir a dimensão do consentimento informado. A medicina moderna exige que o doente seja esclarecido de forma clara sobre as hipóteses terapêuticas e os riscos envolvidos. Num ambiente em que a IA se torna cada vez

mais influente, é fundamental explicar, com simplicidade, até que ponto a decisão resulta de um cálculo automático, qual o grau de certeza do algoritmo e que outras alternativas existem *(Topol, 2019)*. A falta de transparência algorítmica pode comprometer esse consentimento, ao impedir o paciente de compreender minimamente a base das recomendações.

Além disso, a discussão não pode ignorar a eventual concentração de poder nas mãos de empresas tecnológicas que fornecem soluções de IA. Se grandes plataformas controlam a infraestrutura e a lógica dos algoritmos, os hospitais podem ficar reféns de modelos fechados, sem acesso suficiente para proceder a auditorias ou ajustar parâmetros ao contexto local *(Marelli et al., 2021)*. Tal cenário contraria o ideal de uma IA transparente e adaptada às reais necessidades dos sistemas de saúde, levantando questões políticas e económicas sobre a soberania dos dados e a regulação do mercado de inovação *(Freitas & Novais, 2018)*.

Por fim, destaca-se que a IA pode, em muitos casos, fortalecer a humanização ao libertar o profissional de tarefas burocráticas ou repetitivas, dedicando-lhe mais tempo para a escuta ativa e o diálogo com o doente *(Topol, 2019)*. No entanto, este ganho depende de um planeamento institucional que valorize a relação interpessoal e a empatias, evitando que a adoção da IA seja motivada apenas por critérios de custo-efetividade. Assim, a adoção responsável passa por uma visão holística, em que a tecnologia sirva para aprimorar e não para substituir a essência do ato terapêutico, permitindo que a prática médica evolua sem perder de vista o respeito pela dignidade e pelos direitos fundamentais de cada paciente.

Conclusão

A Inteligência Artificial na saúde constitui uma oportunidade excecional para elevar a qualidade dos cuidados médicos, tornando-os mais rápidos, precisos e personalizados. A capacidade de processar rapidamente quantidades massivas de dados e de extrair correlações complexas dá à IA um potencial significativo para melhorar o diagnóstico e o tratamento, contribuindo para uma medicina de precisão e para a otimização de recursos *(Rahmani et al., 2021)*. No entanto, a adoção irrefletida ou desregulada da IA pode colidir com princípios éticos basilares e ameaçar a integridade das decisões clínicas.

Ao longo deste artigo, analisaram-se as implicações da IA para a autonomia do profissional de saúde e para o consentimento informado do paciente, identificando-se um conflito entre a promessa de uma maior segurança terapêutica e a pouca clareza dos algoritmos *(Dias, 2020)*. A chamada 'caixa negra' algorítmica prejudica a capacidade de explicação que a medicina sempre valorizou: o doente tem o direito de saber, em termos acessíveis, as razões por detrás de uma intervenção. Se a IA inviabiliza essa explicação, pode comprometer a relação de confiança e o próprio princípio da autonomia.

Em sintonia com os princípios constitucionais e deontológicos, como a dignidade e a igualdade, observou-se que o desvio algorítmico tem potencial para prejudicar grupos vulneráveis, mantendo desigualdades ou subestimando sintomas específicos de determinada população *(Barocas et al., 2019; Obermeyer et al., 2019)*. Um dos papéis essenciais das autoridades reguladoras e das instituições de saúde consiste em implementar mecanismos de auditoria e monitorização contínua, com vista a detetar e corrigir desvios. Só desta forma se garante que a inovação tecnológica não contraria o princípio de justiça na distribuição de cuidados e na priorização de casos clínicos.

No plano jurídico, o Regulamento Geral sobre a Proteção de Dados (RGPD) e o Regulamento (UE) 2024/1689 (EU AI Act) estruturam um quadro inicial para tutelar direitos fundamentais e promover a segurança, a robustez e a transparência dos algoritmos. Contudo, a celeridade da evolução tecnológica e a complexidade das arquiteturas de IA demandam uma atualização frequente e a capacidade de os Estados-Membros aplicarem, de forma efetiva, as normas aprovadas *(Comissão Europeia, 2020; European Parliament, 2023)*. A responsabilização em caso de dano clínico, resultante de uma recomendação emitida por IA, permanece um tema em aberto, carecendo de aperfeiçoamento jurisprudencial e, possivelmente, de legislação específica que clarifique os deveres de cada interveniente *(Dias, 2020; Pereira, 2015)*.

Em termos de gestão, a formação contínua dos profissionais de saúde revela-se determinante: sem uma literacia digital robusta, o médico ou o enfermeiro arriscam a abdicar da análise crítica, tornando-se meros executores de diagnósticos algorítmicos *(Pedro et al., 2023)*. O paciente, por sua vez, merece ser informado de que parte do seu cuidado se apoia em IA, resguardando-se o seu direito de escolha e assegurando-se que mantém um papel ativo no processo decisório *(OMS, 2021)*. Assim, a cultura institucional deve promover uma integração equilibrada, em que a IA suporte, mas não substitua, a arte e a ciência do exercício médico, que se alicerçam na interação humana, na empatia e no raciocínio clínico contextualizado.

No horizonte futuro, a IA pode democratizar o acesso a determinados cuidados, se forem criadas condições para que regiões mais remotas ou hospitais de menor dimensão também beneficiem de sistemas de previsão e diagnósticos avançados. Contudo, sem políticas públicas que invistam em infraestruturas tecnológicas, formação e padronização de dados, a tendência pode ser a concentração de soluções sofisticadas em grandes centros urbanos, aprofundando desigualdades territoriais *(Benke & Benke, 2018)*. Daí a relevância de uma ação concertada, unindo governos, universidades, indústria e sociedade civil, de forma a evitar que a IA se torne um fator de exclusão em vez de um catalisador de progresso *(Freitas & Novais, 2018)*.

Em resumo, conclui-se que a integridade das decisões clínicas em com recurso da IA depende de três elementos principais:

1. Regulação contínua e dinâmica, que acompanhe a evolução tecnológica e defina com rigor os deveres de transparência, rastreabilidade e responsabilização das entidades que desenvolvem e implementam algoritmos de IA;
2. Formação e literacia digital, que capacite o profissional de saúde a interpretar e avaliar criticamente as recomendações algorítmicas, e que habilite o paciente a compreender o papel da IA no seu tratamento, mantendo intacto o princípio do consentimento informado;
3. Supervisão ética, que inclua auditorias independentes, métodos de transparência algorítmica e estratégias para corrigir desvios, garantindo a neutralidade (ou a maior imparcialidade possível) e a segurança dos sistemas.

A IA pode, efetivamente, reforçar a capacidade de diagnóstico e de intervenção, bem como proporcionar um uso mais racional dos recursos em saúde. Contanto que sejam acautelados valores fundamentais e regras bem definidas, a tecnologia não precisa de colidir com a relação médico-paciente, podendo antes valorizar a componente humanista do cuidado, libertando o profissional para a esfera empática e reflexiva *(Topol, 2019)*. Assim, a adoção da IA, em vez de ameaçar a integridade das decisões clínicas, pode constituir um fator de fortalecimento e atualização da prática médica, no quadro de um compromisso ético e legal rigoroso.

Referencias Bibliográficas

Abidi, S. R. (2019). Intelligent health data analytics: a convergence of artificial intelligence and big data. Healthcare Management Forum, 32(4), 178–182. Disponível em: https://doi.org/10.1177/0840470419846134.

Access Now (2018). Human Rights in the Age of Artificial Intelligence. Disponível em: https://nobias-project.eu/.

Adler, S. (2019). A Quick Guide to Artificial Intelligence (AI). Intelligent Automation Network. Disponível em: https://www.intelligentautomation.network/decision-ai/news/a-basic-guide-to-ai.

Agência para a Modernização Administrativa (2018). ESTRATÉGIA TIC 2020 – Estratégia para a Transformação Digital na Administração Pública.

Altran Group (2017). Maximizing Value from AI – The digital transformers' guide.

Amaro, E. (2022). Artificial intelligence and big data in neurology. Arquivos De Neuropsiquiatria, 80(5) suppl 1, 342–347. Disponível em: https://doi.org/10.1590/0004-282x-anp-2022-s139.

Australian Human Rights Commission, Gradient Institute, Consumer Policy Research Centre, CHOICE, & CSIRO's Data61 (2020). Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias - Technical Paper. Australian Human Rights Commission.

Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairness and Machine Learning. Disponível em: http://fairmlbook.org.

Benke, K. K., & Benke, G. (2018). Artificial intelligence and big data in public health. International Journal of Environmental Research and Public Health, 15(12), 2796. Disponível em: https://doi.org/10.3390/ijerph15122796.

Benzidia, S., et al. (2021). The Impact of Big Data Analytics and Artificial Intelligence on Green Supply Chain Process Integration and Hospital Environmental Performance. Technological Forecasting and Social Change, 165, 120557. Disponível em: https://doi.org/10.1016/j.techfore.2020.120557.

Bird, E., Fox-Skelly, J., & Jenner, N. et al. (2020). The ethics of artificial intelligence: Issues and initiatives. Panel for the Future of Science and Technology. European Parliamentary.

Canotilho, J., & Moreira, V. (1993). Constituição da República Portuguesa anotada (3.ª ed.). Coimbra: Coimbra Editora.

Center for the study of existential risk (2020). Risks from Artificial Intelligence. University of Cambridge. Disponível em: https://www.cser.ac.uk/research/risks-from-artificial-intelligence/

Cheatham, B., Javanmardian, K., & Samandari, H. (2019). Confronting the risks of artificial intelligence. McKinsey and Company.
Comissão Europeia (2020). Livro Branco sobre Inteligência Artificial – Uma abordagem europeia para a excelência e confiança. Bruxelas: Comissão Europeia.

Commissioner for Human Rights (2019). Unboxing Artificial Intelligence: 10 steps to protect Human Rights. Council of Europe.

Conn, A. (2017). How Do We Align Artificial Intelligence with Human Values?. Future of Life Institute.

COUTINHO, Diana (2023). O Consentimento Informado como Gerador de Responsabilidade Civil Médica. 1.ª ed. Coimbra: Editora d'Ideias.

Data Flair (2019). Beware! Criminals are using AI to steal your personal details.

Declaração Universal dos Direitos Humanos (1978). Diário da República, I Série A, n.º 57/78, de 9 de Março.

Deloitte AI and Analytics (2020). Human values in the loop. Design principles for ethical AI.

DIAS, Daniela Andreia Marques (2023). Telemedicina e Responsabilidade Civil Médica: Novos Desafios na Era da Saúde Digital. Dissertação de Mestrado, Faculdade de Direito da Universidade de Coimbra, Área de Especialização em Ciências Jurídico-Civilísticas/Menção em Direito Civil

Dias, P. W. d. O. (2020). Uso da inteligência artificial no diagnóstico e elegibilidade de pacientes para cuidados paliativos: limites éticos e jurídicos. Blucher Social Sciences Proceedings. Disponível em: https://doi.org/10.5151/ienbio-2019-enbio-gt-10.

Dong, J., Wu, H., Zhou, D., Li, K., Zhang, Y., Ji, H., ... & Liu, Z. (2021). Application of big data and artificial intelligence in covid-19 prevention, diagnosis, treatment and

management decisions in China. Journal of Medical Systems, 45(9). Disponível em: https://doi.org/10.1007/s10916-021-01757-0.

EC (2019). Relatório da Comissão ao Parlamento Europeu e o Conselho que avalia a coerência das abordagens adotadas pelos Estados.

EC (2020). Índice de Digitalidade da Economia e da Sociedade (IDES) de 2020: Portugal.

ENISA (2016). Definition of Cybersecurity: Gaps and Overlaps in Standardisation. European Agency for Network and Information Security.

European Parliament (2023). EU AI Act: first regulation on artificial intelligence. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

European Union Agency for Fundamental Rights (2019). Data quality and artificial intelligence - mitigating bias and error to protect fundamental rights.

Flick, U. (2008). Managing Quality in Qualitative Research. Qualitative Research Kit. SAGE Publications Ltd.

Foddy, W. (1993). Constructing Questions for Interviews and Questionnaires: Theory and Practice in Social Research. Cambridge University Press.

Freitas, P., & Novais, P. (2018). Inteligência Artificial e Regulação de Algoritmos, Ministério da Ciência, Tecnologia, Inovações e Comunicações, Brasil.

Friedman, B. M., & Nissenbaum, H. (1996). Bias in computer systems. ACM Transactions on Information Systems (TOIS), 14(3), 330–347.

Gordete, L. F. S. (2024). O papel de uma aplicação móvel no percurso de um utente cirúrgico. Dissertação (Mestrado) – ISCTE - Instituto Universitário de Lisboa, Lisboa.
Government Digital Service & Office for Artificial Intelligence (2019). Understanding Artificial Intelligence, Ethics and Safety. GOV.UK.

Government of Canada (2020). Responsible use of artificial intelligence (AI).
Ianni, M. et al. (2020). Fast and effective Big Data exploration by clustering. Future Generation Computer Systems, 102, 84–94.

Johnson, C., Badger, M., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. National Institute of Standards and Technology. Disponível em: https://doi.org/10.6028/NIST.SP.800-150.

Kolachalama, V. B., Singh, P., Lin, C. Q., Mun, D., Belghasem, M. E., Henderson, J. M., Francis, J. M., Salant, D. J., et al. (2018). Association of Pathological Fibrosis with Renal Survival Using Deep Neural Networks. Kidney International Reports, 3(2), 464–475. Disponível em: https://doi.org/10.1016/j.ekir.2017.11.002.

Kuiava, V. A., Kuiava, E. L., Chielle, E. O., & Syllos, R. (2021). Desenvolvimento de sistema estruturado com inteligência artificial para apoio no diagnóstico de patologias oftalmológicas mais relevantes. Clinical & Biomedical Research. Disponível em: https://doi.org/10.22491/2357-9730.109565.

Leslie, D. (2019). Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute.

Leslie, D., Rincón, C., Briggs, M., Perini, A., Jayadeva, S., Borda, A., Bennett, S. J., Burr, C., Aitken, M., Katell, M., Fischer, C. (2023). AI Ethics and Governance in Practice: An Introduction. The Alan Turing Institute.

Lovis, C. (2019). Unlocking the power of artificial intelligence and big data in medicine. Journal of Medical Internet Research, 21(11), e16607. Disponível em: https://doi.org/10.2196/16607.

Marelli, L., Testa, G., & Van Hoyweghen, I. (2021). Big Tech Platforms in Health Research: Re-purposing Big Data Governance in Light of the GDPR's Research Exemption. SSRN. Disponível em: https://doi.org/10.2139/ssrn.3712168.

Microsoft & Ernst & Young LLP (2020). Artificial Intelligence in the Public Sector, Portugal - How 213 Public Organizations Benefit from AI. EY.

Musikkanski, L., Rakova, B., Bradbury, J. et al. (2020). Artificial Intelligence and Community Well-being: A Proposal for an Emerging Area of Research. Int. Journal of Com. WB, 3, 39–55.

Nia, N. G., Kaplanoğlu, E., & Nasab, A. (2023). Evaluation of artificial intelligence techniques in disease diagnosis and prediction. Discover Artificial Intelligence, 3(1). Disponível em: https://doi.org/10.1007/s44163-023-00049-5.

NoBIAS (2020). Artificial Intelligence without Bias. Disponível em: https://nobias-project.eu/.

Obermeyer, Z., Emanuel, E. J. (2016). Predicting the Future—Big Data, Machine Learning, and Clinical Medicine. The New England Journal of Medicine.

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. Science, 366(6464), 447–453.
OpenAI. (2025). ChatGPT Disponível em: https://chat.openai.com

OMS (2021). Ethics and Governance of Artificial Intelligence for Health: WHO guidance. Genebra: OMS.

Pedro, A. R., Dias, M. B., Laranjo, L., Cunha, A. S., & Cordeiro, J. V. (2023). Artificial intelligence in medicine: A comprehensive survey of medical doctor's perspectives in Portugal. PLoS ONE, 18(9), e0290613.

PEIXOTO, Sara (2024). O Requisito da Atividade Inventiva da Invenção Patenteável e as Invenções Geradas por Inteligência Artificial. Coimbra: Almedina. (Coleção Monografias).

Pereira, A. G. D. (2015). Direitos dos Pacientes e Responsabilidade Médica. Coimbra: Coimbra Editora.

Pereira, M. J. E. (2024). O impacto da inteligência artificial na área da saúde. Dissertação (Mestrado) – ISCTE - Instituto Universitário de Lisboa, Lisboa.

Persing, C. (2018). "Ethics in Cyber Security: WWW in Reference to Cyber Security Does Not Mean What You Think!".

Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J.,

Theron, D., & Barnes, P. (2020). Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (pp. 33–44).
Rahmani, A. M., Azhir, E., Ali, S., Mohammadi, M., Ahmed, O. H., Ghafour, M. Y., … &

Hosseinzadeh, M. (2021). Artificial intelligence approaches and mechanisms for big data analytics: a systematic study. PeerJ Computer Science, 7, e488. Disponível em: https://doi.org/10.7717/peerj-cs.488.

Ramezani, M., et al. (2023). The Application of Artificial Intelligence in Health Policy: A Scoping Review. BMC Health Services Research, 23(1). Disponível em: https://doi.org/10.1186/s12913-023-10462-2.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 - Regulamento Geral sobre a Proteção de Dados (RGPD). Jornal Oficial da União Europeia

Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024 - (EU AI Act). Jornal Oficial da União Europeia.

Richie, C. (2022). Environmentally Sustainable Development and Use of Artificial Intelligence in Health Care. Bioethics, 36(5). Disponível em: https://doi.org/10.1111/bioe.13018.
Serviços Partilhados do Ministério da Saúde (SPMS) (2019). Inteligência Artificial na Saúde. Disponível em: https://www.spms.min-saude.pt/2019/04/inteligencia-artificial-na-saude/.

Soori, M., Arezoo, B., & Dastres, R. (2023). Artificial intelligence, machine learning and deep learning in advanced robotics, a review. Cognitive Robotics. Disponível em: https://doi.org/10.1016/j.cogr.2023.04.001.

Supriya, M., & Chattu, V. K. (2021). A review of artificial intelligence, big data, and blockchain technology applications in medicine and global health. Big Data and Cognitive Computing, 5(3), 41. Disponível em: https://doi.org/10.3390/bdcc5030041.

Thakur, S., Rim, T. H., Ting, D. S. J., Hsieh, Y., & Kim, T. I. (2023). Editorial: big data and artificial intelligence in ophthalmology. Frontiers in Medicine, 10. Disponível em: https://doi.org/10.3389/fmed.2023.1145522.

Thongprayoon, C., Kaewput, W., Kovvuru, K., Hansrivijit, P., Kanduri, S. R., Bathini, T., … & Cheungpasitporn, W. (2020). Promises of big data and artificial intelligence in nephrology and transplantation. Journal of Clinical Medicine, 9(4), 1107. Disponível em: https://doi.org/10.3390/jcm9041107.

Topol, E. (2019). Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again. Basic Books.

Vinuesa, R., et al. (2020). The Role of Artificial Intelligence in Achieving the Sustainable Development Goals. Nature Communications, 11(1), 233. Disponível em: https://doi.org/10.1038/s41467-019-14108-y.

Zhang, S., & He, (2020). Achieving the success of sustainability development projects through big data analytics and artificial intelligence capability. Sustainability, 12(3), 949. Disponível em: https://doi.org/10.3390/su12030949

Direito ao Esquecimento na Sociedade em Rede: Contexto das Plataformas Digitais

José Manuel Anjos Correia [204]

Resumo

O presente artigo explora o Direito ao Esquecimento na sociedade em rede, promovendo um enquadramento no tocante à sua evolução histórica e aplicação no ordenamento jurídico europeu e português. Com enfoque especial para os desafios de aplicação deste direito em contexto de plataformas globais, o presente artigo abordará os efeitos [adversos] para este direito, derivado essencialmente da descentralização da internet, da globalização das plataformas digitais, a replicação viral dos dados (ou efeito "Streisand") e o armazenamento em "*Cloud*" no contexto de transferência internacional de dados. Por último, é sublinhada a respetiva necessidade de harmonização jurídica, a nível global, entre outras, por forma a que se possa garantir de forma efetiva a aplicação eficaz do Direito ao Esquecimento.

Palavras-chave: Direito ao Esquecimento, Internet, Plataformas Globais, Globalização, RGPD.

[204] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Abstract
This article explores the Right to be Forgotten in the network society, providing a framework for its historical evolution and application in the European and Portuguese legal systems. With a special focus on the challenges of applying this right in the context of global platforms, this article will address the [adverse] effects on this right, derived essentially from the decentralisation of the internet, the globalisation of digital platforms, the viral replication of data (or 'Streisand effect') and cloud storage in the context of international data transfer. Finally, the need for legal harmonisation at a global level is highlighted, among other things, so that the effective application of the Right to be Forgotten can be guaranteed.

Keywords: Right to be Forgotten, Internet, Global Platforms, Globalisation, GDPR.

Introdução

A Sociedade em Rede é, nada mais, que o "*olhar sobre a Sociedade da Informação e do Conhecimento numa lógica de rede, isto é, focalizado na forma como a informação e o conhecimento se propagam, criam novas estruturas e interagem com as existentes*"[205].

Alicerçando o conceito da Sociedade em Rede com a globalização hoje vivida, denota-se que nos é trazida uma nova realidade em termos de processamento e veiculação de informação, com acesso e disseminação de informação à escala mundial em fração de segundos[206], podendo-se elencar este efeito aquando da caracterização da sociedade da informação em que hoje nos encontramos.

No sentido desta mais evoluída Sociedade em Rede (face à data de criação da sua definição), e dos contornos evolutivos que impactaram a reconhecida era digital[207], sendo esta a respetiva consequência direta da evolução da sociedade da informação e do conhecimento associada ao desenvolvimento tecnológico, reconhece-se que o contexto desta evolução nos levanta derivados problemas jurídicos. Isto porque, na era digital, da forma em que a conhecemos, é residual, ou até mesmo inexistente, a possibilidade de limitar a divulgação de, mas não se limitando, fatos e informações, na medida em que a informação é distribuída a uma velocidade, como referido acima, que poderá criar um conhecimento universal em meros segundos.

Saliente a esta velocidade da divulgação, a pegada digital[208] e os gigantescos bancos de dados que alimentam a internet, os quais podem ser consultados a qualquer momento, em qualquer época e por qualquer pessoa, resultam na eternização digital das divulgações dos tais fatos e informações.

No contexto descrito acima, é de fácil entendimento que alguns direitos inerentes ao indivíduo ficam quase que [se não mesmo] sonegados derivado dos avanços da Sociedade em Rede, promovido, essencialmente, pelo próprio avanço tecnológico.

Desde logo, o Direito ao Esquecimento neste contexto de Sociedade em Rede tem associado derivadas problemáticas, nomeadamente de: Como aplicar o Direito ao Esquecimento quando estamos perante um contexto de Plataformas Globais?

Neste sentido, e atento ao contexto de globalização vivido nos dias de hoje, não fará sentido que, também a nível global, seja promovida alguma coerência em

---

[205] Esta definição foi-nos introduzida por Manuel Castells como parte da sua análise da sociedade atual, intitulada de "*The Information Age*".

[206] Autor: SILVA, Marco Antonio Marques, em "Direito ao Esquecimento – Posicionamento Jurisprudencial Brasileiro", no "Direito à Verdade, à memória, ao esquecimento", AAFDL-2018, ISBN: 978-972-629-190-0. 2018.

[207] Designação dada à era que atravessamos devido à disseminação das novas tecnologias digitais e ao seu grande impacto em termos socioculturais. (https://apdsi.pt/glossario/e/era-digital/).

[208] "*(…) termo usado para descrever as atividades na internet ou em dispositivos registradas – e, portanto, rastreáveis – de uma pessoa específica*" (https://www.malwarebytes.com/pt-br/cybersecurity/basics/digital-footprint)

matéria de direito aplicável, neste caso focando especificamente no Direito ao Esquecimento já que todos somos titulares de dados pessoais? Talvez a globalização [neste caso em termos de aplicabilidade universal de certos direitos] possa ser a "cura" para os próprios efeitos adversos dela mesma.

Isto na medida em que o Direito ao Esquecimento na Sociedade em Rede, de uma forma resumida e crítica, parece ser um simples direito [escrito] inerente ao indivíduo, o qual comporta previsão/valoração legal, mas carece de valor aquando aplicado na realidade.

Deste modo, os objetivos principais inerentes ao desenvolvimento do presente estudo são a da clara definição do que é, e de que se poderá retratar, efetivamente, o Direito ao Esquecimento (ou "*Right to be Forgotten*", conforme inicialmente trazido a discussão) e identificação de alguns dos desafios associados à aplicabilidade deste direito, inerente aos titulares de dados pessoais, quando estamos perante um contexto de plataformas globais.

Assim, o presente estudo comporta uma importância significativa pois visa o abordar de temas que, apesar de discutidos, ainda se encontram no limbo do controverso e de má definição no contexto global. Neste sentido, a clarificação de conceitos, identificação de desafios tecnológicos e jurídicos e as propostas de solução a abordar resultarão em contribuições significativas para a sociedade, com especial enfoque no setor privado e academia.

Quanto à metodologia de investigação empregada, esta derivou da aplicação conjunta entre a metodologia dogmática [com especial aplicabilidade desta], exploratória e interdisciplinar, pois a complexidade dos temas a abordar leva-nos a que, para além de uma respetiva análise do ponto de vista jurídico e prático às normas legais, haja a respetiva necessidade de correlacionar esta interpretação legal com a interdisciplinaridade do tema a abordar (na medida em que entraremos no campo da tecnologia e da sua evolução), que terá, certamente, por consequência a identificação de um tema pouco explorado derivado da sua complexidade e, também, a atualidade.

Por fim, no tocante à coleta de dados, utilizou-se essencialmente a revisão bibliográfica sobre o direito ao esquecimento [tanto em termos históricos bem como a sua aplicabilidade na era digital], com especial enfoque para bibliografia que exponha, principalmente, os problemas associados a este direito quando estamos perante uma sociedade em constante desenvolvimento tecnológico. Neste sentido, teve-se, por base teórica, de um ponto de vista de construção no passado do direito à privacidade de hoje, o Artigo "*The Right to Privacy*", publicado por Samuel D. Warren e Louis D. Brandeis na revista *Harvard Law Review* de 1890 que, em complemento de várias decisões judiciais da altura, veio trazer uma clara forma de analisar o que se pode vir a desenvolver mais tarde como o direito à privacidade [que tem um relevo enorme no que hoje se pode considerar como o direito ao esquecimento, sendo que este tem por base os princípios fundamentais do "*right to*

be left alone"]. Num contexto mais atual, analisaram-se, essencialmente, as decisões promovidas no Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014, *Google Spain SL* e *Google Inc.* contra *Agencia Española de Protección de Datos* (AEPD) e *Mario Costeja González* e no Acórdão do Tribunal de Justiça (Grande Secção) de 24 de setembro de 2019, *Google LLC* contra *Commission nationale de l'informatique et des libertés* (CNIL), pois estes, para além de impulsionadores do direito ao esquecimento no contexto Europeu, também vieram criar alguns limites à sua extensão e aplicabilidade, tendo-se revelado bastante importantes para o dirimir de entendimentos distintos e clarificação de aplicabilidade deste direito.

1. Caracterização do direito ao esquecimento

A génese do direito ao esquecimento tem por base o princípio de factos ocorridos no passado que poderão produzir consequências negativas no futuro, nomeadamente por via da publicidade de certo tipo de informações que consubstanciariam, essencialmente, prejuízos, ou transtornos, ao lesado.

Nesta senda, o direito ao esquecimento que conhecemos nos dias de hoje adveio da necessidade de (i) fortalecimento da proteção do lesado [nomeadamente num contexto de extensão da garantia de privacidade]; e (ii) adaptação à sociedade em rede e ao ambiente digital.

Este direito, conforme já referido, adveio da necessidade da preservação da privacidade da pessoa humana. O primeiro abordar de um direito parecido ao direito ao esquecimento, mas ao qual este na sua formulação bebeu grande parte dos princípios estruturais, foi o "*right to be left alone*" concebido no artigo publicado na *Harvard Law Review* de 1890 pelos célebres Samuel D. Warren e Louis D. Brandeis. Neste artigo, essencialmente, estabeleceu-se o entendimento de que o indivíduo detinha um direito fundamental à sua privacidade e propriedade, tendo sido base de derivadas discussões que proporcionaram um desenvolvimento dos direitos individuais no contexto jurídico.

Na Europa, em 1983, foi proferida uma decisão pelo Tribunal de Última Instância de Paris (Mme. Filipachi Cogedipresse) onde, e no culminar das demais decisões dos tribunais que abordaram este mesmo tema, nasce um esboço mais claro do que conhecemos hoje em dia como o direito ao esquecimento. Expõe-se um breve trecho da decisão referida: "*(...) qualquer pessoa que se tenha envolvido em acontecimentos públicos pode, com o passar do tempo, reivindicar o direito ao esquecimento; a* ***lembrança*** *destes acontecimentos e do papel que ela possa ter desempenhado é* ***ilegítima se não for fundada nas necessidades da história ou se for de natureza a ferir sua sensibilidade****; visto que* ***o direito ao esquecimento****, que se impõe a todos, inclusive aos jornalistas,* ***deve igualmente beneficiar a todos****, inclusive aos condenados que pagaram sua dívida para com a sociedade e tentam reinserir-se nela*."[209] (OST, 2005, p. 160-161).

Derivado dos constantes desenvolvimentos tecnológicos e da massificação da utilização da internet, criaram-se diversos novos desafios que tiveram, em parte,

[209] Sublinhado e destacado nosso.

como consequência a maior atualidade de um direito ao esquecimento pois, hoje em dia, qualquer conteúdo publicado na internet [constituído por dados pessoais, ou não] é disponibilizado instantânea e permanentemente a nível mundial. Além disso, a utilização crescente das redes sociais promoveu a que haja uma maior e mais gravosa exposição dos utilizadores sem que estes tenham uma noção real da possível violação da sua intimidade.

Quando se concretiza o direito ao esquecimento, não o podemos desassociar do direito à reserva sobre a intimidade da vida privada [consagrado no ordenamento jurídico português, especificamente, no Artigo 80º do Código Civil], pois ambos residem por base na proteção da vida privada e intimidade das pessoas, aliadas à reabilitação e ressocialização do individuo [sendo que haveria uma dificuldade densa de tal acontecer caso houvesse um direito pleno de "lembrança", utilização e armazenamento].

Por último, na caracterização do direito ao esquecimento, podemos ainda concluir que este direito atua em duas frentes sendo elas o próprio direito a ser esquecido (ou "*droit à l´oubli*") e o direito ao apagamento (ou "*right to erasure*"). O que diferencia, essencialmente, estas duas frentes de aplicabilidade do direito ao esquecimento é que enquanto o direito a ser esquecido essencialmente colide com direitos fundamentais (com especial enfoque para o direito à liberdade de expressão e de informação), já o direito ao apagamento resulta numa simples necessidade de remoção ou eliminação dos dados pessoais fornecidos.

2. Direito ao Esquecimento no meio digital – Caso *Google Spain*

Em 2010, um cidadão espanhol, Mario Costeja Gonzáles, apresentou uma reclamação junto da Agência Espanhola de Proteção de Dados (AEPD) [a qual equivale à, hoje em dia, Comissão Nacional de Proteção de Dados (CNPD) em Portugal] contra a *Google Spain*, *Google Inc*. e o jornal *La Vanguardia,* pois aquando da pesquisa do seu nome no motor de busca da Google eram dados como resultados principais um anúncio de leilão público relacionado com dívidas ao fisco, e datado de 1998.

Contudo, essa divida estaria saldada junto da entidade competente há vários anos, mas a informação sobre tal situação mantinha-se disponível, para qualquer pessoa, na internet o que, segundo Mario Costeja, seria pejorativo da sua reputação pois não haveria mais relevância atribuível a tal informação.

Assim, o objetivo de Mario Costeja seria de que (i) em relação ao jornal *La Vanguardia*, fosse alterada ou suprimida a página onde constava o seu nome, por forma a que não fosse mais passível de aparecimento dos seus dados pessoais ou que este, aquando da divulgação em motores de busca, promovesse a utilização de ferramentas passiveis de obstar o acesso a essas informações; e (ii) em relação ao *Google* (*Spain* e *Inc*), houvesse a ocultação ou supressão das informações pessoais identificadores de Mario Costeja nos resultados de pesquisa em causa, o

que, consequentemente, resultaria na não associação às ligações relacionadas com o La Vanguardia.

A 30 de julho de 2010, pela AEPD, foi indeferida a reclamação no tocante à La Vanguardia, por consideração de legalidade na atuação e finalidade, e, contrariamente, foi deferida a reclamação no tocante à Google pois foi considerado pela AEPD que, na medida em que os operadores de motores de busca realizam tratamento dos dados [nomeadamente pessoais] resultante da sua atuação enquanto intermediários da sociedade da informação, estes estão intrinsecamente sujeitos à legislação, e demais, aplicável em matéria de proteção de dados pessoais.

Este assunto foi levado ao Tribunal de Justiça da União Europeia (TJUE) [Processo C-131/12] após suspensão da instância e submissão ao TJUE por parte da Audiência Nacional, resultante da apresentação de recurso por parte da *Google Spain* e *da Google Inc*, separadamente, junto deste órgão jurisdicional, na medida em que ambos os operadores se encontrariam inconformados com a decisão de deferimento do pedido de Mario Costeja por parte da AEPD.

Neste sentido, os temas principais que mereceram discussão e apreciação pelo TJUE foram (i) a respetiva responsabilidade dos motores de busca, e seus operadores, no tocante ao processamento de dados pessoais; (ii) a possibilidade dos indivíduos solicitarem a remoção, ou eliminação, de informações pessoais [incluindo os deus dados pessoais] dos resultados dos motores de busca quando essas informações se tornassem, essencialmente, irrelevantes e/ou desatualizadas e/ou prejudiciais à privacidade do individuo; e (iii) as linhas delimitadores entre o conflito de liberdade de informação aquando do "choque" com o direito à privacidade.

A 13 de maio de 2014, o TJUE pronunciou-se tendo considerado, essencialmente, que (i) os motores de busca [incluindo aqui os seus operadores] são responsáveis pelo tratamento dos dados pessoais pois, sendo que a sua atividade resulta numa ou de uma coleta, organização, armazenamento e disponibilização de tal informação ao público, esta atividade, nomeadamente nestes termos, enquadra-se no conceito de tratamento de dados pessoais; e (ii) apesar de não estarmos perante um direito absoluto, em determinadas circunstâncias [tais como em casos de informação divulgada que se encontre desatualizada, irrelevante, inadequada ou não consentida] o individuo, ou titular, ter o direito de solicitar a remoção dos resultados de busca dos motores, pois tais informações podem já não ser necessárias para o seu principal propósito (esgotamento da finalidade) e/ou afetam negativamente o direito de privacidade e proteção dos dados pessoais do individuo, ou titular.

Deste modo, ao ser chamado a pronunciar-se face à atividade dos motores de busca, o TJUE configura este direito ao esquecimento no meio digital como sendo um mecanismo de direito à autodeterminação pois permite um maior controlo sobre os dados pessoais por parte do titular, bem como a própria decisão de quais, e como, poderão ser consultados e tratados esses dados por terceiros.

Além disso, esta decisão do TJUE poderá considerar-se como sendo o primeiro caso a estabelecer formalmente o direito ao esquecimento no ambiente digital, promovendo os alicerces base para desenvolvimento dos trâmites e limites de tal direito, nomeadamente no tocante aquando da criação e previsão deste direito no atual Regulamento Geral de Proteção de Dados (RGPD).

3. O Direito ao Esquecimento no RGPD

Com traços de influência, positiva, retirados do Caso *Google Spain*, o efetivo direito ao esquecimento foi vertido inicialmente no RGPD, como sendo o direito ao apagamento dos dados ou «direito a ser esquecido».

Conforme vem previsto no nº 1 do Artigo 17º do RGPD, o titular dos dados pessoais pode, e tem o direito, de obter o apagamento dos seus dados pessoais, por parte do responsável pelo tratamento [tendo este o dever de apagar tais dados], sem demora injustificada quando se verifique, pelo menos, uma das seguintes situações: a) os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos da alínea a) do nº 1 do Artigo 6º do RGPD, ou da alínea a) do nº 3 do Artigo 9º do RGPD e se não existir outro fundamento jurídico para o referido tratamento; c) o titular opõe-se ao tratamento nos termos do nº 1 do Artigo 21º do RGPD, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do nº 2 do Artigo 21º do RGPD; d) os dados pessoais foram tratados ilicitamente; e) os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; ou f) os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no nº1 do Artigo 8º do RGPD.

Além disso, e conforme ao previsto no nº 1 do Artigo 17º do RGPD, vislumbra-se que, se viável/possível tendo em conta a tecnologia disponível e os custos da sua aplicação, o responsável pelo tratamento a quem foi solicitado o apagamento dos dados tem o dever de comunicar em cadeia tal pedido[210], por forma a promover uma ação em cadeia [ou seja, sem demora injustificada, procederem, também estes, ao apagamento (ou supressão) dos dados pessoais do titular que requereu o seu apagamento nos termos das alíneas do nº 1 do Artigo 17º do RGPD].

---

[210] Conforme se poderá denotar pelo previsto no Considerando (66) do RGPD: "*Para reforçar o direito a ser esquecido no ambiente por via eletrónica, o âmbito do direito ao apagamento deverá ser alargado através da imposição ao responsável pelo tratamento que tenha tornado públicos os dados pessoais da adoção de medidas razoáveis, incluindo a aplicação de medidas técnicas, para informar os responsáveis que estejam a tratar esses dados pessoais de que os titulares dos dados solicitaram a supressão de quaisquer ligações para esses dados pessoais ou de cópias ou reproduções dos mesmos. Ao fazê-lo, esse responsável pelo tratamento deverá adotar as medidas que se afigurarem razoáveis, tendo em conta a tecnologia disponível e os meios ao seu dispor, incluindo medidas técnicas, para informar do pedido do titular dos dados pessoais os responsáveis que estejam a tratar os dados*."

Contudo, o responsável pelo tratamento dos dados pessoais do indivíduo poderá opor-se, nos termos do nº 3 do Artigo 17º do RGPD, ao apagamento dos dados pessoais e do dever de comunicação em cadeia caso (i) estejamos perante o exercício da liberdade de expressão e de informação do responsável pelo tratamento [ou seja, o não apagamento terá de se demonstrar necessário para efetivação do exercício destas liberdades]; (ii) se demonstre necessário para efeitos de cumprimento de uma obrigação jurídica que exija esse tratamento; (iii) o responsável esteja ao abrigo do exercício de funções de interesse público ou esteja investido do exercício de autoridade pública; (iv) haja motivações maiores em termos de interesse público no domínio de saúde pública; (v) se demonstre necessário para fins de arquivo de interesse público, ou de investigação cientifica ou histórica ou para fins estatísticos; ou (vi) para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

No que toca à transposição do RGPD para o ordenamento jurídico português, o legislador efetuou-a através da Lei nº 58/2019, de 8 de agosto ("lei de execução"), a qual tem por objeto o assegurar da execução, na ordem jurídica interna, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, doravante designado abreviadamente por Regulamento Geral de Proteção de Dados (RGPD).

Apesar de apenas vir prevista uma referência ao direito ao esquecimento, nesta exata redação, na lei de execução, o legislador acautelou alguns outros pontos para efetivação de tal direito aquando da referência ao direito ao apagamento (conforme também é referido de tal forma no RGPD).

Assim, e complementarmente ao já previsto no RGPD, o legislador português prevê mais alguns critérios e parâmetros na lei de execução:

- O exercício do direito de apagamento no que toca a dados de pessoa falecida pode ser exercido por quem esta haja designado para o efeito, ou, na falta de designação, pelos seus herdeiros (nº 2 do Artigo 17º da lei de execução);
- O direito de apagamento previsto no Artigo 17º do RGPD, quando se está perante um prazo de conservação imposto por lei, apenas poderá ser exercido após findo o respetivo prazo de conservação (nº 1 do Artigo 21º da lei de execução);
- O direito ao apagamento no tocante a dados pessoais publicados em jornal oficial comporta uma natureza excecional, pelo que apenas se poderá concretizar nos termos do previsto no Artigo 17º do RGPD, e apenas se essa for a única alternativa [ou seja, apenas se se revelar a imprescindibilidade da aplicação do direito ao esquecimento] e ponderados os demais interesses em presença [mais uma vez, o legislador deixa a análise para o caso em concreto, preferindo não assumir uma posição prévia que possa consistir numa colisão de direitos *à priori* de tal ponderação prévia a realizar];
- Além de tudo o referido, o legislador representa na lei de execução, também, um pendor criminal aquando da verificação de desobediência. Assim, é estabelecido no nº1 do Artigo 52º da lei de execução que "*Quem não cumprir as obrigações*

previstas no RGPD e na presente lei, depois de ultrapassado o prazo que tiver sido fixado pela CNPD para o respetivo cumprimento, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias", sendo que, conforme espelhado na alínea b) do nº 2 desse mesmo Artigo, o disposto enquanto punibilidade no nº1 poderá ser agravado para o dobro [ou seja, pena de prisão até 2 anos ou pena de multa até 240 dias] caso, após devidamente notificado para o efeito, o agente (ou neste caso o responsável pelo tratamento) não proceder ao apagamento ou destruição dos dados [salvo os casos em que tal é excecionado], ou findo o prazo de conservação fixado nos termos da lei de execução.

Para além da lei de execução, no que concerne especificamente ao direito ao esquecimento, a Assembleia da República decreta a Carta Portuguesa de Direitos Humanos na Era Digital ("Carta"), por via da Lei nº27/2021, de 17 de maio, a qual entrou em vigor 60 (sessenta) dias após a sua publicação.

Esta Carta, apesar de bastante criticada, trouxe, também, uma previsão especifica no que concerne ao direito ao esquecimento. Contudo, a redação acolhida pelo legislador no Artigo 13º da Carta não se poderá considerar como uma promoção inovadora de aplicabilidade de tal direito no ambiente digital, pois apenas traz à colação previsões que já se encontrariam consubstanciadas em Regulamento ou Lei especifica[211] (como é o caso do RGPD e da lei de execução).

4. Desafios de aplicação do Direito ao Esquecimento em contexto de Plataformas Globais

Apesar de tudo o referido acima, no tocante à proteção que é garantida aos titulares dos dados pessoais em Portugal e na Europa, a aplicação do direito ao esquecimento enfrenta diversos e complexos desafios práticos, técnicos e jurídicos, nomeadamente quando estamos perante um contexto de plataformas globais que operam em múltiplos territórios, sob diferentes ordenamentos jurídicos e com diferentes regras de aplicabilidade, essencialmente, relativas à proteção da privacidade, liberdade de expressão e da própria gestão ou tratamento dos dados [nestes casos estamos a ponderar em ordenamentos em que estas existem].

4.1. A Descentralização e Globalização

[211] Redação do Artigo 13º "Direito ao esquecimento" da Carta: "*1 - Todos têm o direito de obter do Estado apoio no exercício do direito ao apagamento de dados pessoais que lhes digam respeito, nos termos e nas condições estabelecidas na legislação europeia e nacional aplicáveis. 2 - O direito ao esquecimento pode ser exercido a título póstumo por qualquer herdeiro do titular do direito, salvo quando este tenha feito determinação em sentido contrário*."

A descentralização da internet e a globalização das plataformas digitais promovem um dos maiores, e atuais, desafios, nomeadamente, para a aplicabilidade do direito ao esquecimento.

Ao longo dos últimos anos, e aliado ao constante desenvolvimento de tecnologias e acesso às mesmas, as plataformas digitais [nas quais se incluem os motores de busca e as redes sociais] comportam um cada vez maior pendor global e dominam o ambiente digital a nível mundial. Estas plataformas armazenam e tratam dados, incluindo pessoais, dos seus utilizadores a nível mundial, sendo que os seus [ou subcontratados] centros e servidores de dados se encontram distribuídos por todo o globo. Deste modo, e derivado da descentralização e da globalização, estas plataformas não se encontram, de forma estática, sujeitas a um único conjunto de leis, pelo que, consoante o caso, a aplicabilidade do direito ao esquecimento poderá comportar uma maior dificuldade, ou até mesmo ser impossível.

Assim sendo, e na prática, caso um cidadão português, ou da UE, pretenda aplicar o seu direito ao esquecimento nos trâmites, nomeadamente, do Artigo 17º do RGPD, esse pedido [caso não haja outro tipo de convenção em contrário, nomeadamente por via da vinculação por parte da plataforma a garantir este direito ao utilizador/indivíduo pese embora não se encontra sujeita a qualquer jurisdição da UE] deverá ser atendido no espaço jurisdicional da UE, sendo que tal informação poderá ser mantida acessível noutras jurisdições fora da abrangência da UE.

O referido no parágrafo acima resulta da decisão proferida pelo TJUE, no âmbito do caso "*Google LLC vs. CNIL*", de onde se retiraram as conclusões de que o direito ao esquecimento, em âmbito de RGPD ou jurisdição individual dos Estados da União, se encontra restringido ao território da EU, não comportando [caso contratualmente não resulte o contrário], assim, aplicação a nível global[212].

Neste sentido, é de fácil entendimento que a ausência de um padrão internacional em termos de aplicação do direito ao esquecimento cria diversos cenários, e maioritariamente desiguais, dependendo da jurisdição competente. Ou

---

[212] Conforme resulta da decisão proferida neste caso:
"*Pelos fundamentos expostos, o Tribunal de Justiça (Grande Secção) declara:*
O artigo 12.º, alínea b), e o artigo 14.º, primeiro parágrafo, alínea a), da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, bem como o artigo 17.o, n.º 1, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46 (Regulamento Geral sobre a Proteção de Dados), devem ser interpretados no sentido de que, ***quando aceita um pedido de supressão de referências ao abrigo destas disposições, o operador de um motor de busca não tem de efetuar essa supressão de referências em todas as versões do seu motor, devendo fazê-lo nas versões deste que correspondem a todos os Estados-Membros, e isto, se necessário, em conjugação com medidas que, embora satisfaçam as exigências legais, permitam efetivamente impedir ou, pelo menos, desencorajar seriamente os internautas que efetuam uma pesquisa a partir do nome da pessoa em causa dentro de um dos Estados-Membros de, através da lista de resultados exibida após essa pesquisa, aceder às hiperligações que são objeto desse pedido***."

seja, esta falta de interoperabilidade jurídica no que concerne, para além do direito ao esquecimento, no que concerne aos direitos dos titulares dos dados pessoais resulta no comprometimento, gravoso, da capacidade do titular exercer os direitos que lhe deveriam ser inerentes [aqui no contexto dos conferidos pelo RGPD] de forma plena pois, para além de muitas jurisdições ainda não promoverem uma proteção, só que, equivalente à garantida na UE, a capacidade de imposição de decisões de autoridades nacionais, ou europeias, em jurisdições fora da UE permanece limitada por ilegitimidade.

4.2. O efeito Streisand

A internet, *per si*, comporta uma natureza viral [no sentido de propagação de informação], sendo esta característica um dos maiores obstáculos à aplicação do direito ao esquecimento. Isto porque, uma vez publicados ou divulgados os dados na internet, a replicação destes ocorre, advertida ou inadvertidamente, em múltiplos sites, fóruns, redes sociais, etc., tendo por consequência a quase, ou até mesmo, impossibilidade quando estamos no âmbito da garantia da remoção completa dos dados. Assim, a facilidade existente de replicação promove o cenário de insuficiência na abrangência do pedido a ser realizado pelo titular, pois não se poderá garantir, na sua plenitude, a respetiva identificação de quem, o quê ou onde se encontram os dados.

Esta replicação dos dados é muitas vezes mencionada como "*efeito Streisand*"[213], pois de forma inadvertida [como seja por via de tentar fazer valer os seus direitos] poder-se-á atrair mais atenção [havendo, também, um possível aumento no que toca à disseminação dos dados] sendo que o objetivo principal seria a remoção de determinados dados. Assim, e conforme vimos acima aquando referido o Caso "*Google LLV vs. CNIL*", sendo que os dados, mesmo após o pedido de remoção/apagamento podem continuar acessíveis em outros domínios (sejam eles de controlo direto ou fora do controlo dos operadores), esta situação consubstancia, também, um elevado desafio técnico e legal para as plataformas digitais.

Além disso, e por facto de haver jurisdições que ainda não reconhecem o direito ao esquecimento, e havendo a possibilidade de replicação ou acesso por utilizadores que se encontrem em tais jurisdições [sendo este um dos efeitos da descentralização da internet], a remoção/apagamento dos dados torna-se ainda mais complexo, nomeadamente quando a informação se torna viral.

---

[213] A atriz e cantora Barbara Streisand, em 2003, agiu judicialmente contra uma empresa vendedora de fotografias online e um fotógrafo derivado da publicação não autorizada da mansão da cantora. Previamente ao intentar da ação judicial, a fotografia da mansão da cantora apenas comportava seis *downloads* derivado dos termos em que tinha sido publicada, contudo, e após o conhecimento público e notoriedade do processo e "viralização" da situação, um mês após a distribuição do processo a fotografia já contava com mais de quatrocentos e vinte mil *downloads*. Deste modo, a tentativa de anonimato, por via judicial, criou uma situação incontrolável, e incalculável de replicação dos dados.

4.3. Soberania Digital – O Armazenamento em "*Cloud*"

O armazenamento de dados, tendencialmente pessoais, em "*Cloud*" ou nuvem, e a própria distribuição geográfica que é feita com os dados, levanta inúmeras questões e problemas relacionados no que de respeito diz à soberania digital.

Apesar das multas que podem ser aplicadas às plataformas digitais por forma a que as mesmas se coadunem com as garantias que devem ser promovidas aos titulares dos dados pessoais no âmbito do RGPD, a dispersão geográfica dos dados e a complexidade técnica das infraestruturas tecnológicas da nuvem, e os meios para o conseguir, tornam difícil que se possa concretizar uma remoção completa e em todos os locais dos dados que são submetidos a pedido de apagamento por via do Direito ao Esquecimento. Desde logo porque a nuvem tem como principal característica a replicação automática dos dados, para não falar dos derivados tipos de tratamento que podem ser realizados no âmbito deste armazenamento em nuvem, pois estes também promovem os "*data lakes*"[214] e métodos de processamento fundados em "*Big Data*".

Além disso, por forma a que as empresas consigam garantir uma infraestrutura sólida, nomeadamente em termos de "*backup*" da informação e redundâncias, poderá haver a necessidade de recorrer à transferência internacional de dados por forma a garantir determinado tipo de resiliência operacional. Nestes casos, e sempre que os países, ou alguns destes, para onde ocorrerá a transferência não estejam ao abrigo de decisão de adequação[215] promovida pela Comissão Europeia, há que garantir, do ponto de vista contratual, a respetiva salvaguarda dos direitos dos titulares dos dados, com especial ênfase para o direito ao esquecimento, pois, na medida em que alguns desses países podem comportar legislação menos rigorosa no tocante a estes direitos, a falta de rigor e harmonização internacional podem vir a resultar num impedimento de invocação e aplicabilidade plena dos direitos.

Neste contexto, a aplicabilidade do direito ao esquecimento encontra-se num ambiente bastante desafiante, se não hostil.

5. Considerações Finais

Apesar de muitos outros temas poderem ter sido abordados no presente estudo, na medida em que consubstanciam desafios, também bastante complexos, para

---

[214] Conforme nos dá a conhecer a própria Microsoft, "*Um data lake é um repositório centralizado que ingere e armazena grandes volumes de dados na sua forma original. Em seguida, os dados podem ser processados e utilizados como base para uma variedade de necessidades analíticas*".

[215] Decisão promovida pela Comissão Europeia que visa confirmar, do ponto de vista formal e com efeitos vinculativos para os países do Espaço Económico Europeu ("EEE"), que o nível de proteção de dados num país não pertencente ao EEE ou numa organização internacional é essencialmente equivalente ao nível de proteção no EEE. Ou seja, que garante, minimamente, o que visa garantir o próprio RGPD e demais legislação e regulamentação aplicável em termos de proteção de dados pessoais.

efeitos de aplicabilidade do direito ao esquecimento quando estamos perante um contexto de plataformas globais, podemos considerar, desde já, que este direito enfrenta desafios consideráveis que envolvem questões muito além de jurídicas [sendo elas também, e nomeadamente, técnicas e éticas].

Conforme se demonstrou, a falta de harmonização, previsão e reconhecimento global do direito ao esquecimento, a internet e a sua "viralidade" nesta nova conjuntura de sociedade em rede e os desafios técnicos e jurídicos relacionados com a remoção/apagamento dos dados geram uma dificuldade de aplicação uniforme deste direito.

Neste sentido, considera-se que apenas por via de uma real cooperação internacional, adoção de soluções técnicas eticamente desenvolvidas e criação de padrões globais de uniformização por forma a equilibrar, de forma justa, o direito à privacidade, liberdade de expressão e interesse público é que poderemos conseguir garantir uma eficácia plena do direito ao esquecimento.

Por fim, é passível e pacífico concluir que [alterando o "*Talvez*" para um "somente" e um "*possa*" para um "pode" de uma das partes da introdução do presente estudo] somente "*a globalização [neste caso em termos de aplicabilidade universal de certos direitos]*" pode "*ser a "cura" para os próprios efeitos adversos dela mesma*".

Referências bibliográficas

Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014. Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González. Pedido de decisão prejudicial apresentado pela Audiencia Nacional. Processo C-131/12. Disponível através do link: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62012CJ0131.

Acórdão do Tribunal de Justiça (Grande Secção) de 24 de setembro de 2019. *Google LLC* contra Commission nationale de l'informatique et des libertés (CNIL). Pedido de decisão prejudicial apresentado pelo Conseil d'État (França). Processo C-507/17. Disponível através do link: https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX:62017CJ0507.

AMORIM, Ianê Oliveira de, *O direito ao esquecimento e sua colisão com direitos fundamentais*. Dissertação realizada sob a orientação do Professor Jorge Barros Mendes - Mestrado em Administração Pública. Instituto Politécnico de Leiria. 2021.

ATAÍDE, Rui Paulo Mascarenhas, "Direito ao esquecimento". In:Cyberlaw, Vol. 1, nº7. 2019.
AWS – Amazon Web Services, "*O que é o armazenamento em nuvem?*". Disponível através do link: https://aws.amazon.com/pt/what-is/cloud-storage/.

EFING, Antônio Carlos; KIAME, Eduarda Alencar Maluf, "O direito ao esquecimento no armazenamento de dados: análise comparada entre o direito europeu e o direito brasileiro". In: 4º ANIVERSÁRIO DA RJLB (Palestras). 2020.

European Data Protection Board, "*Transferências internacionais de dados*". Disponível através do link: https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_pt.
KOCHARYAN, Hovsep; VARDANYAN, Lusine; HAMUĽÁK, Ondrej; KERIKMÄE, Tanel., "Critical Views on the Right to be Forgotten after the Entry into Force of the GDPR: Is it Able to Effectively Ensure our Privacy?". In: *International and Comparative Law Review*, vol. 21, no. 2, pp. 96–115. DOI: 10.2478/ iclr-2021-0015. 2021.

Lei n.º 27/2021, de 17 de maio - Carta Portuguesa de Direitos Humanos na Era Digital. Disponível através do link: https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2021-164870244.

Lei n.º 58/2019, de 8 de agosto - Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível através do link: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982.

MARTINS, Guilherme Magalhães, "Direito ao esquecimento na era da memória e da tecnologia". *In: Revista dos Tribunais* | vol. 1019/2020 | p. 109 - 153 | DTR\2020\8414. 2020.
Microsoft, "*O que é um Data Lake?*". Disponível através do link: https://azure.microsoft.com/pt-pt/resources/cloud-computing-dictionary/what-is-a-data-lake.

RAZNETAEVA, Yulia, "The right to Be forgotten in the European perspective". *In: sciendo*. 2020.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 - relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível através do link: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679.

SILVA, Marco Antonio Marques, "Direito ao Esquecimento – Posicionamento Jurisprudencial Brasileiro". *In: Direito à Verdade, à memória, ao esquecimento*, AAFDL-2018, ISBN: 978-972-629-190-0. 2018.

SINGER, Reinhard; BECK, Benjamin, "O "direito ao esquecimento" na internet: significado, efeitos e avaliação da "sentença Google" do Tribunal Europeu de 13 de maio de 2014". *In: Direitos Fundamentais & Justiça* | Belo Horizonte, ano 12, n. 39, p. 19-46, jul./dez. 2018.
SOLOVE, Daniel J., *The Legacy of Privacy and Freedom*. 1967.

STUARD, Ana Paula Didier; MARTINEZ, Luciano Martinez, *O direito ao esquecimento como direito fundamental nas relações de trabalho*. 2019.

TEIXEIRA, Rodrigo Valente Giublin; VILLA, Aline Dias, "Direito ao esquecimento na internet e os direitos da personalidade". *In: Revista Foco, Interdisciplinary Studies*. 2023.

TRIGUEIRO, Fábio Vinícius Maia, *Direito ao esquecimento na sociedade da informação*. In: Dissertação em Ciências Jurídico-Políticas – Menção em Direito Constitucional. Universidade de Coimbra. 2016.

WACHOWICZ, Marcos; LUZ, Pedro Henrique Machado da, "O direito à desindexação dos conteúdos ofensivos na internet". In: *Cyberlaw by CIJIC, Direito: a pensar tecnologicamente* | p. 40 – 61 | Edição n.º VI. 2018.

WARREN, Samuel D.; BRANDEIS, Louis D., "The Right to Privacy". *In: Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. 1890.

Concorrência Desleal: à luz dos Princípios Bíblicos

Mesla L. Bambi [216]

Resumo

Este artigo examina a concorrência desleal no âmbito empresarial, discutindo as suas implicações jurídicas e éticas à luz dos princípios bíblicos. A análise aborda práticas comerciais desonestas que comprometem a integridade do mercado e geram prejuízos a empresas concorrentes e consumidores. Além de explorar os instrumentos legais existentes para coibir essas práticas, o estudo enfatiza a relevância de valores como honestidade, justiça e respeito à dignidade humana, fundamentados nos ensinamentos bíblicos. A pesquisa conclui que a integração de princípios morais e mecanismos legais pode contribuir para um ambiente empresarial mais justo e sustentável, promovendo uma convivência harmónica entre os atores económicos.

Palavras-chave: Concorrência desleal, princípios bíblicos, Justiça social, Responsabilidade ética, Ambiente digital.

[216] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Abstract
This article examines unfair competition in the business environment, discussing its legal and ethical implications in the light of biblical principles. The analysis addresses dishonest business practices that compromise market integrity and generate losses for competing companies and consumers. In addition to exploring the existing legal instruments to curb these practices, the study emphasizes the relevance of values such as honesty, justice, and respect for human dignity, based on biblical teachings. The research concludes that the integration of moral principles and legal mechanisms can contribute to a fairer and more sustainable business environment, promoting a harmonious coexistence among economic actors.

Keywords: Unfair competition, biblical principles, Social justice, Ethical responsibility, Fair commercial practices, Digital environment.

Introdução

A concorrência, pilar essencial do funcionamento dos mercados, incentiva a inovação, a eficiência e o progresso económico. Contudo, quando pautada por práticas desleais, deixa de ser um instrumento de crescimento para se tornar uma ameaça à justiça, à ética e à dignidade humana. A concorrência desleal não é apenas uma afronta às normas jurídicas, mas também um desrespeito aos valores fundamentais que devem reger as relações humanas e comerciais.

Num mundo onde a busca pelo lucro por vezes ultrapassa os limites da ética, é imprescindível refletir sobre os princípios que orientam nossas interações comerciais. Os princípios bíblicos, alicerçados em valores como justiça, honestidade e respeito ao próximo, oferecem um caminho alternativo e inspirador para lidar com os desafios da concorrência desleal. Textos como (Provérbios 11:1; Balança enganosa é abominação para o Senhor, mas o peso justo é o seu prazer) e (Mateus 7:12; Portanto, tudo o que vós quereis que os homens vos façam, fazei-lho também vós, porque esta é a lei e os profetas) não apenas denunciam práticas fraudulentas, mas também orientam a construção de relações pautadas pela equidade e pela reciprocidade.

Historicamente, a concorrência desleal tem sido fonte de disputas económicas e jurídicas, gerando impactos significativos na estabilidade dos mercados e na confiança dos consumidores. Casos de falsificação, apropriação indevida de marcas e manipulação de preços evidenciam como essas práticas podem comprometer não apenas as relações comerciais, mas também os valores éticos que sustentam a convivência humana.

No cenário atual, onde a globalização e a revolução tecnológica ampliaram as possibilidades de interações comerciais, as práticas desleais assumiram novas formas e desafios. Plágios digitais, concorrência predatória em plataformas eletrônicas e estratégias de manipulação de mercado ilustram a urgência de se revisitar os fundamentos da ética nos negócios.

Este artigo busca analisar a concorrência desleal sob a luz dos princípios bíblicos, propondo uma reflexão que transcende as limitações do direito positivo. Ao integrar conceitos jurídicos com fundamentos éticos e espirituais, o estudo destaca que uma abordagem alinhada aos valores bíblicos pode não apenas mitigar as práticas desleais, mas também promover mercados mais justos e sustentáveis.

Num cenário global marcado por intensas disputas comerciais e frequentes casos de exploração, a análise da concorrência desleal através do prisma bíblico revela soluções inovadoras e humanitárias. A aliança entre os valores espirituais e as normas jurídicas pode transformar o mercado em um espaço onde não apenas o crescimento económico, mas também a justiça social e a integridade moral sejam prioridades. Esta abordagem oferece não só um modelo para resolver os conflitos existentes, mas também um caminho para evitar que as práticas desleais corroam as bases de um sistema económico saudável e humano.

Compreender os fundamentos teóricos da concorrência desleal é essencial para estabelecer as bases desta análise. Sob a luz dos princípios bíblicos e do enquadramento jurídico, exploraremos as raízes conceituais que sustentam o debate ético e social sobre práticas comerciais desleais.

1. Fundamentos Teóricos

A concorrência desleal é definida como qualquer prática comercial que desrespeite as normas de honestidade e transparência, prejudicando competidores ou consumidores. No âmbito jurídico, esse conceito é regulado em legislações nacionais e internacionais, como o Código da Propriedade Industrial e as diretrizes da Organização Mundial do Comércio (OMC). Essas normas buscam preservar a integridade do mercado, garantindo igualdade de condições para todos os participantes. Segundo (José de Oliveira Ascensão), "as práticas de concorrência desleal são todas aquelas que, violando o direito ou os bons costumes, prejudicam terceiros ou a livre concorrência" (ASCENSÃO, 2002). Além disso, Menezes Leitão (2005) complementa ao enfatizar que práticas desleais, como publicidade enganosa e difamação, não apenas ferem a ética, mas também violam direitos fundamentais dos consumidores.

Sob a ótica bíblica, a justiça e a honestidade são valores centrais que condenam práticas fraudulentas. Em (Provérbios 20:23, lemos: duas espécies de Peso são abomináveis ao Senhor, e balanças enganosas não são boas). Esse princípio reforça a necessidade de uma conduta ética nos negócios, promovendo o respeito ao próximo e a justiça em todas as relações.

Além disso, a Bíblia incentiva o trabalho honesto como uma forma de glorificar a Deus e contribuir para o bem comum. (Efésios 4:28 afirma: Aquele que furtava não furte mais; antes, trabalhe, fazendo com as mãos o que é bom, para que tenha o que repartir com o que tiver necessidade). Esse ensinamento destaca a importância de uma conduta ética que beneficie não apenas o indivíduo, mas toda a sociedade.

Compreender os fundamentos teóricos é essencial para estabelecer uma base sólida para a análise da concorrência desleal, especialmente ao explorar suas implicações no campo ético e bíblico.

1.1. Análise da Concorrência Desleal no Campo Ético e Bíblico

A concorrência desleal desafia diretamente os princípios éticos fundamentais que deveriam reger as interações humanas e comerciais. Sob a ótica ética, essas práticas violam valores como justiça, honestidade e equidade, prejudicando não apenas os concorrentes diretos, mas também consumidores, trabalhadores e o mercado como um todo. No campo bíblico, tais práticas não apenas configuram uma transgressão ética, mas também um pecado contra Deus e contra o próximo.

Do ponto de vista ético, a concorrência desleal compromete a confiança, elemento essencial para o funcionamento saudável de qualquer mercado. Quando

empresas recorrem a práticas como plágio, dumping ou manipulação de informações, criam um ambiente de desconfiança que desestimula a inovação e prejudica a livre concorrência. A ética empresarial exige transparência, respeito às normas e um compromisso com o bem comum, valores que muitas vezes são negligenciados em contextos de concorrência desleal.

Na perspetiva bíblica, a concorrência desleal é explicitamente condenada como uma forma de desonestidade. (Provérbios 11:1 afirma: "Balança enganosa é abominação para o Senhor, mas o peso justo é o seu prazer.") Este versículo não apenas denuncia práticas comerciais injustas, mas também reflete o compromisso divino com a justiça e a equidade. A Bíblia constantemente exorta os fiéis a agirem com honestidade em todas as áreas da vida, incluindo nos negócios. (A Carta Encíclica *Mater et Magistra*, 1961) reforça esses valores, afirmando que "as relações econômicas devem ser baseadas na justiça e no bem comum, garantindo que nenhuma prática cause danos aos mais vulneráveis." Esses princípios éticos são essenciais para orientar práticas empresariais justas e responsáveis.

Além disso, a concorrência desleal contradiz o mandamento de amar ao próximo como a si mesmo. A partir dos fundamentos éticos e bíblicos, é crucial aprofundar a discussão sobre como a concorrência desleal impacta diretamente a dignidade humana, um valor central nas Escrituras.

1.2. Concorrência Desleal como Violação da Dignidade Humana: Perspetiva Bíblica

A concorrência desleal vai além de uma simples prática comercial injusta; ela representa uma violação direta da dignidade humana. Quando empresas recorrem a práticas fraudulentas ou predatórias para alcançar vantagens competitivas, os impactos se espalham por toda a cadeia de relações, prejudicando trabalhadores, consumidores e a sociedade como um todo.

Do ponto de vista bíblico, a dignidade humana é um valor central que deve ser respeitado em todas as interações. Em (Gênesis 1:27, lemos que o ser humano foi criado à imagem e semelhança de Deus, o que confere a cada pessoa uma dignidade intrínseca e inalienável). Assim, qualquer prática que explore ou desrespeite o próximo é uma afronta a esse princípio divino.

Práticas como falsificação de produtos, exploração de trabalhadores e manipulação de preços ilustram como a concorrência desleal pode degradar a dignidade humana. Por exemplo, a exploração de mão de obra infantil ou o pagamento de salários indignos são práticas que colocam o lucro acima do bem-estar humano, contrariando o mandamento de amar ao próximo como a si mesmo (Mateus 22:39).

Além disso, a Bíblia condena explicitamente práticas desonestas no comércio. (Provérbios 11:1 afirma: "Balança enganosa é abominação para o Senhor, mas o peso justo é o seu prazer"). Essa passagem não só denuncia a injustiça comercial, mas também reforça a importância da honestidade como uma virtude que dignifica

tanto quem pratica quanto quem é afetado. Como enfatiza a Carta Encíclica *Mater et Magistra* (1961), o progresso econômico deve ser guiado pela justiça social e pelo respeito à dignidade humana.

Do ponto de vista prático, combater a concorrência desleal exige não apenas a aplicação rigorosa de leis e regulamentos, mas também a promoção de valores éticos que priorizem o respeito à dignidade humana. A implementação de códigos de conduta nas empresas, baseados em princípios bíblicos como justiça e integridade, pode ser um passo significativo para transformar o mercado em um ambiente mais humano e justo.

Diante dessa violação, surge o papel transformador da comunidade cristã na promoção de mercados mais justos e éticos, alinhados aos ensinamentos bíblicos.

2. O Papel da Comunidade Cristã na Promoção de Mercados Justos

A comunidade cristã tem uma responsabilidade única na construção de mercados justos e sustentáveis, com base nos princípios bíblicos de honestidade, equidade e respeito ao próximo. Ao longo da história, grupos cristãos têm sido pioneiros em iniciativas que promovem a justiça social e econômica, como o movimento de comércio justo e o desenvolvimento de cooperativas baseadas na solidariedade.

O conceito de ("amar ao próximo como a si mesmo" Mateus 22:39) serve de fundamento para a atuação cristã no mercado, incentivando relações comerciais que priorizem o bem comum em vez do lucro a qualquer custo. Por meio de programas de educação ética, campanhas de conscientização e apoio a práticas empresariais justas, a comunidade cristã pode ser um agente de transformação significativa no mercado.

A Encíclica *Mater et Magistra* (1961) enfatiza a importância da solidariedade cristã como um pilar para combater desigualdades econômicas e sociais.
Exemplos práticos incluem iniciativas de comércio justo, que garantem condições dignas para os trabalhadores e promovem a sustentabilidade econômica. Essas iniciativas não apenas combatem as práticas de exploração, mas também oferecem um modelo de mercado que reflete os valores do Reino de Deus. Além disso, igrejas e organizações cristãs podem atuar como mediadoras em casos de conflitos comerciais, promovendo a reconciliação e a justiça restaurativa.

Outro aspeto fundamental é a fiscalização e o incentivo à transparência. A comunidade cristã pode exercer pressão sobre empresas e governos para que adotem práticas mais transparentes e responsáveis, denunciando abusos e exigindo que os valores de justiça e honestidade sejam respeitados.

Ao promover mercados justos, a comunidade cristã não apenas cumpre sua missão de testemunhar os valores do Reino, mas também contribui para a construção de uma sociedade mais justa e equitativa, onde a dignidade humana e o bem comum sejam prioridades.

Embora a comunidade cristã tenha um papel ativo, o surgimento de novas tecnologias trouxe desafios adicionais que precisam ser enfrentados com criatividade e valores sólidos.

3. A Tecnologia e o Ressurgimento de Novas Formas de Concorrência Desleal

A revolução tecnológica trouxe consigo novas possibilidades de interação comercial, mas também amplificou as formas de concorrência desleal. Práticas como manipulação de algoritmos, exploração de dados pessoais e fake reviews são exemplos claros de como a tecnologia pode ser usada de maneira antiética para obter vantagens competitivas.

Menezes Leitão (2005) alerta para os perigos da falta de fiscalização no ambiente digital, que favorece práticas como publicidade enganosa e exploração de dados dos consumidores.

Algoritmos de precificação, por exemplo, podem ser programados para ajustar preços com base em informações pessoais dos consumidores, explorando vulnerabilidades econômicas e criando uma desigualdade ainda maior no acesso a bens e serviços. Essa prática contraria princípios bíblicos como a equidade e a justiça, lembrados em (Provérbios 20:10; Pesos diferentes e medidas diferentes são abominação para o Senhor, tanto uma coisa como a outra).

As fake reviews, por sua vez, distorcem a perceção dos consumidores sobre produtos e serviços, prejudicando a concorrência justa e desrespeitando o princípio da verdade, central no ensinamento bíblico (João 8:32). Além disso, o uso de bots para manipular o mercado ou capturar dados de forma desonesta demonstra como a falta de ética na tecnologia pode comprometer a integridade dos mercados.

Para mitigar essas práticas, é essencial que empresas e reguladores invistam em medidas de transparência e responsabilização. Códigos de conduta voltados para o uso ético da tecnologia, além de regulações claras para o mercado digital, são passos fundamentais para criar um ambiente mais justo.

Por fim, a tecnologia também pode ser usada de forma positiva para promover a justiça e a equidade. Plataformas que valorizam a transparência, como marketplaces que destacam produtos de comércio justo, mostram que a inovação pode ser aliada da ética. Assim, ao alinhar os avanços tecnológicos com os valores bíblicos, é possível transformar o mercado digital em um espaço de respeito e prosperidade compartilhada.

Para lidar com os desafios tecnológicos e éticos, a justiça restaurativa emerge como uma solução prática e transformadora.

5. A Justiça Restaurativa como Solução para a Concorrência Desleal

A justiça restaurativa, tradicionalmente aplicada em contextos criminais, tem se mostrado uma ferramenta poderosa para resolver conflitos em diversas áreas, incluindo o ambiente empresarial. Quando aplicada à concorrência desleal, a justiça restaurativa oferece uma abordagem que vai além da mera aplicação de sanções legais, focando na reparação dos danos, na restauração das relações e na promoção de valores éticos.

Sob a perspetiva bíblica, a justiça restaurativa encontra fundamentos sólidos. Passagens como (Mateus 5:24, que orienta a reconciliação antes de apresentar ofertas a Deus) e (Zacarias 8:16, que incentiva o falar a verdade e o promover a paz, destacam a importância da restauração das relações rompidas). No contexto da concorrência desleal, isso implica criar um espaço onde empresas possam reconhecer suas falhas, reparar os danos causados e se comprometer a adotar práticas mais justas no futuro.

Na prática, a justiça restaurativa pode ser implementada por meio de processos de mediação, onde as partes envolvidas são incentivadas a dialogar e buscar soluções conjuntas. Por exemplo, uma empresa que tenha prejudicado concorrentes ao praticar dumping pode, através da mediação, negociar formas de compensar os danos, ajustar suas práticas comerciais e assumir compromissos éticos. (Ascensão, 2002) sugere que mecanismos de mediação e arbitragem podem ser ferramentas eficazes para solucionar conflitos e restaurar a confiança no mercado.

Além disso, a justiça restaurativa promove uma mudança cultural nas organizações, incentivando uma mentalidade de responsabilidade e transparência. Programas internos de ética empresarial, alinhados a valores bíblicos como honestidade e integridade, podem ser desenvolvidos para prevenir futuras infrações e fortalecer a confiança entre empresas, consumidores e sociedade.

Ao adotar a justiça restaurativa como solução para a concorrência desleal, não apenas os danos imediatos são tratados, mas também se constrói um ambiente empresarial mais justo e sustentável. Essa abordagem reflete os princípios de perdão, reconciliação e busca pelo bem comum, valores que estão no cerne da mensagem bíblica.

Além das soluções institucionais, o papel do consumidor, inspirado pelos valores bíblicos, é essencial para promover a justiça nas escolhas de mercado.

6. O Consumo como Ato de Justiça: Uma Perspetiva Bíblica

O poder de escolha do consumidor é um dos mais influentes fatores de regulação do mercado. Decisões de consumo podem incentivar ou combater práticas desleais, promovendo um mercado mais justo e ético. Sob uma perspetiva bíblica, o ato de consumir é também uma expressão de valores, e cada escolha reflete princípios de

justiça, solidariedade e respeito ao próximo. A Encíclica *Mater et Magistra* (1961) reforça essa ideia ao afirmar que consumidores têm o dever moral de apoiar práticas comerciais justas e responsáveis.

A passagem de (Isaías 1:17, que clama: "Aprendam a fazer o bem! Busquem a justiça, repreendam o opressor..."), pode ser aplicada ao contexto do consumo consciente. Ao evitar empresas conhecidas por práticas exploratórias, como trabalho infantil ou condições desumanas de trabalho, os consumidores exercem um impacto positivo no mercado, exigindo ética e responsabilidade das corporações.

A Bíblia também enfatiza a importância de cuidar dos mais vulneráveis. Em (Provérbios 31:9, lemos: "Defenda os direitos dos pobres e necessitados"). Isso pode ser traduzido no consumo, apoiando iniciativas como o comércio justo, que garante condições dignas para os trabalhadores e promove a sustentabilidade econômica.

Práticas como boicotes às empresas que violam direitos humanos e o apoio a produtores locais são formas concretas de transformar o consumo em um ato de justiça. Por exemplo, ao escolher produtos oriundos de cooperativas que respeitam os princípios bíblicos de honestidade e equidade, o consumidor contribui para a redução das práticas de exploração.

Além disso, as escolhas de consumo podem influenciar positivamente as políticas empresariais. Empresas são incentivadas a adotar práticas mais transparentes e sustentáveis ao perceberem que os consumidores priorizam valores éticos em detrimento de preços baixos. Essa transformação reflete os princípios de (Amós 5:24: "Antes, corra a retidão como um rio, a justiça como um ribeiro perene").

A comunidade cristã desempenha um papel importante ao educar seus membros sobre o impacto das escolhas de consumo. Campanhas de conscientização realizadas por igrejas e organizações baseadas na fé podem capacitar as pessoas a alinharem suas decisões de compra aos valores do Reino de Deus, promovendo não apenas a justiça econômica, mas também a restauração social. Em síntese, consumir é mais do que uma atividade econômica; é um ato moral e espiritual. Ao escolher conscientemente, os consumidores podem contribuir para a construção de um mercado mais justo, que reflita os valores de justiça e solidariedade ensinados pela Bíblia.

Contudo, a transformação individual deve ser acompanhada pela análise crítica de estruturas predatórias que perpetuam a concorrência desleal a nível global.

7. Concorrência Predatória e o 'Pecado Estrutural' no Mercado Global

A concorrência predatória representa uma das formas mais agressivas e prejudiciais de práticas desleais no mercado global. Caracteriza-se por estratégias como dumping, manipulação de preços e práticas monopolistas, que têm como objetivo eliminar competidores e consolidar o domínio de mercado. Tais práticas não apenas

afetam concorrentes, mas também causam danos profundos a trabalhadores, consumidores e economias locais.

Como afirma Ascensão (2002) "a concorrência predatória destrói a base da competição leal e prejudica o bem-estar coletivo"). Patrício Jorge (2005) também observa que tais práticas aprofundam desigualdades e enfraquecem as economias locais.

Na perspetiva bíblica, essas práticas podem ser entendidas como manifestações do que se denomina "pecado estrutural" — uma forma de pecado que transcende o indivíduo e se enraíza nas estruturas sociais e econômicas. Em (Eclesiastes 5:8, lemos: "Se você vir o pobre oprimido numa província, e a justiça e os direitos negados, não fique surpreso; pois um oficial é protegido por outro, e há ainda mais altos sobre eles). "Essa passagem reflete como sistemas injustos podem perpetuar a opressão e a desigualdade.

As estruturas econômicas globais frequentemente incentivam comportamentos predatórios, criando um ambiente onde o lucro a qualquer custo é priorizado em detrimento da ética e do bem comum. Exemplos disso incluem a exploração de mão de obra barata em países em desenvolvimento, a destruição ambiental em nome do progresso industrial e a manipulação de mercados financeiros para favorecer grandes corporações em detrimento de pequenas empresas.

A resposta a esse "pecado estrutural" exige uma transformação profunda das estruturas econômicas. A Bíblia oferece um modelo para isso, enfatizando a justiça e a equidade em passagens como (Amós 5:24: "Antes, corra a retidão como um rio, a justiça como um ribeiro perene."). A promoção de um sistema econômico justo envolve medidas como a regulamentação rigorosa de práticas predatórias, a criação de incentivos para comportamentos empresariais éticos e o fortalecimento de instituições que promovam a justiça.

Além disso, a comunidade cristã pode desempenhar um papel crucial ao denunciar estruturas injustas e pressionar por mudanças. Organizações baseadas na fé têm um histórico de liderança em movimentos de justiça social e econômica, promovendo iniciativas como comércio justo, boicotes a corporações antiéticas e campanhas por direitos trabalhistas.

Ao combater a concorrência predatória e trabalhar para a transformação de sistemas econômicos globais, é possível mitigar os efeitos do "pecado estrutural" e promover um mercado mais justo e sustentável. Essa abordagem não apenas beneficia indivíduos e comunidades, mas também reflete os valores do Reino de Deus, onde a justiça e a equidade são centrais.

Para enfrentar essas estruturas, é necessário investir em educação empresarial que promova práticas éticas e alinhadas aos princípios bíblicos.

8. Educação Empresarial com Base nos Princípios Bíblicos

A educação empresarial desempenha um papel fundamental na formação de líderes éticos e na promoção de uma cultura organizacional que priorize valores como justiça, honestidade e respeito ao próximo. Menezes Leitão (2005) argumenta que programas de educação empresarial devem incluir componentes éticos e sociais para garantir a formação de líderes íntegros.

Sob a perspetiva bíblica, a liderança não é apenas uma questão de autoridade, mas também de serviço ao bem comum. (Marcos 10:43-44 ensina: "Quem quiser tornar-se importante entre vocês deverá ser servo, e quem quiser ser o primeiro deverá ser escravo de todos (…)".

A integração dos princípios bíblicos na educação empresarial pode transformar a maneira como as empresas operam e interagem com o mercado. Programas de formação que incentivem a responsabilidade social, a transparência e a sustentabilidade são essenciais para criar um ambiente corporativo mais justo e equilibrado. Por exemplo, iniciativas de treinamento em ética empresarial que se baseiem em textos como (Provérbios 16:11 "Pesos e balanças honestos vêm do Senhor; todos os pesos da bolsa são feitos por ele") podem ajudar líderes a tomarem decisões justas em seus negócios.

Além disso, o ensino sobre a importância do respeito aos direitos humanos e ao meio ambiente é vital para alinhar as práticas empresariais aos valores do Reino de Deus. Cursos e seminários que abordem temas como comércio justo, inclusão social e práticas de sustentabilidade podem equipar líderes com as ferramentas necessárias para enfrentar desafios éticos no mercado global.

O papel da comunidade cristã é crucial na promoção da educação empresarial com base nos princípios bíblicos. Igrejas e organizações baseadas na fé podem desenvolver materiais educativos, oferecer programas de mentoria e criar redes de apoio para empresários que desejam operar de maneira ética e responsável. Essas iniciativas não apenas fortalecem as capacidades individuais, mas também incentivam a criação de redes de negócios comprometidas com a justiça e a equidade.

Em última análise, a educação empresarial fundamentada nos princípios bíblicos oferece uma visão transformadora do mercado, onde o sucesso não é medido apenas pelo lucro, mas pelo impacto positivo na sociedade. Essa abordagem não apenas contribui para um ambiente corporativo mais ético, mas também reflete os valores de serviço, justiça e amor ao próximo, que são centrais na mensagem bíblica.

A educação empresarial deve também abranger os desafios éticos no ambiente digital, onde práticas desleais e omissões são amplificadas pela tecnologia.

9. Concorrência Desleal no Ambiente Digital e o Pecado da Omissão

O ambiente digital transformou profundamente a dinâmica da concorrência global, criando oportunidades e desafios inéditos. Com o advento de tecnologias como inteligência artificial, big data e algoritmos avançados, empresas têm encontrado maneiras de otimizar suas operações e alcançar novos mercados. No entanto, o mesmo ambiente que promove a inovação tem sido palco para práticas desleais, como manipulação de algoritmos, uso de dados pessoais sem consentimento e disseminação de desinformação para obter vantagem competitiva.

Do ponto de vista bíblico, a omissão diante dessas práticas pode ser considerada um pecado tão grave quanto a própria prática da deslealdade. (Tiago 4:17 afirma: "Portanto, aquele que sabe que deve fazer o bem e não o faz comete pecado"). Empresas que se beneficiam de práticas antiéticas no ambiente digital, mesmo que de forma indireta, compartilham a responsabilidade pelos danos causados.

Um exemplo claro é o uso de fake reviews para manipular a perceção dos consumidores sobre produtos ou serviços. Essas práticas não apenas prejudicam concorrentes, mas também violam a confiança do consumidor, que é um valor fundamental tanto no comércio quanto nos princípios bíblicos de honestidade e transparência (Provérbios 12:22: "Os lábios mentirosos são abomináveis ao Senhor, mas os que agem fielmente são o seu deleite").

Outro aspeto crítico é a coleta e o uso indevido de dados pessoais, uma prática amplamente difundida no ambiente digital. A ausência de transparência e consentimento nessas ações pode ser vista como uma forma de exploração, contrariando o princípio bíblico de respeito à dignidade humana. (Efésios 4:25 instrui: "Por isso, deixando a mentira, fale cada um a verdade com o seu próximo, porque somos membros uns dos outros (…)"

Para combater a concorrência desleal no ambiente digital e o pecado da omissão, é necessário um esforço coletivo que envolva empresas, reguladores e consumidores. Empresas devem adotar práticas éticas, investindo em transparência e conformidade com normas legais, como o Regulamento Geral de Proteção de Dados (RGPD). Além disso, organizações baseadas na fé podem desempenhar um papel vital na conscientização sobre as implicações éticas das tecnologias digitais, incentivando uma abordagem responsável e justa.

Reguladores, por sua vez, têm a responsabilidade de estabelecer marcos legais claros que inibam práticas desleais no ambiente digital e garantam a proteção dos consumidores. A implementação de auditorias obrigatórias em sistemas de inteligência artificial e o fortalecimento de sanções para violações de privacidade são exemplos de medidas que podem criar um ambiente mais equilibrado e justo.

Finalmente, os consumidores também desempenham um papel crucial ao exigir maior transparência das empresas e ao optar por produtos e serviços de organizações que demonstrem compromisso com a ética e a responsabilidade. Campanhas educativas podem ajudar a fortalecer a capacidade dos consumidores de identificar e evitar práticas desleais no ambiente digital. A Encíclica *Mater et Magistra* (1961) destaca que a responsabilidade social no ambiente digital deve ser prioritária para evitar abusos e desigualdades. Em conclusão, a concorrência desleal no ambiente digital é um desafio complexo, que exige uma abordagem multifacetada para ser efetivamente combatida. Ao alinhar os avanços tecnológicos com princípios éticos e valores bíblicos, é possível criar um mercado digital mais justo e respeitoso, onde o progresso e a inovação não sejam alcançados às custas da justiça e da dignidade humana.

Essas práticas digitais não apenas testam a integridade dos sistemas, mas também desafiam os indivíduos a demonstrar sua fé e princípios em um ambiente competitivo.

9.1. A Concorrência Desleal como um Teste de Integridade Cristã

A concorrência desleal não é apenas um desafio jurídico ou econômico, mas também um teste de integridade para aqueles que professam os valores cristãos. Diante de um mercado competitivo e frequentemente marcado por práticas antiéticas, os cristãos que atuam no ambiente empresarial enfrentam a constante tensão entre seguir os princípios bíblicos e ceder às pressões do mercado.

A integridade cristã é frequentemente destacada na Bíblia como um valor inegociável. (Provérbios 10:9 afirma: "Quem anda em integridade anda com segurança, mas quem segue caminhos tortuosos será descoberto"). Aplicar este princípio ao contexto empresarial implica tomar decisões que reflitam honestidade, justiça e respeito, mesmo quando tais escolhas pareçam desfavoráveis do ponto de vista financeiro ou competitivo.

O comportamento ético no mercado também reflete o testemunho cristão. (Mateus 5:16 encoraja: "Assim brilhe a luz de vocês diante dos homens, para que vejam as suas boas obras e glorifiquem ao Pai de vocês, que está nos céus"). Empresários e profissionais cristãos que escolhem agir com integridade, mesmo diante de práticas desleais, demonstram na prática os valores do Reino de Deus.

Práticas como o pagamento justo de salários, o respeito aos concorrentes e a transparência nos negócios não são apenas exigências legais, mas também manifestações de uma fé viva. Tais atitudes refletem o mandamento de amar ao próximo como a si mesmo (Mateus 22:39) e contribuem para a construção de um ambiente empresarial mais humano e justo.

Contudo, manter a integridade em um mercado que frequentemente recompensa a desonestidade pode ser desafiador. Para isso, é crucial que os cristãos busquem apoio em comunidades de fé e fortaleçam sua formação ética e espiritual.

Programas de mentoria, estudos bíblicos voltados para questões empresariais e a criação de redes de apoio entre empresários cristãos podem ajudar a sustentar a integridade mesmo em contextos adversos.

Além disso, a integridade cristã no mercado exige uma postura ativa contra práticas desleais. Denunciar injustiças, apoiar políticas que promovam a ética e incentivar outros a agirem com justiça são maneiras de alinhar a fé com a prática profissional. (Efésios 5:11 exorta: "Não participem das obras infrutíferas das trevas; antes, exponham-nas à luz." (Patrício Jorge, 2005) reforça que lideranças empresariais éticas têm o potencial de influenciar positivamente todo o mercado, promovendo valores cristãos na prática diária.

Em suma, a concorrência desleal desafia não apenas as normas do mercado, mas também os princípios éticos e espirituais de quem busca viver de acordo com os valores cristãos. Encarar este desafio com integridade é não apenas uma forma de resistir às tentações do mercado, mas também um poderoso testemunho da força transformadora do evangelho.

Diante desse teste de integridade, é essencial refletir sobre as consequências da concorrência desleal e buscar soluções éticas que beneficiem todos os envolvidos.

9.2. Reflexões Críticas sobre as Consequências da Concorrência Desleal e a Busca por Soluções Éticas

As consequências da concorrência desleal transcendem os prejuízos imediatos aos negócios diretamente afetados. Essas práticas criam um ambiente de desconfiança que enfraquece a credibilidade do mercado como um todo, desencorajando investimentos e inibindo a inovação. Além disso, consumidores acabam sendo privados de opções justas, pagando preços mais altos ou consumindo produtos e serviços de qualidade inferior.

Trabalhadores também sofrem, seja por meio de exploração direta, como salários injustos, ou pela redução de oportunidades de emprego devido ao fechamento de empresas éticas.

Na perspetiva bíblica, essas consequências são profundamente incompatíveis com os valores de justiça e equidade promovidos nas Escrituras. Textos como (Amós 8:4-6 denunciam aqueles que exploram os vulneráveis para obter ganho econômico: "Ouçam isto, vocês que esmagam os necessitados e arruínam os pobres da terra, dizendo: [...] reduziremos o peso e aumentaremos o preço, e enganaremos com balanças desonestas). Essas práticas não apenas prejudicam indivíduos, mas também corrompem as estruturas sociais, criando um ciclo de exploração e desigualdade.

A busca por soluções éticas deve começar com um compromisso renovado com a justiça e a transparência. Empresas têm a responsabilidade de adotar políticas que reflitam esses valores, como a implementação de códigos de conduta rigorosos e a promoção de práticas de governança corporativa que priorizem o bem comum. Reguladores devem atuar de forma proativa, criando e aplicando leis que inibam práticas desleais e promovam um mercado mais equilibrado. Menezes Leitão

(2005) propõe que sanções mais severas para práticas desleais podem desencorajar comportamentos prejudiciais, enquanto incentivos às boas práticas fortalecem o mercado.

Além disso, consumidores têm um papel fundamental ao demandar maior transparência das empresas e ao optar por produtos e serviços de organizações comprometidas com a ética. A Bíblia chama os indivíduos a "fazer o bem e buscar a justiça" (Isaías 1:17), um princípio que pode ser aplicado ao consumo consciente e à pressão por mudanças estruturais nos mercados.

Por fim, a comunidade cristã pode desempenhar um papel crucial na promoção de mercados éticos, defendendo valores de honestidade e equidade tanto no discurso público quanto em suas práticas individuais. Programas educativos, campanhas de conscientização e parcerias com organizações de comércio justo são exemplos de como a fé pode influenciar positivamente o ambiente econômico.

Em última análise, enfrentar as consequências da concorrência desleal exige uma abordagem holística que integre ética, legislação e espiritualidade. Ao alinhar as práticas de mercado com os valores bíblicos, é possível não apenas mitigar os danos causados por essas práticas, mas também criar um ambiente econômico mais justo e sustentável para todos.

Essas reflexões críticas apontam para a necessidade de propostas concretas que alinhem ética, sustentabilidade e os valores bíblicos em práticas empresariais.

10. Propostas para um Mercado Ético e Sustentável

A criação de um mercado ético e sustentável, que combata a concorrência desleal, requer a integração de valores bíblicos como justiça, honestidade e equidade nas práticas empresariais e regulatórias. A seguir, são apresentadas propostas específicas que combinam esses valores com estratégias práticas para transformar as interações comerciais:

1. **Adotar a Justiça como Base das Transações Comerciais**: Inspirados por passagens como (Amós 5:24 "Antes, corra a retidão como um rio, a justiça como um ribeiro perene"), os governos e as empresas devem implementar políticas que promovam a transparência e a equidade nas práticas comerciais. Isso inclui a criação de regulamentos que desestimulem práticas predatórias, como o dumping, e que exijam responsabilidade ética das empresas.
2. **Fortalecer a Educação Ética Empresarial**: (Provérbios 16:11 afirma que "Pesos e balanças honestos vêm do Senhor"). Assim, é essencial educar líderes empresariais sobre a importância de práticas honestas e justas no mercado. Programas de formação ética, baseados nos valores bíblicos, devem ser oferecidos em universidades, seminários e treinamentos corporativos, incentivando uma abordagem de liderança orientada pelo serviço ao próximo e pela justiça.

3. **Promover o Comércio Justo com Incentivos Fiscais**: O apoio a iniciativas de comércio justo, que assegurem condições dignas de trabalho e práticas sustentáveis, deve ser uma prioridade. Governos podem oferecer benefícios fiscais às empresas que seguirem diretrizes éticas e respeitarem os direitos dos trabalhadores, alinhando-se aos valores de dignidade humana presentes em (Gênesis 1:27, que enfatiza que todos foram criados à imagem de Deus).
4. **Incentivar Redes de Cooperação Empresarial Baseadas na Fé**: As comunidades de fé podem promover redes de apoio econômico que valorizem práticas comerciais éticas. Igrejas e organizações cristãs podem criar parcerias entre empresários comprometidos com os valores do Reino de Deus, incentivando uma economia baseada na confiança, na solidariedade e na justiça.
5. **Implementar Certificações Bíblico-Éticas**: A criação de selos de qualidade que representem o compromisso com os valores bíblicos de honestidade e equidade pode ajudar consumidores e investidores a identificar empresas éticas. Essas certificações podem incluir auditorias para garantir que práticas como transparência financeira e respeito ao meio ambiente sejam cumpridas.
6. **Combater o Pecado Estrutural por Meio de Reforma Legislativa**: Inspirados por (Isaías 1:17 "Aprendam a fazer o bem! Busquem a justiça, repreendam o opressor..."), legisladores devem trabalhar para desmantelar estruturas econômicas que incentivem a concorrência desleal. Isso inclui a revisão de leis que permitam monopólios e a implementação de regulamentos que protejam pequenas e médias empresas contra práticas abusivas.
7. **Conscientizar os Consumidores para o Consumo Responsável**: A educação do consumidor é crucial para promover escolhas éticas de consumo. As igrejas podem liderar campanhas de conscientização, incentivando fiéis a optarem por produtos e serviços de empresas que demonstrem compromisso com a justiça e a sustentabilidade. (Mateus 7:12, que ensina a fazer aos outros o que gostaríamos que nos fosse feito, é um princípio fundamental que deve nortear essas escolhas).
8. **Fomentar a Reconciliação em Casos de Concorrência Desleal**: A justiça restaurativa, amplamente defendida nas Escrituras, pode ser aplicada a disputas comerciais. Empresas que prejudicaram concorrentes devem ser incentivadas a reparar os danos por meio de acordos mediadores, promovendo a reconciliação e o restabelecimento da confiança.
9. **Criar Conselhos de Ética Empresarial Baseados em Princípios Bíblicos**: Conselhos de ética podem ser formados em organizações empresariais, compostos por líderes cristãos e especialistas, para orientar decisões estratégicas alinhadas aos valores bíblicos. Esses conselhos podem atuar na mediação de conflitos, na prevenção de práticas desleais e na promoção da justiça no mercado.

A educação também desempenha um papel crucial, tanto no desenvolvimento de líderes empresariais éticos quanto na formação de consumidores conscientes. Como ensina a *Mater et Magistra* (1961), "uma economia verdadeiramente justa deve ser construída sobre valores que respeitem a dignidade humana e o bem comum."

As propostas apresentadas reafirmam o compromisso com a justiça e a equidade, elementos centrais nas considerações finais deste estudo.

Considerações Finais

A concorrência desleal, ao ultrapassar os limites éticos e jurídicos, compromete não apenas o funcionamento saudável dos mercados, mas também os valores fundamentais que regem as relações humanas. Sob a luz dos princípios bíblicos, identificamos que práticas desonestas no ambiente comercial são mais do que uma violação das normas econômicas: representam uma afronta à dignidade humana e ao propósito divino de justiça e equidade. Ao longo deste artigo, foi evidenciado como a concorrência desleal pode assumir formas variadas e impactar profundamente todos os atores do mercado, desde consumidores até pequenas e grandes empresas. No entanto, os princípios bíblicos oferecem uma base ética sólida para reinterpretar e confrontar essas práticas, promovendo a honestidade, a transparência e a responsabilidade social como pilares fundamentais de um mercado mais justo e equilibrado.

A análise mostrou que a integração de valores espirituais e mecanismos jurídicos pode não apenas mitigar as consequências negativas da concorrência desleal, mas também transformar o mercado em um ambiente que reflita os valores do Reino de Deus. Iniciativas como a educação ética, a justiça restaurativa e o consumo responsável destacam-se como caminhos viáveis para reconstruir a confiança e a equidade nas interações comerciais. Ademais, as propostas apresentadas neste estudo — desde o fortalecimento de regulações até a criação de redes de cooperação empresarial baseadas na fé — demonstram que é possível alinhar práticas econômicas à busca por justiça social e integridade moral. Essas soluções, fundamentadas em ensinamentos bíblicos, não apenas oferecem alternativas para lidar com desafios atuais, mas também apontam para um futuro em que a prosperidade econômica e a justiça caminhem lado a lado. Conclui-se, portanto, que enfrentar a concorrência desleal à luz dos princípios bíblicos não é apenas uma necessidade ética e jurídica, mas também uma oportunidade de testemunhar valores que promovem a dignidade humana, a reconciliação e o bem comum.

O desafio está em transformar essas reflexões em ações concretas, capazes de influenciar positivamente o mercado global e de inspirar novas formas de convivência e cooperação econômica. Assim, este artigo reafirma a importância de unir fé e prática empresarial, demonstrando que os princípios bíblicos não apenas orientam o comportamento individual, mas também têm o poder de renovar estruturas económicas e sociais, tornando-as mais justas e sustentáveis para as gerações presentes e futuras.

Referências Bibliográficas

ASCENSÃO, José de Oliveira - *Concorrência Desleal*. Lisboa: Editora Almedina, 2002. ISBN 9789724016214.

BÍBLIA SAGRADA – *Provérbios 11:1; Mateus 7:12; Provérbios 20:23; Efésios 4:28; Géneses 1:27; Mateus 22:39; Provérbios 20:10; João 8:32; Mateus 5:24; Zacarias 8:16; Isaías 1:17; Provérbios 31:9; Amós 5:24; Eclesiastes 5:8; Marcos 10:43-44; Provérbios 16:11; Tiago 4:17; Provérbios 12:22; Efésios 4:25; Provérbios 10:9; Mateus 5:16; Efésios 5:11; Amós 8:4*.

LEITÃO, Menezes Adelaide - *Direito da Publicidade e Concorrência Desleal: um estudo sobre as práticas comerciais desleais*. *Direito Industrial*, Vol. IV. APDI, 2005. Almedina.

PAÚL, Patrício Jorge - *Concorrência Desleal e Direito do Consumidor*. *Revista da Ordem dos Advogados*, Ano 65, Vol. I, junho de 2005.

Referências Eletrónicas

Princípios Cristãos na Ética dos Negócios: https://biblechat.ai/pt/arquivo-de-perguntas/vida-crista/etica-moral/principios-cristaos-etica-negocios/. Acesso em: 10 jan. 2025.

Reflexões sobre a ética: https://ver.pt/reflexoes-sobre-a-etica/. Acesso em: [10 jan. 2025].

Jorge Patrício Paúl - Concorrência desleal e direito do consumidor: https://portal.oa.pt/publicacoes/revista-da-ordem-dos-advogados/ano-2005/ano-65-vol-i-jun-2005/doutrina/jorge-patricio-paul-concorrencia-desleal-e-direito-do-consumidor-star/. Acesso em: [19 jan. 2025].

Mater et Magistra**.** Encíclica do Papa João XXIII. Cidade do Vaticano, 15 de maio de 1961. Disponível em: http://www.vatican.va/content/john-xxiii/pt/encyclicals/documents/hf_j-xxiii_enc_15051961_mater.html

A impressão digital do culto religioso: da proteção jurídica da imagem dos menores online

Cláudia Alves Pratas [217]

Resumo

Num mundo em contínuo avanço científico e tecnológico, a Internet e o aparecimento das plataformas digitais apresentaram novos desafios aos Estados Democráticos e às sociedades, em geral. Toda a existência humana está hoje no mundo virtual. Dos atos mais simples do quotidiano às conquistas hercúleas – tudo é publicado nas redes sociais. E o fenómeno religioso segue esta tendência. O momento do culto religioso, circunscrito às paredes do local de culto até ao início do séc. XX, é hoje uma manifestação de fé com elevada projeção nas redes sociais. Mas como conciliar esta nova realidade com o direito à preservação da imagem dos menores? Qual o enquadramento jurídico aplicável? Como podem as igrejas e comunidades religiosas partilhar a fé nas redes sociais e, ainda assim, respeitar os direitos fundamentais dos seus membros? Estas são as questões a debater ao longo desta breve reflexão.

Palavras-chave: liberdade de culto; direitos de personalidade; direito à imagem; dados pessoais; menores.

[217] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Abstract
In a world of continuous scientific and technological advancement, the Internet and the advent of digital platforms have presented new challenges to Democratic States and societies in general. Today, all the human existence is shared in the virtual world. From the simplest everyday acts to the most herculean achievements – everything is posted on social media. And the religious phenomenon follows this trend. The moment of religious worship, confined to the walls of the place of worship until the beginning of the 21th century, is today a manifestation of faith with high projection on social networks. But how can we reconcile this new reality with the right to preserve the image of the minors? What is the applicable legal framework? How can the churches and religious communities share their faith on social media and still respect the fundamental rights of their members? These are the questions to be debated throughout this brief reflection.

Keywords: liberty of cult; personality rights; right to image's protection; personal data; minors

"E depois, um dia, ninguém mais
pediu licença. O direito da câmara foi
colocado acima de todos os outros direitos
e desde esse dia tudo mudou,
absolutamente tudo."
Milan Kundera, *A Imortalidade*.

Introdução

A Religião é tão antiga quanto o *primeiro homem*. Desde sempre o conhecimento e a conexão a um *Deus Criador* habitaram no coração do ser humano, que buscou, através de ritos e cultos religiosos, permanecer nessa ligação transcendente. E ainda hoje assim é. A condição única de *animal religiosum* confere ao ser humano a necessidade de caminhar na crença, seja ela qual for. Ainda que os últimos séculos tenham sido marcados pelos ventos laicos, soprando de formas díspares em conjunturas tão diversas, é inegável que o fenómeno religioso permanece vivo no coração do *homo religiosus*, com comprováveis influências civilizacionais (AGUTI, 2023; PRATAS, 2023).

Tanto no passado como no presente, o ser humano tem-se regido por convicções, pela crença e pela liberdade de a manifestar. E esta não é apenas uma questão religiosa ou moral; é uma questão jurídica. Afinal, a fé não só regimenta a esfera privada do *homo religiosus*, como também interfere na sua compreensão do mundo e no modo como se insere e procede na sociedade. Cumpre, tão somente, ao Estado de Direito proteger esta liberdade, aplicável a crenças teístas, não teístas, ateístas, agnósticas e todas as outras que exibem um pensamento transcendente do Universo e/ou um código de conduta (MOREIRA e GOMES, 2014). Como? Através de uma regulação jurídica da sociedade marcada pelo seu pluralismo religioso.

A República portuguesa, por via do art. 41.º, da Constituição da República Portuguesa de 1976 (CRP), apresenta-se como laica – reconhece a existência da Religião, mas apresenta uma neutralidade constitucional perante esta, no respeito pelo princípio da separação entre o Estado e a Igreja. Outra opção do legislador constitucional violaria os pilares de qualquer Estado de Direito Democrático. Tal neutralidade não pode, contudo, ser confundida com um total desinteresse por parte do Estado em relação a tudo o que concerne à esfera religiosa. Pelo contrário, cumpre-lhe o papel de guardião dos direitos fundamentais dos seus cidadãos no exercício das liberdades individuais de religião e de culto.

Numa era em que a Internet tem alcançado todas as esferas da sociedade, a Religião (igrejas e comunidades religiosas, entenda-se) soube tirar partido da rede global para cumprir as suas motivações missionárias, através da captação de imagens de ministros de culto e membros de confissões e consequente partilha nas várias plataformas digitais. Mas quais as repercussões legais do tratamento de dados pessoais decorrentes dos serviços religiosos (em concreto, da recolha, armazenamento e divulgação de imagens de menores não autorizadas)?[218] Este é o mote para uma breve reflexão sobre a necessidade da proteção da imagem dos menores online num contexto de culto religioso. Não se pretende, com esta partilha do pensamento científico, apresentar um panegírico à figura do serviço religioso em Portugal, mas entregar um breve contributo para debate, original em Portugal,

[218] Cfr. art. 4.º, n.º 2, REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (RGPD).

assente em pressupostos jurídicos, que coliga o Direito da Religião à necessidade da proteção dos dados pessoais[219] como resposta à problemática acima desenhada.

1. O direito à liberdade religiosa

O art. 41.º, CRP consagra, sob a epígrafe *liberdade de consciência, de religião e de culto*, o direito à liberdade religiosa individual e coletiva. A norma constitucional não se apresenta única, antes indo beber da inspiração de outros textos jurídicos internacionais cuja influência se tornou lei para o legislador constitucional na consagração do direito à liberdade religiosa, a saber: art. 18.º, Pacto Internacional dos Direitos Civis e Políticos (PIDCP), art. 13.º, n.º 3, Pacto Internacional dos Direitos Económicos, Sociais e Culturais (PIDESC), Declaração sobre a eliminação de todas as formas de intolerância ou discriminação baseadas na religião ou nas convicções, de 1981, art. 9.º, Convenção Europeia dos Direitos Humanos (CEDH) e art. 10.º, Carta dos Direitos Fundamentais da União Europeia (CFDUE).

A liberdade religiosa constitui-se como um direito fundamental, inserindo-se no elenco dos direitos fundamentais de regime constitucional reforçado: o dos direitos, liberdades e garantias (MIRANDA, 1986). Não se assemelha exagerado, pois, enquadrar tais liberdades no regime dos direitos, liberdades e garantias, tendo em consideração os dois elementos basilares que as caraterizam: 1) *elemento formal*, cuja localização sistemática enuncia o art. 41.º na Parte I, Título II da CRP; 2) *elemento material*, que revela uma posição subjetiva positivada numa norma de eficácia/aplicabilidade imediata, "a qual não depende da consecução de condições favoráveis do âmbito da realidade constitucional" (GOUVEIA, 2024, p. 363).

O Direito Constitucional (tal como o Direito Internacional dos direitos humanos) propõe, uma interpretação do direito à liberdade religiosa com um âmbito normativo alargado (ALEXY, 2006), isto é, enquanto direito fundamental deve ser interpretado extensivamente e as suas restrições devem ser excecionais, interpretadas de forma restritiva e devidamente fundamentadas, de acordo com o princípio da proporcionalidade (MACHADO, 2018).

Em traços lassos, o direito à liberdade religiosa postula-se como um conjunto de normas jurídicas que garantem ao cidadão a liberdade de ação de acordo com as suas convicções religiosas.

O objeto desta liberdade é triplo e inspirado no manto normativo da Declaração Universal dos Direitos Humanos (DUDH): a consciência, a religião e o culto, e abarca a "liberdade de mudar de religião ou crença e a liberdade de

[219] Nos termos do art. 4.º, n.º 1, RGPD as imagens (fotografia ou vídeo) constituem-se como dados pessoais, pois que se tratam de "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

manifestar essa religião ou crença, pelo ensino, pela prática, pelo culto e pela observância, em público ou em particular", de acordo com o art. 18.º, DUDH, aplicável por força do art. 16.º, n.º 2.

Se o n.º 1 do art. 41.º se apresenta, na letra de lei, fácil de assimilar quanto às liberdades por ele positivadas, o mesmo não se pode dizer da hermenêutica dos conceitos nele inscritos, pois que ultrapassam, e muito, o pêndulo jurídico. Não cumpre ao legislador abraçar tamanha tarefa de fixação terminológica – em primeiro lugar, porque num quadro de laicidade constitucional nenhuma significação conceptual seria suficientemente isenta e igualitária perante o pluralismo religioso que marca a sociedade portuguesa; em segundo lugar, porque a *Religião* não se define, antes resulta de um direito de autodefinição garantido pelo princípio da separação do Estado e das igrejas comunidades religiosas (art. 41.º, n.º 4, CRP e art. 3.º, Lei da Liberdade Religiosa – LLR). Ainda assim, julgamos ser necessário encontrar um critério geral de conceptualização (seja ele internacional ou nacional) que nos permita fazer um inequívoco enquadramento legal desta temática. Não é nosso apanágio apresentar aqui uma conceptualização dos mesmos – seria, certamente, uma tarefa despicienda tentar caraterizar, com este breve artigo, os conceitos extrajurídicos de 'consciência', 'religião' ou 'culto'[220]. Todavia, deixamos anotações explanatórias do elenco normativo que permitem ao leitor um entendimento primário dos bens jurídicos protegidos pelo art. 41.º.

A triplicidade do art. 41.º, n .º 1 abrange, neste sentido, direitos dissemelhantes, mas complementares. Todos eles assentam na liberdade de religião, intimamente conectada à liberdade de consciência e base da liberdade de culto:

i. O *direito à liberdade de consciência* consagra uma liberdade de escolha de convicções e/ou padrões éticos e morais. A consciência presenta uma dimensão axiológica mais ampla do que a religião, pois ultrapassa a valoração religiosa. Nas palavras de LEITE, "a consciência não tem necessariamente conotações religiosas, uma vez que pode basear-se simplesmente em princípios filosóficos ou éticos, sem fundamento propriamente religioso" (1978, p. 289);

ii. O *direito à liberdade de religião*, que contempla a liberdade de escolher (ou não escolher) uma religião, igreja ou comunidade religiosa, de optar por não ter uma religião, de defender uma ideologia religiosa ou antirreligiosa e o direito a não ser prejudicado pelas suas convicções (PRATAS, 2023);

---

220 Sobre a necessidade de aferir de um conceito jurídico de Religião: JÓNATAS MACHADO (1996). *Liberdade religiosa numa comunidade constitucional inclusiva. Dos direitos da verdade aos direitos dos cidadãos*. Coimbra: Coimbra Editora, pp. 208 e ss; CLÁUDIA ALVES PRATAS (2014). *Direito da Religião: a proteção jurídica das minorias protestantes*. Lisboa: Chiado Editora, pp. 17 e ss; DAVIDE ARGIOLAS (2017). *A responsabilidade civil extracontratual das entidades religiosas*. Coimbra: Faculdade de Direito da Universidade de Coimbra, pp. 189 e ss; JORGE BACELAR GOUVEIA (2024). *Direito da Religião. Laicidade, pluralismo e cooperação nas relações Igreja-Estado*. Lisboa: Almedina, pp. 37 e ss.

iii. O *direito à liberdade de culto*, a face mais visível do fenómeno religioso que permite ao crente a prática de atos públicos de acordo com a religião que professa.

2. A fundamentalidade constitucional da liberdade de culto

Para LOCKE, "ninguém por nascimento está unido a uma Igreja ou seita, mas adere voluntariamente à sociedade religiosa cujo culto lhe parece mais agradável a Deus" (2014, p. 21). A fé não se impõe – escolhe-se. E essa escolha, feita em sã consciência, liberdade e autonomia individual, culmina sempre numa prática de culto. Não há como exercer plenamente a liberdade religiosa sem uma total liberdade de culto. Liberdade de culto apresenta-se como uma manifestação religiosa, isto é, a exteriorização da adoração por parte do *homo religiosus*. No fundo, a concretização prática da liberdade de manifestar a fé pela prática de ritos ou cultos religiosos, de acordo com as doutrinas de fé de cada religião.

Na conceção de LEITE (1978, p. 291) não existe um modo de prestar culto, mas diversas dimensões de culto religioso, que se dividem entre *i)* culto interno e externo; *ii)* culto individual e coletivo e *iii)* culto privado e público. A prática, que varia entre o flanco pessoal e o coletivo, tem lugar de acordo com os sentimentos religiosos individuais e institucionais de cada confissão religiosa.

Preferimos, contudo uma outra distinção – mais simplista, mas inteligível. Distinguimos entre a definição de:

- culto *stricto sensu*, a atividade espiritual na sua plenitude. Abrange as cerimónias de celebração e adoração coletiva, a liturgia e os rituais;
- culto *lato sensu*, que contempla as atividades religiosas e não religiosas. Para MACHADO, são as

> "atividades de aprendizagem e ensino religioso, de promoção das doutrinas religiosas, de ensaio de participações musicais, de planeamento, execução e administração de atividades da confissão religiosa, de realização de refeições comunitárias e de outras atividades visando o fortalecimento das relações sociais e intergeracionais entre os membros das confissões religiosas" (2018, p. 156).

Foquemos, porém, o nosso olhar no culto *stricto sensu*, na dimensão manifesta do culto religioso: o culto externo, individual e coletivo e público que permite ao *homo religiosus* a manifestação plena da sua espiritualidade em comunidade. Ou seja, o momento do serviço religioso praticado em comunidade de acordo com a periodicidade litúrgica de cada igreja ou comunidade religiosa (art. 23.º LLR). Trata-se, desde logo, uma manifestação que não passou despercebida ao olhar do legislador, que consagrou, no art. 8.º, al. C) e f), LLR o direito a praticar rituais de adoração ou outros atos de fé em comunidade.

3. A criança e a crença religiosa

A CRP consagra, no art. 12.º, n.º 1, o princípio da universalidade, que determina que todos os cidadãos gozam dos direitos fundamentais e estão sujeitos aos deveres (fundamentais) nela consagrados. Em matéria de liberdade religiosa, a LLR, de forma inequívoca, consagra, nos art. 8.º e seguintes, a dimensão individual da liberdade religiosa, elencando o modo como essa liberdade está na titularidade das pessoais individuais.

Se esta titularidade se mostra inquestionável, a sua capacidade de exercício coloca já algumas questões, nomeadamente no que concerne ao *fator idade*. Diz-nos a Teoria Geral do Direito que os menores de idade não possuem capacidade de exercício de direitos. Detêm personalidade jurídica, nos termos do art. 66.º, n.º 1, CC, são sujeitos individuais de direitos, mas não podem exercê-los por atos próprios. O Direito considera que o menor não apresenta condições de maturidade no exercício de direitos próprios e. por isso, estabeleceu o regime da menoridade, regulando o poder paternal como um instrumento jurídico com capacidade decisória sobre o exercício dos direitos dos menores (HÖRSTER, 2016, p. 317).

Temos por garantido que o menor de idade é titular do direito à liberdade religiosa, pelo que possui a capacidade de gozo a este adstrita; todavia, carece de capacidade geral de exercício, cabendo ao poder paternal o seu suprimento. O CC, nos preceitos 123.º e 124.º, prevê o poder paternal para os menores de idade, o que suprime, assim, a incapacidade de exercício destes. Regra geral, essa incapacidade de exercício verifica-se até aos 18 anos de idade (art. 130.º, CC) , embora o legislador preveja algumas exceções no art. 127.º. Surpreendentemente, a titularidade e o exercício da liberdade religiosa não constam deste elenco normativo – o CC apenas alude, muito timidamente, à regulação do poder paternal em matéria de *educação religiosa* no art. 1886.º[221].

A consagração legal surge, então, através do n.º 2, do art. 11.º, LLR que consubstancia uma orientação legal que diminui a idade da incapacidade de gozo por menoridade dos 18 para os 16 anos. Quer isto significar que os menores, depois de perfazerem a idade de 16 anos, têm o direito de realizar escolhas de acordo com a sua liberdade de consciência, de religião e de culto. Assim, a determinação dos atos de culto religioso por crianças ou menores de 16 anos de idade, assim como de outras decisões que acompanham o momento do culto, enquadram-se no elenco das decisões tomadas em sede de poder paternal. Na prática, não só o poder paternal pode determinar a escolha de pertença a uma determinada igreja ou comunidade religiosa, de abandono de certa igreja ou comunidade religiosa, do percurso religioso, da obrigatoriedade de assistência de cultos religiosos ou de práticas de culto ou adoração. Decisões com forte impacto na vida e na integridade pessoal e na liberdade dos menores.

[221] Desenvolvidamente, JORGE DUARTE PINHEIRO, "Religião e Direito da Família". *In Revista de Direito Público*, n.º 12, Lisboa, Julho-Dezembro, pp. 90-91.

Não obstante, a era digital trouxe um outro desafio *estranhamente* conectado à liberdade de culto: a captação e partilha de imagens de menores durante os cultos religiosos. Sabe-se que o exercício de um direito, não raras vezes, levanta questões sobre a concorrência dos direitos. No caso, o exercício do direito à liberdade religiosa é o típico exemplo quer de *cruzamento de direitos*, que tem lugar quando o mesmo ato de uma pessoa se desenvolve no âmbito de proteção de múltiplos direitos fundamentais, quer de *acumulação de direitos*, que ocorre quando um bem jurídico (liberdade de culto) leva à acumulação, no mesmo titular, de outros direitos fundamentais (direito à privacidade ou à preservação da imagem)[222]. Como gerir a liberdade de cultuar, num serviço religioso, com o direito a não ter a sua imagem captada e exposta nas redes sociais? Qual o papel das igrejas ou comunidades religiosas na proteção da imagem dos menores? Poderão os progenitores dispor do direito à imagem dos menores?

4. O direito à imagem

No art. 70.º, n.º 1, CC, o legislador consagrou a tutela geral da personalidade, com o escopo primordial de proteger a pessoa humana contra qualquer ofensa ou ameaça de ofensa à sua personalidade física ou moral, que inclui, não só, o lado emocional, mas também o lado espiritual da pessoa. Em bom rigor, a pessoa humana, na sua completude, merece proteção – afinal, é o bem supremo da Ordem Jurídica, o seu fundamento e o seu fim (CAPELO DE SOUSA, 2011, p. 97).

Os direitos de personalidade, sob a inspiração jurídico-constitucional do art. 26.º, CRP, são, assim, um conjunto de direitos subjetivos, privados, absolutos e gerais que, na sua consagração, visam compelir terceiros a absterem-se de praticar atos que, de forma ilícita, possam ofender ou ameaçar ofender a esfera jurídica de outrem (PINTO, 2012; VASCONCELOS, 2019). A sua oponibilidade *erga omnes* garante ao titular o direito indisponível e intransmissível a exigir de terceiros o respeito pelos seus direitos fundamentais.

Para lá da tutela geral, o legislador elencou, nos art. 72.º a 80.º, o universo dos direitos de personalidade. O direito à imagem consta desse catálogo normativo, no art. 79.º. Enquanto direito de personalidade, o direito à imagem tem como objeto a aparência externa da pessoa individual e tutela toda a representação visual da imagem: tudo o que permita o reconhecimento da pessoa. No fundo, a garantia do direito à imagem é a garantia da autodeterminação da pessoa humana à sua imagem, pois esta constitui um instrumento de identificação da pessoa e de manifestação da sua personalidade (FESTAS, 2009). Esta autonomia pessoal garante ao titular do direito a decidir o momento em que a sua imagem pode ser captada. Mas não só – garante também a decidir se a imagem pode ser reproduzida, partilhada, armazenada e economicamente explorada (ANDRADE, 1996).

Com o avanço da tecnologia digital, em especial ao nível dos smartphones e da globalização da Internet, a captação e divulgação de imagens de terceiros

[222] Desenvolvidamente, GOMES CANOTILHO (2007), *Direito Constitucional e Teoria da Constituição*. Coimbra: Coimbra Editora, pp. 1268 e ss.

(alguns *perfeitos desconhecidos*) tornou-se cada vez mais comum e espontânea. A fronteira entre a vida privada e a vida pública (ou *publicável*) enfraqueceu-se e, com isto, assiste-se a reiteradas ofensas públicas do direito à imagem, punidas criminalmente nos termos do art. 199.º, CP.

4.1. O culto religioso e as redes sociais

As igrejas, enquanto lugares de culto, são o símbolo máximo da liberdade religiosa. O âmago da atividade de qualquer comunidade religiosa. Ali os membros unem-se na comunhão e adoração ao divino. Partilham uma identidade pessoal e comunitária assente nos valores religiosos e morais que sustentam a confissão religiosa. Sonham objetivos espirituais e sociais dos membros, promovem a solidariedade, a integração e coesão social.

Com o advento e aumento generalizado do alcance das plataformas digitais, as igrejas e comunidades religiosas tornaram-se mais ativas nas redes sociais, em especial a partir da *era COVID-19*. Os cultos religiosos são transmitidos, de forma sistemática, através de plataformas como o *YouTube*, o *Facebook* ou sites das confissões religiosas, as imagens dos ministros de culto, membros da comunidade ou assistentes são captadas digitalmente e partilhadas nas contas do *Facebook* ou *Instagram* das confissões religiosas, nos *feeds* ou *stories*, e incontáveis vezes partilhadas pelos membros.

Compreende-se que os ministros de culto (art. 15.º, LLR e art. 5.º e 6.º, Concordata de 2004), no momento do culto religioso, estão numa posição de evidência: são eles que exercem os ofícios do culto e ministram os sacramentos próprios da confissão, que proferem os sermões e interpretam os livros sagrados, que dirigem o momento da adoração e louvor. Momentos em que a congregação está de olhos postos na figura humana que exerce os ritos litúrgicos – olhar esse muitas vezes efetuado através da lente da câmara. Mas a captação da imagem vai além destes ministros, chegando aos crentes, adultos ou menores, no momento do culto. Frequentes nas redes sociais são as imagens (fotografia ou vídeo) dos fiéis no momento da adoração, um dos momentos de maior expressão física ou externa do culto religioso.

Destaquemos, contudo, o problema fundamental desta reflexão: a imagem do menor durante o culto e a sua partilha online. Semanalmente, o serviço religioso é documentado nas plataformas, não apenas para cumprimento da chamada missionária das confissões religiosas, mas também com o intuito de compartilhar as alegrias do momento em que a congregação se une em comunhão. A consistência cronológica das publicações online tornou-se já uma *norma social* entre muitas confissões: assistimos atualmente à exposição nas redes de um aspeto fundamental da vida das crianças ou adolescentes, muitas vezes por iniciativa das comunidades religiosas e não dos menores (ou dos seus progenitores).

É nosso entender que a partilha de imagens de menores no contexto de culto tem sido subestimada pelas igrejas e comunidades religiosas e pelos progenitores. Desde logo, a máxima da era digital 'uma vez na Internet, para sempre na Internet' continua a ser negligenciada. De forma claramente inocente, a publicação de imagens dos menores nas redes sociais pode "alimentar interesses inescrupulosos, irresponsáveis, imorais e criminosos por parte de alguns indivíduos"[223]. É manifestamente impossível controlar o nível de alcance da publicação, até porque os perfis das comunidades religiosas são, em larga escala, públicos e, por isso, acessíveis a qualquer utilizador das variadas plataformas digitais.

Em concreto, consideramos que estas partilhas constituem diversos riscos, destacando-se os seguintes:

- *identidade digital*. Todas as publicações em redes digitais criam uma identidade digital do ser humano. No caso dos menores, em que a sua identidade está em formação, cria-se uma pegada digital (muitas vezes explorada pelos progenitores) com a qual o menor pode não se identificar no presente ou no futuro. Muitos menores, em especial os adolescentes, preferem manter a sua fé numa esfera absolutamente privada;
- *falta de segurança*. Com a partilha frequente de imagens nas redes socais, as igrejas e comunidades religiosas fornecem diversos elementos sobre os menores, tais como a localização do local de culto que o menor e a familia frequentam, os horários em que se encontram dentro das instalações religiosas e as rotinas familiares;
- *apropriação e uso indevido de imagens*. As imagens são facilmente descarregadas através das plataformas digitais e podem ser utilizadas por indivíduos ou organizações de práticas criminosas, como pedofilia ou pornografia infantil, que pesquisam nas mais variadas redes material para elaboração de conteúdos ilícitos, através do uso da Inteligência Artificial.

4.2. Das igrejas e da proteção de dados dos menores

Observados os riscos reais, importa compreender o modo as igrejas e comunidades religiosas devem proteger a imagem dos menores, olhando assim ao enquadramento legal em vigor no ordenamento jurídico-constitucional português e no Direito Internacional.

A CRP, no art. 35.º, deixa antever, desde o seu elenco primitivo de 1976 (cujas revisões foram atualizando a proteção dos cidadãos no que toca à preservação da sua liberdade e privacidade), a preocupação do legislador com os 'dados pessoais informatizados', que se dividem em três elementos distintos (GOUVEIA, 1991):

1. Dados que retratam uma realidade, factos ou situação;
2. Dados que se referem a pessoas humanas identificadas ou identificáveis;
3. Dados pessoais alvo de tratamento informatizado.

[223] Cfr. TRE, proc. n.º 789/13.7TMSTB-B-E1, de 25/06/2015 (BERNARDO DOMINGOS) https://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/7c52769f1dfab8be80257e830052d374.

No que releva para esta reflexão, a proteção dos dados pessoais informatizados, em bom rigor, incide sobre três direitos distintos quanto à matéria neles versada. A saber:

1. O *direito ao controlo de dados informatizados*, que garante ao titular a faculdade de tomar conhecimento do teor dos dados pessoais, da finalidade do seu tratamento, de exigir a retificação ou atualização (art. 35.º, n.º 1);
2. O *direito à não divulgação de dados informatizados* por transmissão a terceiros, de forma a garantir a confidencialidade dos mesmos e a evitar um possível cruzamento de dados entre ficheiros distintos (art. 35.º, n.º 2);
3. O *direito à proibição de tratamento de dados pessoalíssimos*, que o legislador constituinte elenca de forma taxativa: dados referentes a convicções filosóficas, políticas, partidárias e religiosas, e a questões do foro privado ou étnico (art. 35.º, n.º 3).

Conhecendo, assim, a letra da lei, perguntamos: constituem as imagens de uma pessoa, identificada ou identificável, recolhidas no momento do serviço religioso um *dado pessoalíssimo*? Invocando o art. 9.º, n.º 2, LLR, entendemos que sim, pois que nelas está patente não apenas a identificação digital da pessoa, mas também o retrato de um facto religioso ou de manifestação ritualística de fé. Contudo, não podemos deixar de olhar ao disposto no art. 35.º, n.º 3, onde o legislador entrega o poder de decisão concernente aos dados pessoais ao seu titular: cumpre a este decidir do tratamento dos seus dados pessoais, através de um consentimento expresso. Ou seja, exige-se dos membros de igrejas ou comunidades religiosas o consentimento expresso sobre o tratamento da sua imagem.

Todavia, a proteção dos dados pessoais informatizados não se esgota na regulação constitucional do art. 35.º, que chega a apontar para outras leis algumas definições e operacionalizações dos direitos fundamentais ali consagrados. É o que sucede, a título de exemplo, com a definição material de 'dados pessoais', conforme se lê no seu n.º 5.

Ao longo da vigência deste texto constitucional têm sido várias as leis em vigor relativas à proteção de dados pessoais informatizados, como a Lei da Proteção de Dados Pessoais face à Informática (Lei n.º 10/91, de 29 de abril) ou a Lei da Proteção de Dados Pessoais (Lei n.º 67/98, de 26 de outubro), estando atualmente em vigência o RGPD e a Lei de Execução do Regulamento Geral de Proteção de Dados (LERGPD), a Lei n.º 58/2019, de 8 de agosto.

O RGPD importa particularmente para o debate, pois reafirma o texto constitucional quanto à proibição geral de tratamento dos dados pessoalíssimos (no caso, os dados relativos à fé religiosa): " 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." (art. 9.º, n.º 1).

À semelhança da consagração de exceção constitucional relativa ao consentimento dos membros de igrejas ou comunidades religiosas, o RGPD vem reafirmar duas importantes exceções ao n.º 1:

1. Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas (art. 9.º, n.º 2, al. a));
2. Se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins religiosos, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares ((art. 9.º, n.º 2, al. d)).

Ou seja, o RGPD coloca na esfera jurídica do titular do direito a faculdade de consentir ou não consentir na captação, armazenamento e divulgação de imagens dos próprios no momento do culto a terceiros (seja por via informática ou por partilha em redes sociais). Esta é a solução encontrada para resolver a questão; infelizmente, a sua aplicação é reiteradamente ignorada entre muitas confissões.

É de saudar igualmente a atenção que o RGPD dirige, de forma concreta, ao tratamento de dados pessoais relativos à fé religiosa por parte das confissões religiosas:

1. *A manutenção do regime antecedente de proteção de dados*:

> "Quando, num Estado-Membro, as igrejas e associações ou comunidades religiosas apliquem, à data da entrada em vigor do presente regulamento, um conjunto completo de normas relativas à proteção das pessoas singulares relativamente ao tratamento, tais normas podem continuar a ser aplicadas, desde que cumpram o presente regulamento." (art. 91.º, n.º 1);

2. *A supervisão das igrejas e comunidades religiosas por uma autoridade de controlo*:

> "As igrejas e associações religiosas que apliquem um conjunto completo de normas nos termos do n.º 1 do presente artigo ficam sujeitas à supervisão de uma autoridade de controlo independente que pode ser específico, desde que cumpra as condições estabelecidas no capítulo VI do presente regulamento." (art. 91.º, n.º 2).

Se é, então, exigível, o consentimento expresso para o tratamento dos dados pessoais, como se impõe o consentimento dos menores? O RGPD evidencia, neste ponto, um especial cuidado com os menores. No considerando n.º 38 pode ler-se que

> "As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus

> direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança".

Deste modo, no art. 8.º, o RGPD materializa esta preocupação, disciplinando o consentimento prestado pelos menores com idades compreendidas entre os 13 e 16 anos[224]. Contudo, esta norma é unicamente aplicável a casos de oferta direta de serviços da sociedade da informação às crianças, que implicam a existência de prestação de serviços.

Assim, cumpre aos progenitores, no exercício do poder paternal, o consentimento expresso relativo aos dados pessoais dos menores de 16 anos, como supramencionado. Isto é, de forma clara e inequívoca, os progenitores devem consentir no tratamento desses dados.

Considerações finais

Com o avanço da Internet e a utilização das plataformas digitais, as igrejas e comunidades religiosas passaram a ocupar um espaço considerável nas redes sociais através da transmissão de serviços de culto online ou partilha de imagens dos crentes no momento em que exercem a sua liberdade de culto.

O escopo primordial deste trabalho consistia em refletir sobre a realidade nas confissões religiosas e abordar os conflitos entre a liberdade de culto e o tratamento de dados pessoais dos menores, dando-se início a um debate urgente sobre esta matéria, não só ao nível do exercício do poder paternal, a quem incumbe fornecer o consentimento expresso relativo ao tratamento de dados dos menores, mas também ao nível do cumprimento das normas europeias e constitucionais por parte das confissões.

Se é verdade que o elenco normativo em vigência obriga, como vimos, ao consentimento expresso, como adequar essa obrigatoriedade nas mais variadas confissões religiosas? Deixamos breves sugestões que podem ser úteis:

[224] No caso português, o legislador determinou a idade mínima de 13 anos (art. 8.º, LERGPD).

1. *Consentimento expresso por escrito*. Nas comunidades religiosas de menor dimensão está será a melhor prática. A existência de um número reduzido de membros facilita a recolha do consentimento;
2. *Informação pública do tratamento de imagens (consentimento tácito)*. Nas confissões religiosas de maior dimensão e com maior número de visitantes a cada serviço religioso, deve informar-se, através de um anúncio afixado (papel ou digital), sobre a recolha, tratamento e divulgação de imagens. Mediante a informação disponibilizada, os membros e visitantes, devidamente esclarecidos, podem decidir como consentir;
3. *Avaliação prévia das imagens*. O culto religioso, apesar de público, manifesta o momento mais intimo de relacionamento do homo religiosus e o divino, pelo que as imagens recolhidas devem passar por avaliação prévia. Há momentos mais delicados que devem ser preservados, no máximo respeito pela dignidade da pessoa humana. Ainda que a *ekklesia* tenha uma franca dimensão espiritual e imaterial, é composta por pessoas humanas e a proteção da dignidade deve ser a base visível de cada reunião de culto;
4. *Respeito pela decisão dos membros*, em especial quando exercem o seu direito ao apagamento de dados pessoais.

Muito há, ainda, por executar. Não basta termos a legislação em mãos – é imperioso aplicá-la à realidade que vivemos. Atualmente, com o RGPD, temos um verdadeiro Direito da Proteção de Dados, mas há que executá-lo de forma que os direitos fundamentais dos cidadãos sejam protegidos.

Bibliografia:

AAVV (2014*). Atas do I Colóquio Luso-Italiano sobre a Liberdade Religiosa* (coord. de PAULO PULIDO ADRAGÃO). Coimbra.

ADRAGÃO, PAULO PULIDO (2002). *A liberdade religiosa e o Estado*. Coimbra: Almedina.

AGUTI, ANDREA (2023). *Introducción a la Filosofia de la Religión*. México: Aliosventos Ediciones AC.

ALEXY, ROBERT (2006). *Theorie der Grundrechte*. Fraukfurt am Main: Suhrkamp Verlag.

ANDRADE, MANUEL DA COSTA (1996). *Liberdade de imprensa e inviolabilidade pessoal – uma perspectiva jurídico-criminal*. Coimbra: Coimbra Editora.
ARGIOLAS, DAVIDE (2017). *A responsabilidade civil extracontratual das entidades religiosas*. Coimbra: Faculdade de Direito da Universidade de Coimbra.

CANOTILHO, GOMES (2007), *Direito Constitucional e Teoria da Constituição*. Coimbra: Coimbra Editora.

CAPELO DE SOUSA, RABINDRANATH (2011). *O Direito Geral de Personalidade*. Coimbra: Coimbra Editora.

FESTAS, DAVID DE OLIVEIRA (2009). *Do conteúdo patrimonial do direito à imagem: contributo para um estudo do seu aproveitamento consentido e inter vivos*. Coimbra: Coimbra Editora.

GOUVEIA, JORGE BACELAR (1991). "Os direitos fundamentais à proteção dos dados pessoais informatizados". *In Revista da Ordem dos Advogados*, ano 51, III, Lisboa.
_____, (2024). *Direito da Religião. Laicidade, pluralismo e cooperação nas relações Igreja-Estado*. Lisboa: Almedina.

HÖRSTER, HEINRICH EWALD (2016). *A Parte Geral do Código Civil Português – Teoria Geral do Direito Civil*. Coimbra: Almedina.

LEITE, ANTÓNIO (1978). "A religião no Direito Constitucional português". *In* AAVV, *Estudos sobre a Constituição portuguesa*. II. Lisboa.

LOCKE, JOHN (2014). *Carta sobre a tolerância*. Lisboa: Padrões Culturais Editora.

MACHADO, JÓNATAS (1993). *O regime concordatário entre a "Libertas Ecclesiae" e a Liberdade Religiosa*. Coimbra.
_____ (1996). *Liberdade religiosa numa comunidade constitucional inclusiva. Dos direitos da verdade aos direitos dos cidadãos*. Coimbra: Coimbra Editora.

_____, (2018). "O regime jurídico-tributário da doação de imoveis para fins religiosos". *In Novos Estudos sobre Liberdade Religiosa, risco e segurança no século XXI*. Forte da Casa: Petrony.

MIRANDA, JORGE (1986). "Liberdade religiosa, igrejas e Estado em Portugal". Instituto da Defesa Nacional. Ano XI;Nº 39 (Jul-Set).

MOREIRA, VITAL; GOMES, CARLA DE MARCELINO (2014). *Compreender os direitos humanos. Manual de educação para os direitos humanos*. Coimbra: *Ius Gentium Conimbrigae*/Centro de Direitos Humanos.

PINHEIRO, JORGE DUARTE (2014). "Religião e Direito da Família". *In Revista de Direito Público*, n.º 12, Lisboa, Julho-Dezembro

PINTO, CARLOS ALBERTO DA MOTA (2012). *Teoria Geral do Direito Civil*. Coimbra: Coimbra Editora.

PRATAS, CLÁUDIA ALVES (2014). *Direito da Religião: a proteção jurídica das minorias protestantes*. Lisboa: Chiado Editora.
- _____, (2023). *As influências mosaicas na Constituição da República Portuguesa de 1976: um estudo comparativo de Direitos Fundamentais*. Lisboa: Faculdade de Direito da Universidade Nova de Lisboa.
VASCONCELOS, PEDRO PAIS DE (2019). *Direito de Personalidade*. Coimbra: Almedina.

Direitos da propriedade industrial: Tutela da inovação no ordenamento jurídico português

Lizeth Diniz Simão [225]

Resumo

A pesquisa examina a eficácia do ordenamento jurídico português na proteção dos direitos de propriedade industrial, destacando sua importância para a promoção da inovação tecnológica e do crescimento económico em um cenário global de rápidas transformações. A investigação analisa os instrumentos jurídicos do Código da Propriedade Industrial, o impacto de normativas internacionais, como a Convenção de Paris e o Acordo TRIPS, os desafios enfrentados pelos titulares de direitos e as perspetivas para aprimorar a tutela da inovação. Com uma abordagem metodológica dedutiva e descritiva-exploratória, o estudo combina análise teórica e prática, avaliando aspetos legislativos e tendências tecnológicas. Os resultados apontam que, embora o sistema jurídico ofereça proteção robusta, enfrenta desafios como custos elevados, morosidade nos processos de registos e infrações recorrentes. A harmonização com normativas internacionais fortaleceu a competitividade global, mas ainda há lacunas na aplicação prática. As tecnologias emergentes, como blockchain e inteligência artificial, são vistas como soluções promissoras para modernizar o sistema e aumentar sua eficiência. A pesquisa conclui que reformas legislativas e administrativas são essenciais para alinhar a proteção da propriedade industrial às demandas de um mercado global dinâmico e tecnológico, garantindo maior eficácia na promoção da inovação.

Palvras-chave: Direito da propriedade industrial. Inovação. Normativas internacionais. Ordenamento jurídico português. Tecnologia.

[225] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Industrial property rights: Protecting innovation in the Portuguese legal system

Abstract
The research evaluates the effectiveness of the Portuguese legal framework in protecting industrial property rights, emphasising its relevance for fostering technological innovation and economic growth in a rapidly evolving global context. It examines the legal instruments of the Industrial Property Code, the impact of international regulations such as the Paris Convention and the TRIPS Agreement, the challenges faced by rights holders, and future opportunities to enhance innovation protection. Adopting a deductive and descriptive-exploratory methodological approach, the study integrates theoretical and practical analyses, assessing legislative frameworks and technological trends. Findings reveal that while the legal system provides robust protection, it faces challenges such as high costs, delays in registration processes, and recurrent infringements. International regulations have strengthened global competitiveness, though practical application gaps remain. Emerging technologies, including blockchain and artificial intelligence, are identified as promising tools for modernising the system and increasing efficiency. The research concludes that legislative and administrative reforms are vital to aligning industrial property protection with the demands of a dynamic and technologically advanced global market, ensuring greater effectiveness in fostering innovation.

Keywords: Industrial property law. Innovation. International regulations. Portuguese legal framework. Technology

Introdução

A proteção jurídica da propriedade industrial constitui uma ferramenta essencial para o estímulo à inovação e ao desenvolvimento económico em um mundo marcado pela constante evolução tecnológica. No contexto português, o Código da Propriedade Industrial, consolidado pelo Decreto-Lei n.º 110/2018, desempenhará um papel central na organização dos instrumentos de tutela desses direitos, garantindo a compatibilidade com normativas internacionais como a Convenção de Paris e o Acordo TRIPS. Dessa forma, a pesquisa partirá do questionamento sobre como o ordenamento jurídico português assegurará a proteção eficaz dos direitos de propriedade industrial, par assim promover a competitividade em um cenário global em transformação.

O primeiro objetivo específico da pesquisa será examinar os instrumentos jurídicos previstos na legislação portuguesa para a proteção da propriedade industrial. Esse aspeto envolverá uma a análise detalhada das disposições do Código da Propriedade Industrial e de suas aplicações práticas, incluindo a atuação do Instituto Nacional da Propriedade Industrial (INPI). A investigação abordará ainda a forma como esses instrumentos vão estimular o desenvolvimento de tecnologias e inovações, para garantir a segurança jurídica aos titulares de direitos industriais e favorecer a competitividade no mercado global.

Outro ponto de análise será a avaliação do impacto das normativas internacionais no ordenamento jurídico português, com ênfase na Convenção de Paris e no Acordo TRIPS. Essa etapa da pesquisa buscará compreender como as diretrizes globais serão integradas às legislações nacionais e em que medida vão influenciar a eficiência prática do sistema de proteção de propriedade industrial em Portugal. Será avaliado, ainda, como a conformidade com esses tratados vai fortalecer a posição de Portugal no cenário internacional, para promover a inserção em cadeias de valor globais.

A pesquisa também se debruçará sobre os desafios enfrentados pelos titulares de direitos de propriedade industrial no país, aspetos como custos elevados, complexidade dos processos e a ocorrência de infrações. Essa abordagem permitirá identificar as barreiras que podem limitar a eficácia do sistema e propor possíveis estratégias de aprimoramento. Pretende-se, assim, delinear soluções que sejam capazes de fortalecer o sistema jurídico português no contexto das demandas tecnológicas e económicas contemporâneas.

Por fim, será explorada a questão das perspetivas futuras para a tutela da inovação no ordenamento jurídico português, vindo a destacar as oportunidades trazidas pela transformação digital e as tecnologias emergentes, como a inteligência artificial e o blockchain. Essa parte da pesquisa buscará apontar caminhos para a modernização do sistema jurídico, considerando o equilíbrio entre a proteção dos direitos industriais e o acesso público ao conhecimento, um aspeto fundamental para o desenvolvimento sustentável e inclusivo.

A relevância social, acadêmica e jurídica do tema justifica a escolha do objeto de estudo, considerando o papel crucial da propriedade industrial no estímulo à criatividade e à competitividade. A pesquisa contribuirá para o aprofundamento do debate sobre a eficácia do ordenamento jurídico português, oferecendo subsídios que poderão influenciar a formulação de políticas públicas e o aprimoramento das práticas institucionais. Sob o enfoque acadêmico, o estudo trará uma abordagem inovadora ao explorar a interseção entre direito, tecnologia e economia.

Metodologicamente, a pesquisa será pautada por uma abordagem dogmática, utilizando métodos descritivos e exploratórios para a análise das legislações, tratados internacionais e estudos de caso. Essa estratégia permitirá uma compreensão aprofundada das normas vigentes e de sua aplicação prática, bem como uma avaliação crítica dos desafios e oportunidades para o ordenamento jurídico português. A pesquisa buscará integrar a teoria e a prática, propondo soluções fundamentadas para questões concretas.

A partir desse arcabouço teórico e metodológico, espera-se que a pesquisa contribua para o fortalecimento da tutela jurídica da propriedade industrial em Portugal. Pretende-se que os resultados revelem um panorama abrangente sobre a eficácia das normas e a relevância de sua modernização, destacando as potencialidades de um sistema alinhado às transformações tecnológicas globais. O estudo almejará, portanto, oferecer uma reflexão crítica e propositiva sobre o tema, consolidando a relevância do direito da propriedade industrial como instrumento de desenvolvimento.

1. Instrumentos Jurídicos na Legislação Portuguesa para a Tutela da Propriedade Industrial

A proteção jurídica da propriedade em Portugal é estruturada a partir de instrumentos legais robustos que buscam harmonizar os interesses dos titulares de direitos e os avanços tecnológicos. Sob o enfoque da segurança jurídica, verifica-se que O Código da Propriedade Industrial (CPI), instituído pelo Decreto-Lei n.º 110/2018, representa um marco normativo abrangente para a proteção dos direitos de propriedade industrial em Portugal. Este diploma legal organiza e disciplina, entre outros aspetos, as normas relativas a patentes, marcas, desenhos ou modelos industriais e comerciais. Esses elementos constituem pilares fundamentais na promoção da inovação e no fortalecimento da competitividade no mercado, refletindo o compromisso do ordenamento jurídico português com o estímulo à pesquisa e ao desenvolvimento tecnológico. Além disso, o CPI transpõe para o direito interno as Diretivas (UE) 2015/2436 e 2016/943, que tratam, respetivamente, da harmonização das legislações sobre marcas e da proteção de know-how e informações comerciais confidenciais contra a sua aquisição, utilização e divulgação ilegais.

Essas integrações reforçam o alinhamento de Portugal às normativas internacionais e contribuem para consolidar um sistema jurídico capaz de enfrentar

os desafios de um mercado globalizado em constante evolução. A aplicação do CPI não apenas protege os direitos exclusivos dos titulares, mas também garante um ambiente de concorrência leal, vindo a incentivar investimentos em inovação. Assim, este arcabouço legal reafirma o papel estratégico da propriedade industrial como motor do crescimento económico e como elemento essencial para posicionar Portugal de forma competitiva no cenário internacional.

À luz dos direitos fundamentais, percebe-se que as patentes desempenham um papel estratégico ao garantir exclusividade temporária às invenções. De acordo com Luís Otávio Pimentel (2021), o direito de patente incentiva o investimento em pesquisa ao assegurar retorno económico aos inventores. Ademais, destaca-se que a concessão das patentes em Portugal segue critérios rigorosos de novidade, atividade inventiva e aplicação industrial, conforme delineado no CPI, o que assegura a credibilidade do sistema jurídico e protege os interesses coletivos.

As marcas, por sua vez, configuram-se como instrumentos essenciais para a identificação de produtos e serviços no mercado. Sob essa ótica, infere-se que sua proteção fomenta a lealdade comercial e a confiança do consumidor, como enfatizado por Gonçalves (2013). Para além disso, Mendes (2008) argumenta que a proteção das marcas não se limita ao âmbito nacional, integrando-se a normativas internacionais que garantem sua validade em contextos transnacionais, o que reforça a integração de Portugal ao mercado global.

No âmbito dos desenhos e modelos industriais, a legislação portuguesa busca salvaguardar o caráter estético das criações, para promover a inovação no design de produtos. À medida que se aprofunda a análise, constata-se que esses direitos favorecem a competitividade empresarial ao conferir exclusividade sobre características distintivas. Conforme preceitua Trindade (2019), a proteção desses elementos estimula o desenvolvimento de produtos visualmente atrativos, que agrega valor económico e cultural às criações.

A proteção jurídica da propriedade industrial em Portugal abrange diversos instrumentos, entre os quais se destaca a tutela dos segredos comerciais. Regulada pelo Código da Propriedade Industrial (CPI), esta proteção visa assegurar que informações confidenciais com valor económico sejam resguardadas contra práticas desleais. O CPI define segredos comerciais como informações que possuem valor comercial por serem sigilosas e que são objeto de medidas razoáveis para manter seu caráter reservado. Essa abordagem reflete um esforço para harmonizar a legislação portuguesa com as diretrizes Europeias e fortalecer a segurança jurídica no ramo empresarial.

Outro aspeto relevante é a tutela dos segredos comerciais, prevista no CPI como mecanismo de proteção contra práticas desleais. Nesse contexto, convém ressaltar que a confidencialidade de informações estratégicas é um ativo valioso para as empresas, especialmente em setores de alta tecnologia. Segundo os ensinamentos de Pereira (2015), a proteção dos segredos comerciais fortalece a

competitividade ao mitigar riscos de concorrência desleal e espionagem industrial, questões cada vez mais sensíveis em mercados globalizados. Essa proteção é particularmente importante em um cenário de rápidas inovações, onde o conhecimento técnico e informações estratégicas assumem papel central no sucesso empresarial.

O Instituto Nacional da Propriedade Industrial (INPI) desempenha um papel central na administração e fiscalização desses instrumentos jurídicos. Conforme a doutrina maioritária, entende-se que a atuação do INPI assegura a eficácia e a uniformidade na aplicação do CPI. Além de processar pedidos de registo, o instituto promove iniciativas educativas e facilita o acesso às informações, contribuindo para a conscientização sobre a importância da propriedade industrial.

No tocante às estratégias nacionais, destaca-se a Estratégia Nacional de Investigação e Inovação para uma Especialização Inteligente (ENEI), que define prioridades para o investimento em inovação. Sob outra perspectiva, verifica-se que essa política articula esforços entre governo, academia e setor privado, como argumentado por Mendes (2008). Ademais, incentivos fiscais, como o SIFIDE, têm se mostrado eficazes na promoção de atividades de investigação e desenvolvimento, consolidando-se como ferramentas estratégicas no fomento à inovação. Apesar dos avanços legislativos, a eficácia prática dos instrumentos jurídicos enfrenta desafios. Conforme aponta Trindade (2019), a morosidade nos processos de registos e os custos elevados são obstáculos que impactam negativamente a proteção da propriedade industrial.

Ainda que haja consenso quanto à relevância da legislação portuguesa, persiste o debate sobre a adaptabilidade frente às demandas tecnológicas emergentes. Sob essa ótica, infere-se que a evolução normativa deve ser contínua, acompanhando as transformações nas dinâmicas económicas e sociais. Conforme os ensinamentos de Pimentel (2021), um sistema jurídico eficaz deve equilibrar a proteção dos direitos exclusivos com a promoção de acesso à inovação, evitando práticas monopolistas.

2. Impacto das normativas internacionais

A integração das normativas internacionais, especialmente a Convenção de Paris para a Proteção da Propriedade Industrial e o Acordo sobre aspetos dos Direitos de Propriedade Intelectual Relacionados ao Comércio (Acordo TRIPS), no ordenamento jurídico português, representa um marco significativo para o fortalecimento do sistema de proteção da propriedade intelectual em Portugal, alinhando-o aos padrões e compromissos internacionais estabelecidos no âmbito da Organização Mundial do Comércio (OMC) e da União Internacional para a Proteção da Propriedade Intelectual (OMPI).[226]

[226]A OMPI, atualizada na versão de Estocolmo (1967) e por força do TRIPS /OMC (1994), celebrada no âmbito das Nações Unidas, integra a Convenção de Paris (1883), o primeiro acordo internacional relativo à Propriedade Intelectual para a Proteção da Propriedade Industrial (CUP); integra ainda a Convenção da União de Berna (1886), relativa à proteção das obras literárias e artísticas.

A Convenção de Paris, que data de 1883, constitui um dos pilares do sistema global de propriedade intelectual, ao estabelecer normas mínimas de proteção para invenções, marcas, modelos industriais e outros direitos, além de promover a cooperação entre os países signatários na defesa desses direitos. Já o Acordo TRIPS, que foi incorporado à OMC em 1995, visa harmonizar as leis de propriedade intelectual entre seus membros, com um enfoque especial na facilitação do comércio internacional, protegendo, entre outros, as patentes, direitos autorais, marcas e desenhos industriais, impondo obrigações de reconhecimento mútuo e de efetiva aplicação dos direitos.

No contexto jurídico português, a adesão a essas convenções e acordos internacionais se reflete na adaptação e incorporação de suas disposições ao ordenamento interno, processo que implica a revisão de legislações e a criação de novos dispositivos legais que assegurem a conformidade com as normas globais. A integração da Convenção de Paris no sistema jurídico português ocorre principalmente por meio do Código da Propriedade Industrial (CPI), que trata das regras relativas à proteção de patentes, marcas e modelos industriais, alinhando-se às exigências da Convenção, como a garantia de prioridade no registo de patentes e a não discriminação entre os cidadãos nacionais e os estrangeiros, princípios fundamentais que asseguram a efetividade do direito à proteção no contexto internacional.

Assim, a Convenção de Paris, ao garantir um sistema jurídico de proteção na reciprocidade, facilita a obtenção de registos internacionais, vindo a garantir que os titulares de direitos industriais em Portugal a possibilidade de expandir as proteções para outros países que sejam partes da Convenção.

Por sua vez, a integração do Acordo TRIPS no ordenamento jurídico português reflete-se principalmente na adequação das legislações nacionais às normas internacionais estabelecidas pelo acordo, que impõem padrões mínimos de proteção para os direitos de propriedade intelectual, com uma ênfase particular na harmonização dos procedimentos de registo, fiscalização e aplicação desses direitos. A transposição das disposições do Acordo TRIPS para a legislação portuguesa reforça a proteção dos direitos de propriedade intelectual, promovendo uma maior segurança jurídica tanto para os titulares de direitos quanto para os operadores económicos, ao mesmo tempo em que assegura que o país esteja em conformidade com as regras do comércio internacional e com os compromissos assumidos na OMC. A comparação entre o impacto das normativas internacionais, como a Convenção de Paris e o Acordo TRIPS, no contexto jurídico português e em outros países da União Europeia revela tanto benefícios quanto desafios resultantes da harmonização internacional na proteção da inovação tecnológica.

Nesse sentido, a União Europeia, sistema mais harmonizado e eficiente para a proteção da propriedade intelectual em todos os seus Estados membros. Essa uniformidade facilita o reconhecimento e a aplicação de direitos de propriedade

intelectual, promovendo uma maior segurança jurídica e incentivando a inovação tecnológica, ao criar um ambiente de confiança para empresas e investidores. Para Portugal, como parte integrante da União Europeia, os impactos das normativas internacionais se traduzem em um alinhamento legal com os outros países da região, para permitir que empresas portuguesas possam atuar no mercado europeu com uma proteção consistente para as suas criações, enquanto ao mesmo tempo se assegura que as inovações tecnológicas desenvolvidas no país estejam protegidas nas demais jurisdições Europeias.

No entanto, embora exista uma base comum, como as diretivas e regulamentos europeus que orientam a implementação do Acordo TRIPS e da Convenção de Paris, as práticas e procedimentos administrativos podem variar entre os Estados membros, o que pode ocasionar ineficiências ou disparidades no processo de concessão de direitos. Por exemplo, o tempo de processamento de um pedido de patente, o custo do registo de uma marca ou as abordagens de fiscalização e aplicação podem ser diferentes em Portugal, França ou Alemanha, refletindo uma flexibilidade que, embora necessária para respeitar as particularidades locais, pode gerar complexidades para os titulares de direitos que buscam uma proteção uniforme e de fácil acesso em todos os países da União Europeia. Por outro lado, a harmonização internacional proporciona benefícios substanciais, especialmente na proteção da inovação tecnológica, ao facilitar a proteção de patentes e direitos autorais em múltiplos países através de processos unificados, como o Sistema de Patente Europeia e o Sistema de Marcas da União Europeia. Esses mecanismos proporcionam uma solução prática para empresas e inovadores, que podem registar suas invenções e criações em diversos países com um único procedimento, garantindo a proteção em toda a região europeia sem a necessidade de realizar múltiplos registos nacionais. Esse tipo de simplificação é crucial para startups e empresas de base tecnológica, que, ao expandirem seus negócios internacionalmente, podem acessar mercados maiores com maior segurança jurídica e menos custos administrativos.

2.1. Desafios na proteção dos direitos de propriedade industrial

No que se refere às barreiras económicas, o processo de registo e manutenção de patentes, marcas e outros direitos de propriedade industrial, embora essencial para a criação de um ambiente competitivo e inovador, impõe custos elevados que frequentemente tornam inacessíveis para as PMEs, as quais, devido à sua limitada capacidade financeira, se veem impossibilitadas de registar suas inovações ou de manter os direitos adquiridos. O custo de uma patente, que envolve taxas para registo, exame, e manutenção periódica, além das despesas com consultoria jurídica especializada, representa um entrave substancial, principalmente para empresas de pequeno porte, que frequentemente priorizam a viabilidade imediata das operações em detrimento da proteção de seus direitos industriais. Essa realidade reflete uma disparidade no acesso à proteção da propriedade intelectual, uma vez

que as grandes empresas, com recursos financeiros mais robustos, têm acesso facilitado a esse sistema, o que resulta em uma desigualdade competitiva no mercado, onde as PMEs, apesar de desenvolverem inovações relevantes, ficam vulneráveis à apropriação indevida das suas criações.

Além disso, a falta de uma cultura sólida de proteção da propriedade intelectual nas PMEs agrava ainda mais essa situação, uma vez que muitos gestores dessas empresas não percebem a importância do registo das inovações, seja por desconhecimento dos benefícios dessa proteção, seja por uma visão de curto prazo em relação ao impacto do registo no seu negócio. Esse cenário de ineficiência na proteção das inovações tecnológicas acaba por prejudicar o desenvolvimento económico pequenas e médias empresas, ao dificultar o seu acesso ao mercado internacional, onde a proteção de propriedade intelectual é, frequentemente, um pré-requisito fundamental para a entrada e manutenção em mercados competitivos.

Paralelamente, outro desafio relevante diz respeito à efetividade das sanções contra pirataria e concorrência desleal, que, embora previstas em diversas legislações, muitas vezes se mostram ineficazes diante da complexidade das infrações e da falta de recursos para sua implementação. A pirataria, que envolve a reprodução ilegal de produtos protegidos por patentes, marcas e outros direitos de propriedade industrial, bem como a concorrência desleal, caracterizada pela utilização indevida desses direitos, continua a ser uma prática recorrente no mercado, especialmente no contexto digital, onde a distribuição de produtos falsificados e o uso não autorizado de marcas e patentes ocorrem com grande velocidade e em larga escala.

A globalização do comércio e o avanço das tecnologias de comunicação e informação, em particular a internet, ampliaram o alcance da pirataria e da concorrência desleal, tornando mais difícil o rastreamento e a punição de infratores, uma vez que esses crimes, muitas vezes, transcendem as fronteiras nacionais e exigem uma cooperação internacional mais eficaz para que as sanções possam ser aplicadas de maneira consistente e uniforme.

Ademais, a escassez de recursos e a complexidade das investigações que envolvem infrações de propriedade industrial dificultam a atuação das autoridades responsáveis pela fiscalização, que muitas vezes se veem sobrecarregadas e sem ferramentas adequadas para lidar com o crescente número de infrações. Além disso, o ambiente digital, caracterizado pela descentralização e anonimato das transações, cria um cenário propício para a prática de pirataria e concorrência desleal, o que aumenta ainda mais a dificuldade de aplicação das sanções previstas na legislação. A falta de uma fiscalização eficiente e de um sistema robusto de monitoramento resulta em uma sensação de impunidade por parte dos infratores, que continuam a explorar as inovações alheias sem sofrer as consequências legais adequadas.

A rápida evolução tecnológica, especialmente no que tange a inovações como a inteligência artificial (IA) e o blockchain, tem gerado lacunas significativas na proteção dos direitos de propriedade industrial, uma vez que as normativas existentes, muitas vezes, não estão adequadas para lidar com a complexidade e as especificidades dessas novas tecnologias. A IA, por exemplo, levanta questões jurídicas de difícil resolução, especialmente no que diz respeito à titularidade de invenções ou criações desenvolvidas autonomamente por sistemas de aprendizado de máquina.

A natureza da IA, em que algoritmos e sistemas de aprendizado podem gerar inovações ou soluções de forma autônoma, desafia o conceito tradicional de autor ou inventor, que pressupõe a atuação de uma pessoa física como titular do direito de propriedade. O problema reside na identificação do responsável por uma invenção criada por um sistema de IA, uma vez que este não pode ser reconhecido legalmente como sujeito de direitos. Além disso, surge a dúvida sobre como proteger adequadamente as inovações geradas por IA em um sistema que ainda exige a participação humana para o reconhecimento e a exploração de patentes ou direitos autorais, o que impõe uma necessidade urgente de revisão dos marcos legais relativos à propriedade industrial, a fim de incluir essas novas formas de criação intelectual.

No contexto do blockchain, a tecnologia de registo descentralizado, que possibilita a criação de registos imutáveis e transparentes sem a necessidade de uma autoridade central, também apresenta desafios significativos para a proteção da propriedade industrial. O blockchain tem a capacidade de registar, de maneira segura e descentralizada, informações relacionadas a transações, contratos e criações intelectuais, mas essa natureza descentralizada dificulta a aplicação das regras tradicionais de propriedade intelectual, que normalmente dependem de um registo centralizado e da ação de uma autoridade para a concessão de direitos e a fiscalização de infrações.

O uso de blockchain para registar criações intelectuais, como patentes ou marcas, desafia os modelos tradicionais de proteção, uma vez que a tecnologia permite que as informações sejam imutáveis e publicamente acessíveis, o que pode entrar em conflito com os princípios de privacidade e exclusividade típicos da propriedade industrial. Ademais, as dificuldades em identificar e responsabilizar os infratores, dada a natureza anônima e descentralizada do blockchain, tornam a proteção da propriedade intelectual mais complexa, uma vez que as infrações podem ocorrer sem a deteção imediata por parte dos sistemas tradicionais de fiscalização.

Essas lacunas na proteção de novas tecnologias exigem uma atualização urgente das normas de propriedade industrial, de modo a integrar as inovações tecnológicas de maneira eficaz e a garantir que os direitos dos inovadores sejam devidamente protegidos. A adaptação das legislações deve considerar, por exemplo, a possibilidade de reconhecer os sistemas de IA como colaboradores ou assistentes nas criações intelectuais, sem desconsiderar a atribuição de direitos aos

humanos responsáveis pela programação, treinamento e direcionamento dos algoritmos. Em relação ao blockchain, seria necessário criar uma estrutura normativa que permita a utilização da tecnologia para registar inovações, sem comprometer a segurança e a privacidade dos titulares, ao mesmo tempo em que se preserva a possibilidade de fiscalização e a identificação de infrações.

2.2. Desafios Enfrentados pelos Titulares de Direitos de Propriedade Industrial em Portugal

O cenário jurídico português evidencia uma série de desafios que os titulares de direitos de propriedade industrial enfrentam para assegurar a proteção efetiva das suas criações. Esses obstáculos incluem desde a complexidade dos processos administrativos até insuficiência de medidas que impeçam infrações. Sob o prisma da inovação tecnológica, tais dificuldades limitam o potencial competitivo das empresas e a consolidação de um ambiente favorável ao desenvolvimento. Assim, torna-se necessário examinar as principais barreiras e propor melhorias para fortalecer o sistema.

O registo de direitos de propriedade industrial em Portugal, como patentes e marcas, apresenta custos significativos que podem representar um obstáculo, sobretudo para pequenas e médias empresas. Esses custos incluem tanto as taxas iniciais de registo quanto os encargos anuais necessários para a manutenção dos direitos ao longo do tempo. No caso das patentes, por exemplo, a proteção é válida por até 20 anos, mas exige o pagamento de anuidades para sua continuidade. Essa estrutura financeira, ainda que necessária para sustentar o sistema, tem gerado questionamentos quanto à sua acessibilidade e impacto sobre a inovação.

De acordo com Costa (2023), os encargos financeiros, somados à burocracia associada ao processo, restringem o acesso de pequenas e médias empresas, comprometendo a democratização do sistema. Ademais, a duração prolongada para a concessão de patentes fragiliza a proteção jurídica, deixando os inventores suscetíveis a práticas desleais enquanto aguardam a finalização do processo. Esses fatores contribuem para uma perceção de ineficiência no sistema, especialmente em um cenário global onde a agilidade e a acessibilidade são essenciais para promover a competitividade e a inovação.

O Instituto Nacional da Propriedade Industrial (INPI) tem adotado medidas para mitigar os efeitos desses custos e tornar o processo mais acessível. Entre essas iniciativas, destaca-se a redução de 50% nas taxas para atos realizados online, essa medida não apenas simplifica o procedimento como também busca atender às necessidades de empresas com recursos financeiros limitados. Apesar disso, muitos titulares de direitos ainda enfrentam dificuldades para arcar com os custos totais envolvidos.

Outro ponto que merece atenção é a relação entre os custos e a eficiência do sistema. O tempo necessário para concluir o processo de registo de uma patente

ou marca impacta diretamente a capacidade das empresas de proteger as inovações em mercados altamente competitivos. A demora na concessão dos direitos fragiliza a segurança jurídica e aumenta os riscos de concorrência desleal e pirataria. Assim, a modernização administrativa e a digitalização mais ampla do sistema são apontadas como soluções para melhorar a eficiência e reduzir os entraves existentes.

Embora iniciativas como a redução de taxas representem avanços, os custos e a duração dos processos continuam a ser barreiras significativas para a plena utilização do sistema de propriedade industrial. A adoção de tecnologias emergentes e a simplificação dos trâmites burocráticos poderão contribuir para um ambiente mais inclusivo e eficaz, que promova a democratização do acesso à proteção jurídica e estimule a inovação em todos os níveis do mercado. Assim, Portugal poderá consolidar um sistema mais robusto e alinhado às exigências do cenário global.

Infrações como pirataria, concorrência desleal e violação de patentes constituem outro desafio significativo no contexto português. À luz do direito comparado, verifica-se que a repressão a essas práticas ainda carece de maior celeridade e eficácia. Segundo Pais (2019), embora o ordenamento jurídico preveja sanções para essas infrações, a aplicação prática dessas medidas enfrenta limitações, como a falta de recursos para fiscalização. Dessa maneira, consolida-se a interpretação de que o fortalecimento institucional é essencial para mitigar tais violações.

A análise crítica das medidas judiciais e administrativas disponíveis para os titulares revela uma lacuna na efetividade da proteção oferecida. Conforme preceitua Sousa (2023), as ações judiciais, embora indispensáveis, apresentam custos elevados e prazos dilatados, o que desestimula os prejudicados a buscar reparação. Por outro lado, medidas cautelares, como apreensão de bens infratores, são ferramentas subutilizadas, o que enfraquece o sistema de resposta imediata às infrações. Sob essa ótica, infere-se que a eficiência das ações depende de maior agilidade e acessibilidade.

Casos práticos ilustram os impactos desses desafios sobre a capacidade de inovação tecnológica. No âmbito nacional, empresas de base tecnológica enfrentam dificuldades para proteger software e invenções relacionadas à inteligência artificial, setores que demandam adaptações legislativas. Nos dizeres de Pimentel (2016), a ausência de regulamentação específica para novas tecnologias compromete a competitividade das empresas portuguesas no mercado global. Assim, torna-se evidente que a modernização do arcabouço normativo é um requisito inadiável.

A digitalização dos processos administrativos é outro aspeto relevante para o aprimoramento do sistema. Sob outra perspectiva, verifica-se que a automação pode reduzir a burocracia e agilizar a tramitação de registos e litígios. Como assevera Costa (2023), a implementação de tecnologias de blockchain no controle de

patentes e marcas garantiria maior segurança e transparência, representando um avanço significativo na gestão dos direitos de propriedade industrial.

A experiência portuguesa demonstra que, embora haja avanços significativos, persistem desafios que limitam o pleno potencial do sistema. Assim, cabe aos legisladores e operadores do direito a tarefa de superar tais barreiras, para que a propriedade industrial desempenhe o seu papel como catalisador da inovação e do desenvolvimento económico.

3. Tecnologias emergentes e a modernização da proteção jurídica

A modernização da proteção jurídica frente às tecnologias emergentes exige uma adaptação das normas vigentes, de modo a incorporar inovações tecnológicas que, por sua natureza disruptiva, desafiam os sistemas tradicionais de registo e proteção, como ocorre no caso do blockchain e da inteligência artificial (IA). A utilização do blockchain no registo e proteção de patentes e marcas, por exemplo, oferece uma série de vantagens ao sistema jurídico, particularmente no que se refere à segurança e à imutabilidade dos registos, características fundamentais para garantir a autenticidade e a integridade dos direitos de propriedade industrial.

O blockchain, ao permitir o armazenamento descentralizado de informações de forma segura e transparente, apresenta-se como uma tecnologia capaz de superar as limitações dos sistemas tradicionais de registo, nos quais a centralização e a possibilidade de manipulação dos dados podem gerar dúvidas sobre a veracidade e a proteção dos direitos. Nesse contexto, o uso de blockchain para o registo de patentes e marcas no ordenamento jurídico português poderia, além de garantir a autenticidade dos registos, facilitar a rastreabilidade e a verificação de direitos, proporcionando um ambiente mais seguro e confiável para os titulares de direitos de propriedade industrial.

A incorporação dessa tecnologia ao sistema jurídico, no entanto, exige a criação de um marco regulatório específico que contemple as particularidades do blockchain, alinhando-o aos princípios da proteção jurídica da propriedade intelectual e assegurando que a sua aplicação não conflite com os requisitos formais e materiais exigidos pelo Código da Propriedade Industrial (CPI).

Por outro lado, a inteligência artificial surge como uma ferramenta promissora para a automação dos processos administrativos no Instituto Nacional da Propriedade Industrial (INPI), para facilitar a gestão de pedidos de registo e a análise de patentes e marcas. A aplicação de IA em sistemas administrativos permite uma maior eficiência na análise de grandes volumes de dados, o que, em um contexto jurídico, pode resultar na aceleração dos processos de concessão de direitos, redução de erros humanos e melhoria na qualidade da avaliação de novos pedidos. A IA pode ser utilizada para automatizar tarefas repetitivas, como a análise preliminar de documentos, o que permitiria aos funcionários do INPI dedicar mais tempo à resolução de questões mais complexas e estratégicas.

Além disso, a IA pode ser integrada em sistemas de busca e consulta de patentes e marcas, vindo a facilitar o exame de originalidade e a identificação de conflitos, ao permitir uma pesquisa mais rápida e precisa nos bancos de dados de propriedade industrial. No entanto, assim como no caso do blockchain, a introdução de IA nos sistemas administrativos do INPI demanda a adaptação da legislação portuguesa, onde o uso dessas ferramentas tecnológicas esteja em conformidade com os princípios jurídicos e regulatórios de proteção de direitos de propriedade intelectual. A modernização da proteção jurídica frente às tecnologias emergentes, como o blockchain e a inteligência artificial, exige uma abordagem integrada que considere a adaptação das normativas existentes, como o Código da Propriedade Industrial, à nova realidade tecnológica. O uso dessas tecnologias no contexto do sistema de propriedade industrial no ordenamento jurídico português representa uma oportunidade para aprimorar a eficiência e a segurança dos processos de registo e proteção de patentes e marcas, ao mesmo tempo em que desafia o legislador a criar um ambiente jurídico mais flexível, capaz de acompanhar as inovações sem comprometer os direitos dos titulares de propriedade intelectual.

A incorporação dessas tecnologias ao INPI e ao sistema jurídico de proteção de propriedade industrial requer, assim, não apenas um esforço de inovação legislativa, mas também um compromisso com a criação de um sistema jurídico adaptado às necessidades do mercado globalizado e digitalizado, que garante os direitos de propriedade intelectual sejam devidamente protegidos e respeitados em um ambiente cada vez mais dinâmico e complexo. A titularidade das criações geradas por inteligência artificial (IA) constitui um dos maiores desafios jurídicos no contexto da proteção da propriedade intelectual, especialmente no direito português, onde as normas tradicionais de autoria e invenção não foram inicialmente concebidas para lidar com as complexidades das inovações produzidas por sistemas autónomos.

No direito português, a legislação sobre propriedade intelectual estabelece, de maneira geral, que os direitos de autor e as patentes são atribuídos a pessoas físicas, ou, em alguns casos, jurídicas, que são reconhecidas como os criadores ou inventores de uma obra ou invenção. No entanto, ao se deparar com criações geradas por IA, surgem questões sobre quem deve ser considerado o titular desses direitos, uma vez que a IA, por sua própria natureza, não é um sujeito jurídico capaz de ser reconhecido como autor ou inventor no sentido tradicional. [227]

Em situações em que uma obra ou invenção é gerada exclusivamente por uma IA, sem intervenção direta de um ser humano, o direito português se vê diante da difícil tarefa de atribuir titularidade. A tradicional concepção de autoria, que

[227]No direito português, os direitos de autor e as patentes encontram-se regulados pelo Código do Direito de Autor e dos Direitos Conexos (CDADC) e pelo Código da Propriedade Industrial (CPI). Estes preveem que apenas pessoas físicas ou jurídicas podem ser reconhecidas como titulares de direitos de propriedade intelectual. No caso de criações geradas por inteligência artificial, a ausência de personalidade jurídica da IA levanta debates significativos sobre a atribuição de titularidade e os limites da legislação vigente. Para mais informações, consultar o CDADC e o CPI, disponíveis em: https://dre.pt/.

exige a presença de um criador humano, não se aplica diretamente ao contexto da IA, uma vez que os algoritmos de aprendizado de máquina não são sujeitos de direitos. Esse cenário cria um vácuo jurídico, pois não há uma norma clara que determine quem deve ser considerado o titular dos direitos sobre uma criação gerada por uma IA. Uma solução possível seria considerar como titular a pessoa ou entidade responsável pela criação, programação ou treinamento da IA, o que levanta questões sobre o grau de envolvimento humano necessário para justificar a titularidade, bem como sobre a extensão dos direitos a serem atribuídos ao programador ou desenvolvedor.

Ademais, outro desafio significativo reside na dificuldade de definir o escopo dos direitos de propriedade intelectual atribuídos a criações geradas por IA. A questão central está em identificar quais elementos da criação são resultado exclusivo do trabalho humano e quais são fruto da autonomia da IA. Em muitos casos, a IA não opera de forma completamente autônoma, sendo direcionada por humanos para atingir certos objetivos ou soluções específicas, mas, ao mesmo tempo, pode gerar resultados inesperados e inovadores que fogem ao controle direto dos seus programadores. Esse fenómeno, por sua vez, exige uma reflexão profunda sobre os conceitos de originalidade, autoria e invenção, que são fundamentais para o reconhecimento de direitos de propriedade intelectual. O desafio, portanto, é equilibrar a proteção dos direitos dos desenvolvedores humanos com a garantia de que a inovação e a criatividade, independentemente da sua origem, sejam devidamente reconhecidas e protegidas.

No contexto do direito português, a lacuna legislativa em relação à titularidade das criações geradas por IA torna-se ainda mais evidente quando se observa que, embora existam discussões a nível Europeu sobre a necessidade de adaptação das normas de propriedade intelectual à era digital, a legislação portuguesa ainda não oferece respostas claras e específicas para essas questões. A falta de uma regulamentação específica sobre IA no âmbito da propriedade intelectual contribui para a incerteza jurídica, o que pode desencorajar a inovação ou criar disputas entre as partes envolvidas na criação de obras ou invenções geradas por IA. A solução para essas questões exige uma atualização das normas jurídicas, com a criação de um marco regulatório que contemple a realidade das criações tecnológicas, oferecendo um quadro claro para a atribuição de titularidade e a definição de direitos.

3.1. Perspetivas Futuras para Tutela da Inovação no Contexto Tecnológico

O avanço das tecnologias disruptivas impõe novos desafios e oportunidades ao ordenamento jurídico português no âmbito da proteção da propriedade industrial. Sob a perspectiva das inovações tecnológicas, verifica-se que a legislação precisa acompanhar a complexidade de temas como inteligência artificial, blockchain e biotecnologia, que estão a redefinir as dinâmicas do mercado global. Dessa

maneira, consolida-se a interpretação de que o aperfeiçoamento do arcabouço normativo é crucial para fomentar a competitividade e a sustentabilidade no cenário contemporâneo. [228]

A evolução do direito da propriedade industrial no contexto das novas tecnologias demanda maior adaptabilidade das normas vigentes. Segundo os ensinamentos de Gonçalves (2024), tecnologias emergentes, como a inteligência artificial, apresentam desafios específicos, especialmente no que tange à titularidade das invenções. Nesse contexto, convém ressaltar que o debate sobre a proteção de criações autónomas ainda encontra lacunas regulatórias em Portugal, exigindo que o legislador antecipe as implicações jurídicas dessas transformações.

A biotecnologia, por sua vez, representa outro campo que desafia os parâmetros tradicionais do direito industrial. Conforme preceitua Martins (2020), a regulamentação das invenções biotecnológicas deve equilibrar o estímulo à inovação com a proteção dos recursos genéticos e dos interesses coletivos. Sob essa ótica, infere-se que as políticas públicas precisam integrar a dimensão ética e ambiental à proteção jurídica, de modo a garantir um desenvolvimento inclusivo e responsável nesse setor estratégico.

Tendências internacionais também desempenham papel relevante na reformulação da legislação nacional. À luz dos acordos multilaterais, percebe-se que Portugal deve alinhar-se às práticas internacionais para preservar sua competitividade no mercado global.

Outro aspeto central refere-se à digitalização dos processos administrativos relacionados à propriedade industrial. Com efeito, é imperioso observar que a automação e o uso de tecnologias como blockchain podem aumentar a transparência e a eficiência dos registos. De acordo com Almeida (2021), a integração dessas ferramentas ao sistema jurídico nacional reduz a burocracia e garante maior segurança às informações sensíveis, configurando-se como um avanço necessário no contexto atual.

No âmbito das parcerias público-privadas, destaca-se a importância de incentivar a colaboração entre o setor estatal e o empresarial na promoção da inovação tecnológica. Conforme a doutrina maioritária, entende-se que programas de cofinanciamento e transferência de tecnologia podem alavancar investimentos e criar um ambiente mais propício à proteção das criações intelectuais. Sob outra perspectiva, verifica-se que iniciativas conjuntas também fomentam a capacitação de profissionais para atuar nas áreas de propriedade industrial e inovação.

A análise crítica da tutela da inovação tecnológica também exige uma reflexão sobre o equilíbrio entre proteção jurídica e acesso público. Embora a propriedade industrial desempenhe papel crucial na promoção do desenvolvimento

[228] As tecnologias disruptivas, como a inteligência artificial, o blockchain e a biotecnologia, apresentam desafios únicos ao regime jurídico da propriedade industrial, particularmente no contexto português. A necessidade de atualização do quadro normativo reflete-se no objetivo de promover inovação e competitividade, alinhando-se às diretrizes internacionais, como as definidas pela Organização Mundial da Propriedade Intelectual (OMPI). Para mais informações sobre o impacto dessas tecnologias na propriedade industrial, consultar: https://www.wipo.int/.

económico, é importante destacar que um sistema excessivamente restritivo pode dificultar a difusão do conhecimento. Nos dizeres de Silva (2011), a regulamentação deve priorizar a sustentabilidade, permitindo que os benefícios das tecnologias cheguem a um público mais amplo, sem comprometer os direitos dos criadores.

Enquanto o entendimento doutrinário maioritário defende a importância de regulamentar de maneira mais rígida setores como a inteligência artificial, há quem sustente que o excesso de regulamentação pode inibir a inovação. Nesse sentido, o debate sobre a flexibilização das regras precisa ser conduzido com cautela, considerando os impactos sociais e económicos de tais decisões.

A experiência de outros países pode servir como referência para a formulação de políticas mais eficazes no contexto português. Sob a ótica do direito comparado, verifica-se que nações que investiram na modernização dos sistemas de propriedade industrial alcançaram maior competitividade no mercado global. Dessa forma, Portugal tem a oportunidade de adotar estratégias semelhantes, adaptando-as à sua realidade jurídica e económica. Exemplos como Alemanha, Estados Unidos, Coreia do Sul e China demonstram como a combinação de medidas administrativas eficientes e incentivos governamentais pode impulsionar a inovação tecnológica e fortalecer o sistema de proteção jurídica.

Na Alemanha, o Deutsches Patent- und Markenamt (DPMA) implementa um sistema de proteção à propriedade industrial eficiente, oferecendo procedimentos rápidos e suporte técnico aos titulares de direitos. Essa abordagem, aliada a um ambiente jurídico estável, tornou o país referência em inovação e competitividade no cenário Europeu.[229]

Nos Estados Unidos, o United States Patent and Trademark Office (USPTO) prioriza a acessibilidade e agilidade nos processos de registo, promovendo um ambiente que incentiva a pesquisa e o desenvolvimento em setores estratégicos, consolidando o país como líder global em diversas áreas tecnológicas.[230]

A Coreia do Sul destaca-se como um exemplo de sucesso ao combinar altos investimentos em pesquisa com um sistema de propriedade industrial eficiente. O Korean Intellectual Property Office (KIPO) desempenha papel essencial no suporte aos inventores, facilitando o registo de patentes e garantindo proteção robusta.[231]

A China, por sua vez, realizou reformas substanciais no China National Intellectual Property Administration (CNIPA), o que resultou no aumento exponencial de registos de patentes e no fortalecimento da sua posição no comércio

[229] O Deutsches Patent- und Markenamt (DPMA) da Alemanha exemplifica um sistema eficaz, combinando agilidade processual e suporte técnico, consolidando o país como líder europeu em inovação.

[230]Nos Estados Unidos, o USPTO promove um sistema acessível e ágil, incentivando o desenvolvimento tecnológico e fortalecendo o papel do país como líder global em inovação.

[231]O KIPO, na Coreia do Sul, combina altos investimentos em pesquisa com procedimentos eficazes de registo de patentes, destacando-se como referência em inovação tecnológica.

internacional. Ambos os países demonstram que sistemas ágeis e políticas alinhadas ao contexto tecnológico impulsionam a inovação e atraem investimentos.[232]

A observação desses exemplos evidencia que políticas públicas efetivas, combinadas com modernização administrativa, podem ser adaptadas ao contexto português para fortalecer a proteção da propriedade industrial. A integração de práticas bem-sucedidas, como a digitalização dos processos, a promoção de incentivos fiscais e o fortalecimento institucional, permitirá a Portugal não apenas acompanhar as demandas do mercado global, mas também consolidar-se como referência na promoção da inovação tecnológica e no desenvolvimento econômico sustentável.

O futuro da tutela da inovação tecnológica em Portugal dependerá da capacidade de integrar instrumentos jurídicos eficazes às demandas de um mercado em constante transformação. A criação de um ambiente jurídico mais dinâmico, associado a políticas públicas de incentivo à inovação, representa um caminho promissor para assegurar a competitividade do país e estimular o desenvolvimento de tecnologias que atendam às necessidades da sociedade contemporânea.[233]

4. Propriedade industrial e competitividade económica

O sistema jurídico de propriedade industrial, ao garantir a proteção de patentes, marcas, desenhos industriais e outros direitos de propriedade intelectual, desempenha um papel crucial na criação de um ambiente de negócios seguro e previsível, o que se traduz diretamente na capacidade do país de atrair investimentos. Nesse contexto, a confiança no sistema jurídico de propriedade industrial, aliado à clareza das regras e à eficiência dos processos de registo e fiscalização, torna-se um fator determinante para a decisão de investir em um país. Quando o ordenamento jurídico garante a proteção efetiva desses direitos, os investidores podem ter a certeza de que suas participações empresariais e inovações estarão resguardadas, o que, por sua vez, estimula o fluxo de capitais estrangeiros, impulsionando o crescimento económico e a criação de novos empregos.

A proteção jurídica da propriedade industrial, ao atuar como um mecanismo de segurança para as inovações, também tem um impacto direto na competitividade das empresas portuguesas no mercado internacional. As empresas que possuem suas inovações protegidas por direitos de propriedade industrial têm a possibilidade de se destacar em mercados globais, onde a proteção das criações intelectuais é um requisito essencial para a concorrência. A contribuição da propriedade industrial para a internacionalização das empresas portuguesas, portanto, deve ser compreendida no contexto da sua capacidade de oferecer um

[232]A modernização do CNIPA na China impulsionou significativamente os registos de patentes e consolidou o país como protagonista no comércio internacional.

[233]Portugal pode beneficiar-se da adaptação de estratégias bem-sucedidas de outros países, como a digitalização, incentivos fiscais e fortalecimento institucional, para modernizar a proteção da propriedade industrial e fomentar a inovação.

diferencial competitivo que facilite a entrada em novos mercados. Quando uma empresa portuguesa consegue garantir a proteção das suas invenções e marcas no exterior, ela amplia significativamente as possibilidades de operação em mercados internacionais, sem o risco de violação de seus direitos. O sistema jurídico de propriedade industrial português, ao harmonizar suas normas com as diretrizes internacionais, facilita a expansão das empresas portuguesas para mercados europeus e globais.

A utilização de instrumentos como o Sistema de Marcas da União Europeia e o Sistema de Patente Europeia permite que as empresas registem as criações em múltiplos países com um único processo, simplificando o acesso a mercados internacionais e aumentando a visibilidade e o alcance de suas inovações. Além disso, a adesão a tratados internacionais, como a Convenção de Paris e o Acordo TRIPS, fortalece ainda mais a capacidade das empresas portuguesas de proteger seus direitos de propriedade intelectual fora do país, a proteção jurídica da propriedade industrial, ao assegurar os direitos de exclusividade sobre inovações e criações, não apenas impulsiona a competitividade das empresas no mercado nacional, mas também atua como um alicerce fundamental para sua internacionalização. O fortalecimento do sistema de propriedade industrial no ordenamento jurídico português, aliado à adaptação às exigências internacionais, tem um impacto direto na atração de investimentos estrangeiros e na expansão das empresas portuguesas no comércio internacional. Dessa forma, a propriedade industrial, além de ser um instrumento de proteção, configura-se como uma ferramenta estratégica para o crescimento económico e a inserção competitiva de Portugal no cenário global.

A inovação tecnológica desempenha um papel crucial no desenvolvimento sustentável, especialmente no contexto do ordenamento jurídico português, onde a proteção da propriedade industrial se configura como uma ferramenta estratégica para fomentar inovações que, ao mesmo tempo em que impulsionam a competitividade económica, contribuem para a preservação ambiental e o bem-estar social. A interseção entre inovação tecnológica e sustentabilidade reflete-se no desenvolvimento de soluções que buscam não apenas a geração de valor económico, mas também o respeito aos limites ecológicos e a promoção de práticas empresariais socialmente responsáveis.

Nesse sentido, a inovação tecnológica contribui diretamente para o alcance dos Objetivos de Desenvolvimento Sustentável (ODS) das Nações Unidas[234], principalmente nas áreas de energia renovável, eficiência energética, agricultura sustentável e gestão de resíduos, onde novas tecnologias têm o potencial de transformar setores inteiros, tornando-os mais ecológicos e eficientes.

[234]Os Objetivos de Desenvolvimento Sustentável (ODS) foram adotados pelas Nações Unidas em 2015 como uma agenda universal para erradicar a pobreza, proteger o planeta e garantir que todas as pessoas desfrutem de paz e prosperidade até 2030. A agenda inclui 17 objetivos interligados que abrangem dimensões económicas, sociais e ambientais do desenvolvimento sustentável. Mais informações disponíveis em: https://sdgs.un.org/goals.

A proteção de inovações tecnológicas, por meio do sistema de propriedade industrial, assegura que os inventores e empresas possam se beneficiar dos seus investimentos, que cria um incentivo para o desenvolvimento de novas soluções que atendam a essas necessidades, sem que as inovações sejam rapidamente copiadas, o que poderia desincentivar a pesquisa e o avanço em áreas estratégicas para a sustentabilidade. No contexto português, a criação de um sistema jurídico robusto para a proteção dessas inovações, aliado ao incentivo à pesquisa e ao desenvolvimento tecnológico, é fundamental para promover o surgimento de soluções que possam ser aplicadas em diversas áreas, desde o uso de energias limpas até a redução da pegada ecológica nas indústrias.

Além disso, a inovação tecnológica sustentável tem o potencial de criar um ciclo virtuoso que não apenas impulsiona a economia, mas também contribui para a criação de empregos verdes e o fortalecimento de uma economia de baixo carbono. A implementação de tecnologias que favorecem a eficiência no uso de recursos naturais, a redução de emissões de gases de efeito estufa e a minimização do impacto ambiental das atividades humanas é crucial para que as empresas se alinhem com os requisitos globais de sustentabilidade.

A proteção jurídica dessas inovações no ordenamento jurídico português facilita a entrada das empresas no mercado global, proporcionando um diferencial competitivo, pois a sustentabilidade tornou-se um fator estratégico para consumidores e investidores, que cada vez mais priorizam empresas comprometidas com a responsabilidade ambiental. Dessa forma, a inovação tecnológica não apenas atende a exigências ambientais e sociais, mas também abre portas para novos mercados.

Conclusão

A pesquisa desenvolvida partiu da premissa de que o ordenamento jurídico português, consolidado pelo Código da Propriedade Industrial e em conformidade com tratados internacionais, desempenha um papel estratégico na promoção da inovação tecnológica e económica. A investigação foi direcionada por uma análise crítica sobre como a legislação nacional garante proteção eficaz aos direitos de propriedade industrial, mesmo diante das rápidas transformações globais. Esse ponto de partida demonstrou ser relevante para compreender as interações entre direito, economia e tecnologia no contexto contemporâneo.

O exame detalhado dos instrumentos jurídicos previstos no Código da Propriedade Industrial revelou a existência de um sistema robusto e tecnicamente fundamentado, porém ainda suscetível a desafios práticos.

A análise apontou que a legislação portuguesa oferece proteção ampla por meio de patentes, marcas, desenhos industriais e segredos comerciais, assegurando segurança jurídica aos titulares desses direitos. Contudo, a complexidade dos processos e os custos elevados foram identificados como entraves que impactam negativamente o acesso a esses instrumentos, especialmente para pequenas e médias empresas.

A investigação sobre o impacto das normativas internacionais, como a Convenção de Paris e o Acordo TRIPS, demonstrou que a integração de Portugal a esses tratados reforçou a harmonização legislativa e aumentou a competitividade no cenário global onde também foi possível analisar que O Código da Propriedade Industrial, em consonância com as normativas europeias e internacionais, assegura que as inovações, sejam elas patenteadas, registadas como marcas ou protegidas de outras formas, gozem de um regime jurídico eficaz, permitindo que empresas portuguesas se destaquem no mercado global.

Contudo, as barreiras económicas ainda representam um desafio significativo para as pequenas e médias empresas (PMEs), que, frequentemente, não conseguem acessar o sistema de proteção devido aos custos elevados de registo e manutenção. Além disso, a efetividade das sanções contra pirataria e concorrência desleal continua sendo um tema relevante, uma vez que a aplicação das leis ainda enfrenta dificuldades, principalmente no ambiente digital e transnacional.

Os dados analisados evidenciaram que esses acordos consolidaram padrões mínimos de proteção e garantiram reciprocidade jurídica, beneficiando os titulares de direitos industriais. Contudo, observou-se que a implementação prática ainda enfrenta desafios relacionados à fiscalização e à adequação das normas às especificidades locais.

A pesquisa também identificou os principais desafios enfrentados pelos titulares de direitos de propriedade industrial em Portugal, incluindo a pirataria, a concorrência desleal e a violação de patentes. A análise crítica indicou que, embora existam mecanismos legais para combater essas infrações, como ações judiciais e medidas cautelares, a morosidade dos processos judiciais compromete a eficácia dessas ferramentas. Nesse aspeto, a necessidade de modernização administrativa e de maior celeridade nas decisões jurídicas foi amplamente discutida e evidenciada.

Outro aspeto relevante foi a análise das perspetivas futuras para a tutela da inovação no contexto tecnológico. A transformação digital, associada a tecnologias como blockchain e inteligência artificial, foi identificada como uma oportunidade para superar os desafios existentes. A investigação sugeriu que a adoção de soluções tecnológicas poderia reduzir a burocracia e aumentar a eficiência dos processos de registo e fiscalização, promovendo um ambiente jurídico mais dinâmico e transparente.

A combinação de métodos teóricos e exploratórios foi suficiente para sustentar as conclusões obtidas, validando a escolha metodológica como apropriada para a pesquisa. O estudo concluiu que o ordenamento jurídico português apresenta bases sólidas para a proteção da propriedade industrial, mas enfrenta desafios que exigem reformas legislativas e administrativas.

A pesquisa propõe, como solução, a ampliação do uso de tecnologias digitais, a revisão dos processos administrativos e o fortalecimento da fiscalização. Essas medidas, se implementadas, poderão tornar o sistema jurídico português mais

eficiente e adaptado às demandas de um mercado global em constante transformação.

No contexto das novas tecnologias emergentes, como inteligência artificial e blockchain, surge a necessidade urgente de adaptar as legislações existentes para garantir que as criações tecnológicas mais recentes também sejam devidamente protegidas. Essas tecnologias não apenas desafiam os conceitos tradicionais de titularidade e autoria, mas também abrem novas oportunidades para a proteção e registo de inovações, desde que o ordenamento jurídico se atualize para acompanhar a complexidade.

Referências

AZEVEDO, J.B. (2020). **A Proteção do Investimento Estrangeiro - Uma Nova Política Europeia?** https://www.academia.edu/45607727/A_PROTE%C3%87%C3%83O_DO_INVESTIMENTO_ESTRANGEIRO_UMA_NOVA_POL%C3%8DTICA_EUROPEIA

ALMEIDA, P. (2021). Direito da Propriedade Industrial: Atualizações e Desafios no Contexto Português. **Revista Jurídica Luso-Brasileira**, v. 7, n. 1, p. 12-28.

ASCENSÃO, J. O.; VICENTE, D. M. (2002). **Direito da Propriedade Industrial**. Coimbra: Almedina.

COSTA, A. (2023). Propriedade Intelectual e Validação de Patentes: os Guardiões da Inovação em Portugal. **Revista de Propriedade Intelectual e Inovação**, v. 8, n. 3, p. 89-105.

BARBOSA, D. B. (2002). **A Propriedade Intelectual como um direito de cunho internacional**. Rio de Janeiro: DBBA, 2002. https://www.dbba.com.br/wp-content/uploads/pi_direito_internacional.pdf

CAMPOS, S. L. B.; FIGUEIREDO, J. M. (2022). Aplicação de inteligência artificial no ciclo de políticas públicas. **Cadernos de Prospecção**, v. 15, n. 1, p. 196-214. https://periodicos.ufba.br/index.php/nit/article/view/42957

CRUZ, D. C. (2023). **Na luta contra a contrafação: o papel da Polícia de Segurança Pública no combate ao fenómeno e no enforcement dos Direitos de Propriedade Industrial**. https://comum.rcaap.pt/bitstream/10400.26/46048/1/D8%20-%20TIF_Dennis%20Cruz_Na%20luta%20contra%20a%20contrafa%C3%A7%C3%A3o%20O%20papel%20da%20PSP%20no%20combate%20ao%20fen%C3%B3meno%20e%20n o%20enforcement%20dos%20DPI_152256.pdf

CRUZ, R. (2018). **Os reflexos da mundialização do TRIPS na regionalização da União Europeia**. Dissertação. Lisboa: Instituto Nacional da Propriedade Industrial. https://inpi.justica.gov.pt/Portals/6/PDF%20INPI/Teses%20Acad%C3%A9micas/Os%20reflexos%20da%20mundializa%C3%A7%C3%A3o%20do%20TRIPS%20na%20regionaliza%C3%A7%C3%A3o%20da%20Uni%C3%A3o%20Europeia%20-%20Rui%20Cruz.pdf

GIL, A. R. (2018). **A Autorização de Residência para Atividade de Investimento (ARI)**. Dissertação. Faculdade de Direito da Universidade de Lisboa, Lisboa. https://repositorio.ulisboa.pt/bitstream/10451/34111/1/ulfd135393_tese.pdf
GONÇALVES, Luís Couto. **Propriedade Industrial**: Volume I. Lisboa: Quid Juris, 2013.
GONÇALVES, Nuno Manuel da Silva. **A Função Social do Direito de Autor**. Coimbra: Almedina, 2005.

GONÇALVES, L. C. (2023). **Código da propriedade industrial anotado**. Leya. https://books.google.com.br/books?hl=pt-BR&lr=&id=kRPMEAAAQBAJ&oi=fnd&pg=PA5&dq=C%C3%B3digo+da+Propriedade+Ind ustrial+(CPI)+portugal&ots=sU5-76OxIC&sig=85ocfKlwPmsSpOsdcnp3GgV5J6o#v=onepage&q=C%C3%B3digo%20da%20Propriedade%20Industrial%20(CPI)%20portugal&f=false

PAIS, S. O. (2019). **Entre Inovação e Concorrência**. Coimbra: Almedina.

PEREIRA, A. D. (2012). **Direitos de Autor e Liberdade de Informação**. Coimbra: Almedina.

PEREIRA, A. D. (2015). **Direito da Propriedade Intelectual & Novas Tecnologias**. Coimbra: Almedina.

PIMENTEL, L. O. (2016). **Propriedade Intelectual**: Aspectos Jurídicos, Econômicos e Sociais do Direito à Informação. Florianópolis: Editora do Autor.

PIMENTEL, L. O. (2021). **Fundamentos do Direito da Propriedade Industrial**. Rio de Janeiro: Lumen Juris.

PINTO, M. (2021). Inovação tecnológica e propriedade intelectual: Um estudo acerca da inovação tecnológica e da defesa da propriedade intelectual no âmbito empresarial. **Revista Brasileira de Direito Empresarial**, v. 5, n. 2, p. 75-90.

PORTUGAL. **Decreto-Lei n.º 110/2018**, de 10 de dezembro. Código da Propriedade Industrial. Aprova o novo Código da Propriedade Industrial e transpõe para a ordem jurídica interna as Diretivas (UE) 2015/2436 e 2016/943.

ROCHA, C. A. (2022). **Blockchain como ferramenta de registro e proteção da propriedade intelectual**. https://repositorio.ufc.br/handle/riufc/71903

RUSSI, A. (2020). LICENCIAMENTO COMPULSÓRIO NA PROPRIEDADE INDUSTRIAL: UMA VISITA À LEGISLAÇÃO LUSITANA. **Unisul de Fato e de Direito: revista jurídica da Universidade do Sul de Santa Catarina**, v. 10, n. 20, p. 23-28. https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/UNISUL_n.20.pdf#page=12

SILVA, J. (2024). Propriedade Industrial: o motor invisível do crescimento económico e da inovação. **Revista Portuguesa de Economia e Gestão**, v. 12, n. 4, p. 121-140.

SILVA, P. S. (2011). **Direito Industrial**. Coimbra Editora, Coimbra.

SOUSA, M. (2023). Uso da Propriedade Industrial em Portugal na perspetiva internacional. **Revista de Direito Internacional e Comparado**, v. 15, n. 1, p. 58-73.

TRINDADE, L. (2019). O novo quadro legal da Propriedade Industrial em Portugal. **Revista de Direito Intelectual**, v. 20, n. 1, p. 25-42.

A metamorfose do Direito global: uma análise sobre o seu sentido atual e/ou virtual [235]

[235] O senso comum possui uma forte tendência em qualificar o real em oposição ao virtual.

Suellen Assunção Abbade [236]

Resumo

A lógica do pensamento moderno acerca do Direito encontra-se em crise. A tradição do formalismo – entendido como um autorreferencialismo baseado em discurso egocêntrico de conceitos, institutos e de Direito – não mais é suficiente para explicar e permitir a compreensão do Direito moderno. As plataformas digitais revelaram um mundo baseado no universal – diferente daquele sentido totalizante do formalismo. O mundo pulverizou-se e o sentido de Direito também. Já não bastam instituições para regular as relações sociais. As escoras que até então balizavam o comportamento, revelam-se agora insuficientes. Surge, assim, a necessidade de compreensão dessas novas forças nascidas da perspectiva do virtual. De modo que conceitos como sociedade, cultura, social-histórico e *psique* ganham importância na identificação daquilo que é pertencente à *sociedade instituída* e à *sociedade instituinte*. Nesse passo, o Direito apresenta-se como uma virtualização da realidade atual, de maneira que os processos de significação e simbolização fundamentais da instituição sejam considerados além do Estado, transformando a cultura em algo anterior ao Poder Constituinte.

Palavras-chave: Direito, Crise, Formalismo, Virtualidade, Sociedade instituinte, Sociedade instituída, Poder Constituinte.

The Metamorphosis of Global Law: An Analysis of Its Current and/or Virtual Meaning

Por esses termos, o real é aquilo que existe e que se porta dentro da realidade. Contrariamente, o virtual conduz a noção da ausência da existência e, portanto, simboliza a ilusão. Contudo, essa visão constitui uma imprecisão conceitual, pois o virtual deve ser compreendido na exata medida daquilo que os escolásticos definiam como uma potência. Isto é, o virtual seria aquilo que existe como potência e, como tal, suscetível de constante atualização, sem operar na concretude efetiva ou formal. No virtual, o real está latente, ao passo que o real é existente. Daí que, rigorosamente, "o virtual não se opõe ao real, mas ao atual". LÉVY, Pierre, **O que é virtual?** p. 15.

[236] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Abstract
The logic of modern thinking about Law is facing a crisis. The formalism tradition - understood as a self-referentialism based on an egocentric discourse of concepts, institutes and the Law - is no longer sufficient to explain and understand modern Law. Digital platforms have revealed a world based on the universal - different from the totalising sense of formalism. The world has become pulverised and so has the meaning of Law. Institutions are no longer enough to regulate social relations. The pillars that had previously guided behaviour are now proving to be insufficient. Thus, the need arises to understand these new forces born from the perspective of the virtual. Concepts such as society, culture, the social-historical and the psyche become more important in identifying what belongs to the instituted society and the instituting society. In this way, the Law presents itself as a virtualisation of current reality, so that the institution's fundamental processes of signification and symbolisation are considered beyond the State, transforming culture into something prior to the Constituent Power.

Keywords: Law, Crisis, Formalism, Virtuality, Instituting society, Instituted society, Constituent Power.

Introdução

O Direito moderno perdeu, de certa forma, a sua referência com a ascensão do mundo global a partir da digitalização (da realidade insculpida por meio das plataformas). Este trabalho se ocupa precisamente deste fenómeno jurídico moderno, que se distancia de qualquer determinismo obtido por meio das instituições estatais ou de si mesmo. Desse modo, não se vai falar de um Direito da sociedade, mas de um Direito na sociedade, já que faz parte de um processo de coevolução entre o virtual e atual. Sendo o Direito o virtual e a sociedade instituída o atual, procuramos explicitar primeiramente todas as fases de coevolução humana e do Direito, explicitadas nas culturas do *gentleman*, do gestor e do *homo digitalis*. É para este último que a nossa atenção se voltará. Após, passaremos a analisar a falência da sociedade instituída, considerada como único modelo assegurador da

transformação social e do Direito. Pois, o Direito positivado é antes de tudo um produto da sociedade instituinte. A leis deixam de ter uma importância isolada e passam a compartilhar com a cultura estruturas em que o desenvolvimento atual se escora. Por último, vamos analisar o Direito global no mundo digital a partir das plataformas como realizadores de novas relações sociais e originando uma análise do Direito por um viés híbrido, formado por fatores internos (*psique*) e externos (sociedade instituída), que caracterizam uma verdadeira simbiose entre a hierarquia e heteronomia.

1. Breve excursão sobre a personalidade do Homem criativo

Não nos surpreende a ideia de que os *Homo Sapiens* teriam experimentado de um privilégio evolutivo para chegarem onde chegaram. Afinal, qual outro animal desenvolveu habilidades notoriamente tão complexas e flexíveis, do ponto de vista cognitivo, quanto os *sapiens*?

Todos sabemos que tudo ao nosso redor está em constante modificação. Aliás, pode-se estender a compreensão de vida pela mudança. E, dentro deste conceito, sabemos que, embora o planeta Terra tenha surgido há cerca de 3,4 bilhões de anos, os primeiros registos fósseis de seres parecidos aos humanos são muito mais recentes, datando cerca de 4 milhões de anos. Portanto, somos os frutos recentes de uma transformação no tempo, denominada "evolução", a qual foi reconhecida somente há menos de 200 anos.

De lá para cá, o próprio conceito de "evolução" mudou. Passamos da compreensão de uma progressão rumo à perfeição para a de simples mudança ao longo do tempo[237], de modo que atualmente sabemos que nada há de especial ou extraordinário no desenvolvimento do *Homo Sapiens* e, em corolário do seu cérebro, além do experimentado por outros animais: uma mudança ao longo do tempo definida por certas circunstâncias. Circunstâncias tais que acabam por revelar a existência de uma fascinante variedade de vida na Terra, categorizada, pelo menos, desde Aristóteles.

Aristóteles qualificou as diversas formas visíveis a olho nu de vida na Terra, organizando-as segundo uma escala hierárquica, fixadas em ordem decrescente desde a Causa primeira no topo até os minerais na base, ficando os animais numa posição intermediária, classificados segundo o "grau de perfeição de suas almas"[238]. Tomando como base isso, por muito tempo, considerou-se que dentro de uma escala da natureza o Homem figurava como superior, estando apenas abaixo de Deus.

---

[237] HERCULANO-HOZEL, Suzana, **A vantagem Humana – Como nosso cérebro se tornou superpoderoso**, p. 20.

[238] VIEIRA, Ariza Fabiana Vieira; MARTINS, Lilian Al-Chueyr Pereira, A scala naturae de Aristóteles no tratado De Generatione Animalium. In **Filosofia e História da Biologia**, vol. 5, n. 1. São Paulo: Universidade de São Paulo, 2010. [consult. 8 nov.2024], p. 29 e ss. Disponível na internet:< https://biblat.unam.mx/es/revista/filosofia-e-historia-da-biologia/articulo/a-scala-naturae-de-aristoteles-na-obra-de-generatione-animalium < ISSN 1983-053X.

Somente nos séculos XVIII e XIX o conceito de mutabilidade foi incorporado ao conjunto de todos os seres. Assim, com Charles Darwin, em 1859, acrescentou-se à evolução o eixo temporal. Daí que para muitos a ideia de evolução fosse baseada na progressão dos seres, nos exatos termos da figura abaixo.

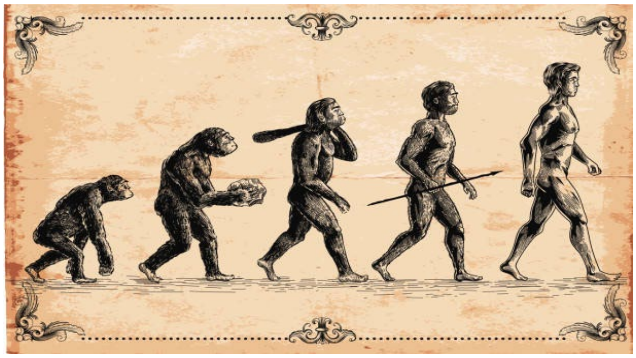


Figura 1[239]

Hoje sabe-se que a ideia de escala evolutiva ascendente está ultrapassada, visto que as espécies nem sempre "evoluem" para formas mais complexas, a exemplo da existência abundante de seres unicelulares. Há evidência até de seres que num passado foram maiores e mais complexos do que os de hoje. Isso indica-nos que o termo "Evolução" significa mudança ao longo do tempo e não progresso. Assim, "quando muda o programa do desenvolvimento, surgem novas formas, nem mais nem menos «avançadas»: apenas diferentes"[240].

Essa "diferença", baseada no avanço, permitiu ao Homem tornar-se num ser criativo. Thomas Vesting destaca, pelo menos, três momentos criativos do Homem ocidental: o *gentleman,* o gestor e o *homo digitalis*[241]. Todos eles contribuindo para a formação e desenvolvimento de uma cultura dos direitos universais de liberdade, porém, não no sentido formal, mas no plano sociocultural, de modo que Direito e cultura caminhem juntos numa perfeita coevolução.

1.1. Cultura do *gentleman*

O *gentleman*, em que pese suas variações linguísticas designativas, é referido, neste trabalho, sob a perspectiva do Homem burguês do século XVIII. Este, um indivíduo, dotado de boa educação e espírito de cooperação com pessoas do mesmo nível social, é definido dentro de um espaço, onde tanto o conhecimento como os ideais

[239] Disponível em: https://www.gettyimages.pt/search/2/image?phrase=evolução.
[240] HERCULANO-HOZEL, Suzana, **A vantagem Humana – Como nosso cérebro se tornou superpoderoso**, p. 27.
[241] VESTING, Thomas, **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade jurídica na modernidade**, p. 15.

comuns exercem a função reconciliadora – no ambiente interno da subjetividade – com as forças da *psique*[242].

A cultura, entendida como uma segunda natureza do Homem seria "transmitida por imitação e por hábito"[243]. O mundo técnico representa bem isso. Não representa apenas um mundo de ferramentas inventivas, muito além, representa a possibilidade de uma liberdade criativa, "Quando o homem começa a interpretar seu presente historicamente a partir da própria necessidade de posicionamento excêntrico no mundo, uma forma mais calculada da mudança social anuncia-se: a referência à tradição é flexibilizada e substituída por uma subjetividade prospectiva"[244]. Isto é, o Homem extravasa aquele papel simplesmente emulativo da sua tradição para criar a abertura de novas possibilidades. O grande problema desse comportamento, ao nosso ver, é que ele cria uma ilusão, pois a visão de mundo termina por fixar-se numa base irrealista que submina[245] ou supramina[246] os entes que compõe o mundo, no entanto, isso será melhor explicado *infra*. Por hora, basta compreendermos que essa fixação basilar na tradição, embora crie no sujeito uma base correlacional – raízes na historicidade –, termina por dificultar-lhe o desprendimento à ligação a um determinado lugar, de modo a impossibilitar sua transformação num "sujeito sem mundo"[247]. A ideia de progresso desse Homem burguês primevo encontra-se cravejada numa justificativa histórica, de modo que o presente se dê baseado na correlação entre o passado e futuro, ignorando, portanto, a possibilidade de um mundo moldado em incertezas.

"A transição da corte para a cidade"[248] fez nascer uma nova classe de sujeito: o sujeito burguês romântico moderno, localizado dentro da chamada classe média liberal, em que a ideia de interioridade traz o resgate da autonomia privada, pois o surgimento do sujeito autónomo (considerado como individualidade), configura uma transformação na sociedade, onde comerciantes, negociantes, artesãos, mecânicos e etc. dificilmente voltam-se para o mundo em geral, mas centra-se no seu modo de vida (no seu círculo social). Daí a ideia de centralização estatal, já que as vizinhanças se relacionavam em rede, de tal sorte que se deslocou a noção de soberano para uma "cadeia de autoridade hierárquica"[249]. Por outro lado, numa

---

[242] VESTING, Thomas, **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade jurídica na modernidade**, p. 99.

[243] MUNFORD, Lewis, **As Tansformações do Homem, trad. Fernanda Barão e Isabel Fernandes**, p. 39.

[244] VESTING, Thomas, **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade jurídica na modernidade**, p. 105.

[245] Considera os objetos que compõem o mundo como algo rasos demais para fundamentar a realidade. HARMAN, Graham, **O objeto Quádruplo – uma metafisica das coisas depois de Heidegger**, p. 40-44.

[246] Considera certa importância aos objetos, porém retira essa importância ao esgotar seu valor na relação com outros. HARMAN, Graham, **O objeto Quádruplo – uma metafisica das coisas depois de Heidegger**, p. 44-47.

[247] VESTING, Thomas, **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade jurídica na modernidade**, p. 106.

[248] CAMPOS, Ricardo, **Metamorfoses do Direito Global- Sobre a interação entre Direito, Tempo e Tecnologia**, p. 174.

[249] VESTING, Thomas, **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade**

vertente mais anglo-americana, a ordem liberal não se baseava num Direito definido *ex ante*. Pelo contrário, partia-se da noção de que a sociedade era formada por instituições e que estas encontravam-se na *psique* dos indivíduos, de modo que eles nelas se apoiassem aquando da estruturação da sua interioridade complexa[250]. Assim, todos os direitos formais seriam produto da confrontação prática com o mundo. Este seria o gérmen moderno da diferenciação do mundo do *civil law* para o *common law*.

A concepção europeia abraçada entre Estado e Sociedade fez surgir a crença de que os direitos subjetivos nascem da liberdade do indivíduo. No entanto, o cenário ideal seria não contemplar uma liberdade pré-estatal nos moldes anglo-americanos, que deixa suspensa uma liberdade quase que ilimitada, nem uma forte negação dessa liberdade como suposto pelos moldes europeus do *civil* law.

O que se vislumbrou para o Estado, no desenvolvimento da sociedade jurídica de matriz romano-germânica, foi o papel de mero formalizador das relações entre os indivíduos. Contudo, com o evoluir do tempo, esse poder da "vontade humana" – insculpido pelo Direito privado e reservado ao Estado a sua formalização – viu a ampliação da necessidade dessa formalização, de tal maneira que a figura estatal ganhou tanta relevância no campo dos Direitos ao ponto do Direito Público ser por ele absorvido, bem como o Direito subjetivo ser transformado numa concessão de poder desse mesmo Estado em proveito do particular. Logo, a "vontade das pessoas" passou a ter um papel secundário para dar primazia à formalização da subjetividade. A busca por uma certeza ganhou força frente à liberdade. A estabilidade – como fator primordial do mundo jurídico – limitou a esfera de exercício desses direitos subjetivos, que devem sempre encontrar-se na posição de um expectante da tutela estatal[251].

1.2. Cultura do *gestor*

A cultura gestorial, por sua vez, é marcada pelo surgimento das grandes empresas de produção industrial em massa. Aqui, aquele ideal burguês *gentleman* perde força, cedendo espaço para o gestor. Antes, a figura principal era do indivíduo (o empresário autônomo – *self-made man*), agora o espaço é ocupado principalmente pelos *managers*.

O capitalismo, estruturado na produção em massa, advém de uma necessidade pública[252]. Ora, se de um lado subsiste uma classe que verga pelo luxo

jurídica na modernidade, p. 164.

[250] VESTING, Thomas, **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade jurídica na modernidade**, p. 174/175.

[251] Shoshana Zuboff afirma que "a liberdade é apenas ignorância à espera de ser conquistada". Com efeito, retratando a ideia do poder instrumentarista exercido pelo capitalismo da vigilância na busca pela pré-definição dos nossos comportamentos. Esse assunto será retomado mais à frente. ZUBOFF, Shoshana, **A Era do Capitalismo da Vigilância – A disputa por Um Futuro Humano na Nova Fronteira do Poder**, p. 405.

[252] ZUBOFF, Shoshana, **A Era do Capitalismo da Vigilância – A disputa por Um Futuro Humano na Nova Fronteira do Poder**, p. 47.

e pelo consumo de bens de primeira linha, do outro eclode uma volumosa classe de assalariados que, embora tenham pouco, não deixam de sonhar com o muito. Foi de olho nessa necessidade pública gerada no seio dessa classe desprovida de grandes recursos e privilégios – mas que deseja o mais – que Henri Ford desenvolveu seu modelo de produção, transformando uma produção de artigos de luxo, diferenciada e de alto custo, numa produção padronizada, em grande volume e de baixo custo. Surgia o *fordismo* – derivado das novas formas de mercado mais produtivas e de acordo com a mentalidade do povo. A especialização aqui é elemento *sine qua non* no desenvolvimento dessa novel forma de engrenagem industrial, diante da produção de larga escala.

O sociólogo Émile Durkheim considera o *mercado* como uma instituição, isto é, como um fato social. Desse modo, "a *causa* da mudança do fenômeno industrial – fábricas, especialização, divisão complexa do trabalho – residiria única e exclusivamente da emergência de *novas condições existenciais*, designativas de uma vida eficaz"[253]. Logo, a especialização não ocorre para produzirmos mais, "mas para podermos existir nestas novas condições existenciais que nos foram atribuídas"[254]. É simplesmente esse movimento natural de eterna busca humana por uma vida eficaz a causa geradora desses fenómenos de mercado. Nela, o Homem se reinventa.

A cultura gestorial é associada a cultura do *gentleman*, pois aquele conhecimento burguês repartido por entre os indivíduos, caracterizado por ser amador, artesanal, encontrava-se disperso na sociedade, como uma cultura geral (universal). Já na cultura gestorial, ele (conhecimento) desloca-se para as academias, tornando-o mais profissionalizado e concentrado no espaço fabril. Assim, se antes o empresário poderia aglutinar diversas funções (gestor, engenheiro, comerciante e etc.), o gestor é especializado, com determinadas qualificações técnicas, de modo que departamentos são criado para absorver essas especializações. "Com isso, a totalidade das qualificações e inteligência concentrada na empresa tornam-se tão complexas que ninguém mais consegue ter uma visão geral delas"[255]. Aqui a produção de conhecimento é transferida para a empresa. Ele não está preso naquela formação humanística e isso permitiu uma maior liberdade criativa, pois o conhecimento produzido é compartilhado entre as diversas instituições.

Cumpre ressaltar que aquela diferença existente entra a cultura burguesa anglo-americana e a europeia continental, é transferida também para essa cultura gestorial. Tanto que de um lado vê-se claramente emergir um capitalismo gestorial competitivo (*competitive managerial capitalism)*, enquanto na outra ponta, é

[253] ZUBOFF, Shoshana, **A Era do Capitalismo da Vigilância – A disputa por Um Futuro Humano na Nova Fronteira do Poder**, p. 48.
[254] ZUBOFF, Shoshana, **A Era do Capitalismo da Vigilância – A disputa por Um Futuro Humano na Nova Fronteira do Poder**, p. 48.
[255] VESTING, Thomas, **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade jurídica na modernidade**, p. 217.

alimentado um capitalismo gestorial cooperativo (*cooperative managerial capitalismo*)[256].

Na gestão competitiva, as atenções são orientadas para a descoberta e exploração de novos mercados, da auto-organização social e da criação de novas instituições privadas. Na gestão cooperativa, ao revés, a finalidade das grandes empresas dá-se fincada no interesse do Estado nacional. Assim, as empresas que competem entre si chegam a formar cartéis sob a tolerância do Estado em prol do aumento do seu desempenho econômico, ou até mesmo em prol de finalidades político-militares[257].

Na cultura do *gentleman,* o conformismo social (caráter social[258]) se orienta pelas expectativas formadas pela sociedade, ao passo que a consciência do indivíduo burguês é orientada de acordo com o tipo ideal de caráter concebido internamente por ele. O *homo* gestor, por sua vez, tem a sociedade em que está inserido como seu grande espelho, embora tenha como importante o comportamento dos seus pares. Logo, seria impreciso considerar o desenvolvimento da sociedade burguesa como direcionada do Homem dirigido internamente para aquele dirigido externamente. Não se pode ignorar a figura do outro (terceiro independente: a sociedade). A sociedade baseada nos sistemas não parte de uma conformação interna do Homem, mas o considera como um ser biológico, físico, psíquico e social, de modo que a sociedade não seja produto de uma *psique* humana, mas sim resultante da comunicação entre homens. Logo, intenção, desejos e finalidades estão relacionados ao que se comunica: a sociedade. Com isso, tanto o aspecto interno como externo coexistem de modo a confluírem na figura de um terceiro que é responsável pelas condições de possibilidade da ordem social[259].

A análise a partir dessa perspectiva revela duas sociedades ocidentais distintas: a anglo-saxônica e a europeia ocidental. Na primeira, existe a primazia da ideia de fragmentário, fracionado e relativo. Na segunda, parte-se do senso de

---

256 VESTING, Thomas, **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade jurídica na modernidade**, p. 223.

257 VESTING, Thomas, **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade jurídica na modernidade**, p. 223.

258 A leitura de caráter social trabalhada neste texto é aquela em que a personalidade é definida pela experiência de grupo. Nas sociedades com alto potencial de desenvolvimento, cria no seu grupo uma forte tendência de seguir a tradição, chamados de grupos *dirigidos pela tradição*. Aquelas sociedades, por outro lado, que ainda se encontram em transição, possuem uma tendência de firmar seus grupos dentro da sua concepção, de modo a internalizar suas finalidades. A estas são categorizadas como internamente dirigidas, pois as pessoas e a própria sociedade são dependentes de uma *direção interna*. Agora, aquela sociedade de incipiente população em declínio tendenciam a ser afetadas pela expectativas e preferências dos outros, por isso, dependentes de direção exterior (alheia). Definem-se, portanto, como *dirigidas externamente*. RAMOS, Edith, Um exame da tipologia do caráter social de Riesman. In **Arquivo brasileiro de Psicologia aplicada**. Rio de Janeiro, 1975. [consult. 8 nov. 2024], p. 41. Disponível na internet: < https://periodicos.fgv.br/abpa/issue/view/1153 >

259 LUHMANN, Niklas, **La moral de la sociedad**, p. 103 e ss.

substancial, total e solipsista[260]. Acima, essa diferença já ficou bem delineada e ela nos permite compreender a noção do Estado em cada uma delas. Enquanto numa o modelo de subjetivação, baseado não no autocontrole e na auto-organização, marca a cultura do gestor – centrada na fragmentação do espaço social, onde a espontaneidade como mecanismo de coordenação dirige os mercados –, na outra ocorre exatamente o contrário: centralização do espaço social na figura do Estado que conduz o gestor a submeter-se sempre a uma autorização proveniente das criações estatais. Lá, há o apelo pela desburocratização. Aqui, há o seu endeusamento, criando-se o que Weber denominou de "soberania burocrática"[261], onde o espaço empresarial é um mero reflexo do espaço político.

O gestor, antes de um Homem econômico, é um Homem político. Isso é refletido inclusive na teoria luhmaniana, quando considera as empresas privadas e a administração pública como apenas expressões diferentes para designar o mesmo tipo de organização formal, portanto, há uma diluição de ambas na burocracia.

É importante ter em mente o quanto a mutabilidade cultural tem impactos na formação de uma cultura jurídica. O gestor anglo-saxão tem como algo comum (natural) a ideia de uma sociedade auto-organizadora, logo, para ele, o Direito já existe antes mesmo de qualquer formalização Estatal. O gestor continental está sempre à espera da carruagem burocrática, de modo que quando ela chega, já não consegue atender suas necessidades de tão anacrónica que é. O Direito, sob este ponto de vista, sempre será a sombra defasada de uma sociedade submissa a um *Leviatã,* cujo ego solipsista amarra, deturpa e cria anomalias.

1.3. Cultura do *homo digitalis*

A transposição do gestor para o *homo digitalis* desloca a capacidade criativa do Homem do ambiente das grandes empresas e seus departamentos de pesquisas para o desenvolvimento dos chamados "*clusters* de alta tecnologia constituídos entre empresas, instituições de pesquisa, universidades, investidores de risco e outros atores"[262]. Assim, a cooperação migra das organizações corporativas estáveis para as *start-ups*, *spin-offs* e cooperação entre empresas na forma de projetos.

A cultura do *homo digitalis* fundamenta-se na ideia de um mundo virtual. Mundo este que nada tem de ilusório, pois assenta na ideia de atualização, instaurando um "verdeiro devir que alimenta de volta o virtual"[263]. Por outras palavras, a noção de virtual é contraposta a de atual, pois o virtual é uma tendência que acompanha uma situação (um acontecimento) que reclama por uma solução (atualização). Dessa forma, a atualização seria essa *resposta* reclamada pelo virtual (possibilidades). Por consequência, a virtualização seria um movimento inverso da

[260] DELEUZE, Gilles, Walt Whitman. In **Essays critical and clinical**. Pennsylvania: University of Minnesota, 1997, p. 57.
[261] WEBER, Max, Economia e sociedade: Fundamentos da sociologia compreensiva, vol. I, p. 199.
[262] VESTING, Thomas, **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade jurídica na modernidade**, p. 267.
[263] LÉVY. Pierre. **O que é virtual?**, p. 17.

atualização. Enquanto a atualização persegue uma *solução* no sentido de uma estabilização, a virtualização concentra-se na *problematização*. Nesses moldes, a atualização partiria de um problema para uma solução, ao tempo que a virtualização se movimenta no sentido contrário, isto é, parte de uma solução (dada) para uma nova problematização a partir desta solução. "Com isso, a virtualização fluidifica as distinções instituídas, aumenta os graus de liberdade, cria um vazio motor"[264]. Por isso, diz-se que a virtualização é um dos principais vetores criativos da realidade.

Nesse contexto, o novo paradigma da plataforma – substrato da cultura da tecnologia e da informação – traz para o centro a já existente figura da virtualização[265], a qual reinventa o meio onde ocorrerão as interações sociais numa "não-presença"[266]. Esse abalo provocado no conceito de fronteiras e limites atinge os sistemas como um todo e, por consequência, também o sistema jurídico pautado na figura estatal.

A sociedade na era digital não se baseia mais naquela estabilidade promovida pela cultura gestora. Aqui, a realidade é pulverizada pela virtualização. As figuras do espaço-tempo são desatreladas das antigas concepções de território do "aqui" e do "agora", de sujeito, de bens, submetidos ao velho dogma do real. Mas, nem por isso, tornam-se ilusões. O espaço e tempo têm lugar e momento no ambiente virtual, embora aferidos de maneira diferente daquela cotejada pela ultrapassada ideia totalizante europeia[267].

---

[264] LÉVY. Pierre. **O que é virtual**?, p. 18.

[265] A memória, a imaginação o conhecimento, a religião e demais ficções já eram representações da virtualização praticada, mesmo antes do surgimento das redes digitais e da informatização. LÉVY, Pierre, **O que é virtual**?, p. 20.

[266] O filósofo Michel Serres fala do mundo virtual segundo a perspectiva da "não-presença". SERRES, Michel, **Atlas**, p. 135 e ss.

[267] O tempo é relativo desde antes da teoria de Einstein. Isso porque cada categoria de vida inventa sua forma de viver, isto é, o seu mundo. Dessa sorte, a noção de tempo e espaço de um inseto não é mesmo para outro, assim como não é o mesmo para o *homo sapiens*, que possui, sobretudo um universo cultural rico de maneira que a variabilidade do tempo e dos espaços são diversas. Um exemplo é a criação das redes de transportes que modificou e criou uma variante para a concepção de tempo e distância. Esse fenômeno é hoje mais eloquente porque temos a consciência de que não vivemos sozinhos e isolados no mundo. Os entes não podem ser mais subminados por baixo e tampouco supraminados por cima, pois acabam sendo submetidos a uma representação obsoleta ou, ao revés, a uma representação de caráter suplementar, geradoras de ilusões. Nesse sentido, seguimos a teoria de Graham Harman, quando fala da análise da realidade a partir da quadratura de quatro estruturas: o tempo, o espaço, a essência e o *eidos*. O tempo, para o autor, é interrelação entre a estabilidade e mudança e partindo dessa premissa estaria correlacionado com a virtualização, como contraposição da atualização. O espaço seria o lugar onde ocorrem as "relações e não relações", de modo que represente a "tensão entre os objetos reais velados e as qualidades sensitivas associadas a eles". Todavia, conjuminada com essa tensão surge uma outra: realizada a partir dos objetos e suas qualidades, da onde se retira o seu *eidos*, isto é o seu núcleo. É importante ressalvar que ele jamais será um produto dos sentidos, mas é adstrito ao intelecto. Finalmente, a quarta e última tensão consiste na relação entre o objeto real (objeto real unificado) e suas qualidades reais ocultas

Dessa leitura, fica evidente a mudança da tessitura dos sistemas com o desabrochar das, de tal maneira que a ordem já não esteja fincada numa centralidade. Numa rede, o máximo que se pode visualizar são nós maiores[268], bem como acessos provenientes de locais já bastante definidos. Com isso, noções de hierarquia, centralidade e poder central são escamoteadas por uma nova ordem originada "de estruturas descentralizadas, múltiplas e adaptáveis, que são abertas para o imprevisto e conseguem privilegiar o evento em relação à lei"[269].

A discussão traz à baila um antigo problema filosófico universal: será que as descobertas do mundo são frutos de um processo de criação ou, simplesmente, provenientes de revelações? Dito de outra forma, os processos ocorridos no mundo são os responsáveis por criar ou apenas por desnudar a realidade? Não é nossa intenção aprofundar a dúvida, entretanto, a resposta só parece ser possível a partir da análise melhorada dessa realidade. Ora, como já afirmamos *supra*, a virtualização não é um processo novo, o que é novo são as maneiras de interrelacionar esses acontecimentos com a realidade. A relação do Homem com os objetos e vice-versa é uma via necessária. Dessa forma, a percepção mais próxima da realidade só é possível a partir da consideração daquele quadrante explicado na nota de rodapé 31 deste trabalho, a qual ressalta que tempo, espaço, essência e *eidos* são interracionados entre si com e entre os homens.

Disso, extrai-se que a cultura é uma operação de cojuminação entre todos esses quadrantes, portanto, é virtual e como tal não se baseia na presença, mas na criação de novas conjunturas e relações a partir das soluções trazidas pelo que é atual. Daí, a nossa defesa na existência de uma tão obstinada coevolução entre o Direito e a sociedade (em sentido amplo)[270], já que ambos, sendo virtualização, extravasam a ótica do real e do atual. Quando muito, podem ser considerados como um problema a ser sempre repensado, mas nunca a ser solucionado (estabilizado), institucionalizado. Essa visão se demonstra como a mais adequada e que poderá oferecer a eficácia, em termos de coevolução, que os acoplamentos sistemáticos favorecem.

Portanto, o Direito é uma virtualização, assim como a sociedade em sentido amplo, transformado pela cultura e, com isso, dessicronizado do Estado. Haveria a desencarnação do Direito em relação ao Estado para uma reencarnação na cultura, na figura do Poder Instituinte.

(multiplicidades de qualidades). Como se pode verificar do dito acima, há sempre uma relação entre o homem e o objeto de vice-versa, de modo que um não seja mais importante que o outro, mas complementares na conformação da realidade. HARMAN, Graham, **O objeto Quádruplo – uma metafisica das coisas depois de Heidegger**, p. 151/152.

[268] "A rede não pode ser determinada de modo substancial, mas apenas relacional (conjunto de nós ligados)." VESTING, Thomas, **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade jurídica na modernidade**, p. 275.

[269] VESTING, Thomas, **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade jurídica na modernidade**, p. 270.

[270] A sociedade em sentido amplo é entendida como virtualização, pois não é capaz de ser materializada ou estabilizada tal como nos termos indicados *infra* na esfera do social-histórico, por isso, diz-se sê-la, nesse aspecto, virtualização. Não se fala neste momento ainda em institucionalização e, portanto, em atualização.

2. O Poder Instituinte como o meio de transformação do Direito global

2.1. O movimento da sociedade *instituinte* para a sociedade *institucionalizada*

A ideia de *instituição* foi densamente estudada por Cornelius Castoriadis para quem o sujeito, considerado isoladamente, não existiria, já que é um ser fabricado pelo social. Dessa forma, a concepção daquilo que é social e daquilo que é histórico encontrar-se-ia radicada na ideia de que a atividade humana representaria a criação e autotransformação da sociedade no tempo, no espaço, na essência e no *eidos*. Ao passo que o histórico estaria fincado na ideia da criação humana instituindo o social. Assim, o social-histórico, nesse contexto, denotaria o fundamento e a conexão entre duas dimensões: social e histórica. "O social é isso mesmo, auto-alteração, e nada é senão isso. O social faz-se e só pode fazer-se como história (...). O histórico é isso mesmo, auto-alteração desse modo específico de 'coexistência que é o social e nada fora disso"[271]. Dito de outra forma, o social-histórico é indissociável e denota o elo entre duas dimensões: sincrónica (simultaneidade) e diacrónica (sucessão) da permanente atividade humana criadora do social. Daqui pressupõe-se que a instituição social (fazer e pensar humano no tempo, no espaço, na essência e no *eidos*) é a própria história como uma rede diacrónica das sucessivas instituições sociais, de modo que o ato de dissocializar a história da instituição significaria o mesmo que pensar o mundo independente da sua criação.

Veja-se que o social-histórico imprime na sociedade um modo de organização. Salutar, seria, todavia, esclarecer que ela (organização) não é determinada por leis naturais e tampouco por considerações racionais, mas sim pelo "imaginário". Por esses termos, seria o produto da tensão e da união entre sociedade *instituída* e sociedade *instituinte*. Isto é, da "história feita e da história se fazendo"[272]. O social-histórico é visto unicamente por suas instanciações: linguagem, religião, leis, valores, costumes, usos e etc., entretanto, jamais limitado a elas. Excede-as. É lido sob a ideia do transbordamento em relação e aquilo que é instituído, pois é formado naquilo que é fenomenológico e também naquilo que é ontológico.

Destaque-se que a análise da realidade aponta para uma oposição que não se dá entre o indivíduo e a sociedade, mas entre a sua *psique* e a sociedade, haja vista que é na *psique* que se situa o nosso imaginário e a verdadeira liberdade. Nele, ocorrem todos os processos imaginários. A realidade, por esses termos, seria a representação de tudo que existe fora da *psique*. É o modo de ser da realidade psíquica e ao mesmo tempo é o constitutivo do indivíduo social. Por isso é inconcebível a existência do indivíduo num isolamento. Ele é pura fabricação do social. É verdade que sua *psique* é irredutível ao social, mas também é igualmente inquestionável o fato de que a socialização da *psique* é que implica na fabricação social do indivíduo, portanto, do sujeito. A isto Castordiaris chama de *sublimação*:

[271] CASTORIADIS, Cornelius, **A instituição imaginária da sociedade**, p. 252.
[272] CASTORIADIS, Cornelius, **A instituição imaginária da sociedade**, p. 131.

processo de constrangimento da *psique* que substitui seus objetos próprios – indiciados pelos impulsos nos termos freudianos – pelos objetos que valem *na* e *pela* instituição social[273]. Com isso, a socialização seria a obra de uma instituição cada vez mais mediada por indivíduos já socializados, denominados sujeitos.

Neste ponto, nasce o problema da autonomia e da heteronomia. A autonomia lida da pespectiva do indivíduo que cria e transforma por meio do social-histórico. E a heteronomia – que é a institucionalização da sociedade – age como um limite externo proveniente da instituição. Aqui nasce o grande problema do Direito: "combinar uma sociedade fundada em regras universais substantivas, e, compatível com a diversidade da criação, dos modos de vida e dos diferentes sistemas de necessidades"[274]. Assim, a autolimitação seria a comunicação entre a ideia de uma sociedade – entendida como universalidade – e a responsabilidade dos indivíduos, ambos cruciais para a autonomia. O dilema do Direito reside aqui naquilo que é a sua concepção como sistema aberto e fechado ao mesmo tempo. Isso reflete bem a ideia inicial de que o sujeito é produto da sociedade institucionalizada e instituinte, de modo que não possa existir no individualismo. Daí, o questionamento quanto ao fato de as organizações sociais (instituições) funcionarem como o rosto e o conteúdo do Direito, abrigando-se no rótulo de Estado e, por conseguinte, em algumas realidades, de democracia. O Direito, lido dessa forma, passa a ser observado a partir de rótulos ancorados na apatia do indivíduo.

É claro que o fato de o indivíduo possuir uma *psique* irredutível às forças socio-históricas impõe a necessidade de que haja instituições sociais, cuja tarefa seja fornecer um sentido, de modo a forçar e induzir o comportamento humano por caminhos mais sensatos. Fora a isso, teríamos o caos da *psique* singular, manifestada por meio das transgressões e das patologias psíquicas – embora, repise-se, elas sejam o substrato da alteração do mundo social. É aquele velho movimento diacrónico e sincrónico do social-histórico.

2.2. O poder instituinte na cultura do *homo digitalis*: uma nova leitura do Direito global

Frise-se que a noção de poder, dentro da teoria desenvolvida nesta pesquisa, perpassa pela concepção da uma espécie de sentido com capacidade de conduzir alguém a fazer aquilo que seria impossível de ser feito pelo indivíduo espontaneamente. Surge, assim, o indivíduo institucionalizado, pertencente a sociedade sem deixar de ser uma autopertença enquanto produto. Ou seja, o mesmo sujeito socializado (institucionalizado) reúne na sua *psique* a característica de ser um produto de si mesmo, assim, ele é considerado como aquele que modifica a sociedade, mas que é passível de ser modificado por esta mesma sociedade institucionalizada. É sujeito ativo e passivo desse social-histórico, pois não pode ser

[273] CASTORIADIS, Cornelius, **A instituição imaginária da sociedade**, p. 356.

[274] MEIRA, Fábio Bittencourt, Castoriadis (o instituinte) e a instituição. In **EnANPAD**. Rio de Janeiro, 2010. [consult.8 nov. 2024], p. 14. Disponível na internet: <https://arquivo.anpad.org.br/diversos/down_zips/53/eor1869.pdf>

considerado como um "ser" separado do mundo que o transforma e é transformado por ele.

Fala-se, destarte, no fechamento sistémico e na possibilidade de uma sua nova abertura. Enquanto uma força tenta aprisionar, a outra, por si, liberta. É o contraste entre o atual (escorado nas instituições) e o virtual (*psique instituinte*) que fazem do sistema um mecanismo dinâmico.

Por esses termos, o Direito – como um processo de virtualização – seria "sujeito a um poder instituinte antes de poder tornar-se objeto do Poder Constituinte"[275].

Viu-se que o poder instituinte é um poder social. Já se falou que o poder social é fruto da relação com e entre os seres e os entes. Os seus sentidos são extraídos dessa relação quádrupla representada pelo tempo, espaço, essência e *eidos*. Esses elementos relacionam-se entre si e dessa interação são retirados os sentidos que provocam a revelação da *sociedade instituinte* (hábitos coletivos de uma sociedade) cuja formalização transplanta-se na chamada sociedade institucionalizada (leis formalizadas), centralizada na figura do Poder Constituinte. O poder instituinte escapa, por esses termos, ao poder constituinte – considerado como a concretização do chamado "espírito da lei" (de Montesquieu), "poder do costume" (Rousseau) ou "moral" (Tocqueville). Extravasa-o, portanto.

O grande erro em desconsiderar a existência do poder *instituinte* dá-se pela confusão do universal com a totalização. O universal "é a presença (virtual) da humanidade em si mesma"[276]. A totalização representa a estabilização de sentidos de um sistema. Nesse jaez, o mundo digital (atual) da cibercultura[277] – desenvolvido nas plataformas – abre novos horizontes em direção a uma universalidade, entendida como um sistema de sentidos compartilhados que não visam jamais a sua apreensão novamente pela comunidade atual. Daí que, embora sedimentado no universal, não é aprisionado pelo conceito de total.

Por essa razão, a cultura digital não tem o poder de manufaturar o enfraquecimento do Direito, como assim defendeu Luhman[278] em sua tese sobre a anomalia do sistema. Mas, certamente, conduzirá ao enfraquecimento do Estado-nação, nos termos da percepção institucional de condições e requisitos pré-determinados.

A sociedade mundial caminha no sentido da universalização e o Direito, por conseguinte, segue não-somente a regulação. Impõe-se sobre ele o movimento de virtualização da cultura, de tal sorte que esse Direito global não deva ser adequado ao Direito Estatal – numa perfeita subsunção daquele neste. O movimento é inverso:

---

[275] VESTING, Thomas, **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade jurídica na modernidade**, p. 43.

[276] LÉVY, Pierre, **Cibercultura**, p. 125.

[277] Expressão utilizada por Pierre Lévy para ilustrar a "comunidade atual" (expressão mais apropriada que aquela dita "comunidade virtual") desenvolvida no ciberespaço, onde a aprendizagem cooperativa é feita por meio da soma dos conhecimentos angariados no campus da rede. LÉVY, Pierre, **Cibercultura**, p. 135.

[278] CAMPOS, Ricardo, **Metamorfose do Direito Global – Sobre a interação entre Direito, tempo e tecnologia**, p. 74.

é o Direito global, como universal, que deve escorar a constituição do Direito Estatal. Podemos afirmar que isso só será possível a partir da consideração do poder instituinte como anterior e necessário ao tão defendido e sedimentado Poder Constituinte. Aqui surge a ideia de um Direito global não sem o Estado, mas além dele. Como algo precedente a ele. Sendo o Direito virtualização, o poder instituinte estampado no sócio-histórico é o responsável por limitar esse futuro de possibilidades, pois ao mesmo tempo que cria também sucede. É sincrónico e diacrónico.

Os sistemas de sentidos, com isso, nunca se encontram restritos em um estado ontológico. Há que considerar também o momento fenomenológico. Um exemplo disso é a economia que tem a escassez como um elemento regulatório, de tal sorte que ela funciona da mesma forma como uma vinculação no tempo, no espaço, na essência e no *eidos*. Diariamente, em nossas vidas, os preços não estão fixados em lugar nenhum (espaço). Os preços do futuro não estão inscritos em nenhum documento (tempo). As decisões diárias são tomadas por conta dessa projeção para o futuro como um horizonte possível de precificação (essência e *eidos*). Temos a escassez controlada pelo mecanismo monetário. É o presente limitando o futuro de possibilidade a partir da interrelação entre a *psique instituinte* e sociedade instituída. É a estabilização provocando novas transformações (ou criações), que sofrem, por sua vez, novas limitações pelo social-histórico.

Shoshana Zuboff, na sua teoria sobre o "capitalismo de vigilância", parte de uma leitura parecida com a acima delimitada da anomalia do Direito, porém, propugna que o ambiente tecnológico tendencia levar ao fim do Direito, uma vez que a ideia de contrato partilhada nesse ambiente seria uma utopia a que a autora designa por "não-contratos" e cuja finalidade é a de simplesmente desfazer aquela ideia pré-digital do contrato como uma "ilha de previsibilidade"[279]. Isso sem falar no destino predestinado do fim da democracia a partir desse abrupto corte na liberdade, por meio da apropriação dos chamados *excedentes comportamentais* que seriam a matéria-prima utilizada na angariação da previsibilidade comportamental.

Um exemplo bem escolhido pela citada autora na obra *A era do Capitalismo da vigilância* remete aos casos de incumprimento contratual (atraso de uma parcela mensal) por parte de um consumidor que adquiriu um automóvel com sistema de monitoração. O credor pode instruí-lo para não permitir que o motor arranque. Mais ainda, pode, por meio desse sistema, conseguir assinalar a própria localização da viatura para uma possível e futura apreensão. Essa seria a "nova forma de contrato". Para Zuboff, esses não-contratos abandonam as promessas de previsibilidade e as promessas "legalmente vinculativas", de modo a substituí-las por cálculos determinados pelos processos automáticos, os quais eliminam a antiga institucionalização dos contratos e, desta maneira, propriamente do Direito[280]. Conclui disso que serão os algoritmos, por meio de uma capacidade de inteligência

[279] ZUBOFF, Shoshana, **A Era do Capitalismo da Vigilância – A disputa por Um Futuro Humano na Nova Fronteira do Poder**, p. 369.

[280] ZUBOFF, Shoshana, **A Era do Capitalismo da Vigilância – A disputa por Um Futuro Humano na Nova Fronteira do Poder**, p. 48.

automática, que mediarão como alcançar os objetivos económicos da sociedade atual e, para isso, utilizar-se-ão do *excedente comportamental*. Isso é vislumbrado nos casos dos seguros de veículos: o valor deles poderá ser balizado nesses dados excedentes, de modo que eles determinarão a sua majoração ou não. Tudo vai depender das informações colhidas a partir daqueles dados excedentes do usuário no ano anterior, por exemplo. A autonomia seria, então, deslocada para o limbo junto com o Direito.

Por outro lado, diante dessa realidade, surgem outros focos do discurso intelectual que aponta não para o desaparecimento do Direito, mas para a mudança de poder, que seria concentrado nessas supercorporações tecnológicas localizadas num pluralismo jurídico[281].

O certo é que nem um nem outro argumento oferece um balanço moderado sobre o processo de virtualização e atualização da globalização, bem como do Direito. A fórmula seja talvez apelar para o foco nas metamorfoses ocorridas, isto é, nas mudanças. Pois por meio delas é que se tem base suficiente para determinar o que é universal (virtual) e a partir daí desnudar a atualização concretizada na cultura da *sociedade instituinte*.

Aqui, o conceito híbrido de Direito ganha força. Parte de uma perspectiva interna (*sociedade instituinte*) como motor para a corporificação daquilo que será constituído como Direito regulado (externo – *sociedade instituída)*.

A sociedade não deve ser pensada como uma justaposição entre ela e o Estado. Mas, numa coevolução, onde os processos sociais influenciam-se mutuamente numa sincronia e diacronia. Assim, migra-se do domínio político para o relacional. O Direito é fruto desse relacional interno (*psique*) e externo (sujeito socializado). Por isso, defendemos que o Direito possui uma vertente fenomenológica e ontológica.

A hibridização do Direito atua num mundo no qual a realidade é a digital e as plataformas estão se tornando em infraestruturas de todas as esferas da vida: relações íntimas (Tinder), interações sociais (redes sociais), interações familiares e grupos de trabalho (grupos de WhatsApp), serviço notarial (e-notarial) e etc.[282]. Todas elas elaboram e conectam dados pessoais de consumidores, empresas, instituições públicas, de modo a manufaturar novas representações digitais da sociedade baseadas na hierarquia e heterarquia. Ao mesmo tempo que verticalizam as relações, também horizontalizam numa simbiose: tudo, dentro e fora da mente, é um objeto que pode ter ou não qualidades. Qualidades estas que dependerão da relação com o sujeito a partir da percepção do mundo como social-histórico.

---

[281] TEUBNER, Günter, A Bukowina Global sobre a Emergência de um Pluralismo Jurídico Transnacional. In **Impulso**. Piracicaba, 2003. [consult. 9 nov. 2024], p. 9-31. Disponível na internet: <file:///C:/Users/Gilson/Downloads/Teubner2003_PluralismoJrco.pdf>.

[282] CAMPOS, Ricardo, **Metamorfose do Direito Global – Sobre a interação entre Direito, tempo e tecnologia**, p. 288.

Considerações finais

A metamorfose do Direito é considerada como uma metamorfose da própria sociedade. O Direito moderno não se alimenta de instâncias superiores (hierarquia). Logo, não está à jusante em relação à sociedade. Mas está em um processo de coevolução com ela. Apesar de ser considerado uma virtualização, ou seja, estar em um eterno movimento de relação com o espaço, tempo, essência e *eidos*, visa a problematização e não a estabilização, que é uma preocupação da atualização do Direito positivo

A sociedade é formada a partir da cojuminação da *psique* com a instanciação. De modo que aquela não está reduzida a esta. Ela transborda, mas, ao mesmo tempo, é limitada pelo social-histórico. É dessa tensão entre o *instituído* e o *instituinte* que surge o Direito como um produto de um processo híbrido. Desse processo, nascem novas formas de resolução de litígios que consigam abarcar e mitigar as contradições criadas no seio das instituições, garantindo uma proteção além do Estado. Há aqui uma clara tensão entre o "rule of code" e o "rule of law". O Direito está além das instituições. Não é voltado para estabilizações, mas para as problematizações. Isso é um ponto importante da pesquisa porque, sendo assim, ele (Direito), a partir do processo de virtualização, autoriza a sua constante transformação e elimina, por sua vez, todas aquelas anomalias criadas pelos sistemas baseados unicamente no Poder Constituinte. É importante olhar para o poder instituinte como um grande mecanismo de atualização do Direito híbrido.

5. Referências Bibliográficas

CAMPOS, Ricardo. **Metamorfose do Direito Global – Sobre a interação entre Direito, tempo e tecnologia**. Rio de Janeiro: Contracorrente, 2022.

CASTORIADIS, Cornelius. **A instituição imaginária da sociedade**, 3.ª ed. São Paulo: Paz e Terra, 1995.

DELEUZE, Gilles. Walt Whitman. In **Essays critical and clinical**. Pennsylvania: University of Minnesota, 1997.

HARMAN, Graham. **O objeto Quádruplo – uma metafisica das coisas depois de Heidegger**, trad. Thiago Pinho. Rio de Janeiro: Eduerj, 2023.

HERCULANO-HOZEL, Suzana, **A vantagem Humana – Como nosso cérebro se tornou superpoderoso**, trad. Laura Teixeira Motta. São Paulo: Companhia das Letras, 2021.

LÉVY, Pierre. **Cibercultura**. Lisboa: Instituto Piaget, 1997.

LÉVY. Pierre. **O que é virtual?**, trad. Paulo Neves. São Paulo: Editora 34, 2017.

LUHMANN, Niklas. **La moral de la sociedad**, trad. Iván Rodrígues Ortega. Madrid: Trotta editora, 2013.

MEIRA, Fábio Bittencourt. Castoriadis (o instituinte) e a instituição. In **EnANPAD**. Rio de Janeiro, 2010, p. 14. Disponível na internet:<https://arquivo.anpad.org.br/diversos/down_zips/53/eor1869.pdf>.

MUNFORD, Lewis. **As Tansformações do Homem**, trad. Fernanda Barão e Isabel Fernandes. Lisboa: Antígona, 2021.

RAMOS, Edith. Um exame da tipologia do caráter social de Riesman. In **Arquivo brasileiro de Psicologia aplicada**. Rio de Janeiro, 1975.

SERRES, Michel. **Atlas**, trad. Alicia Martorell. Madrid: Cátedra, 1995.

TEUBNER, Günter. A Bukowina Global sobre a Emergência de um Pluralismo Jurídico Transnacional. In **Impulso**. Piracicaba, 2003. Disponível na internet: <file:///C:/Users/Gilson/Downloads/Teubner2003_PluralismoJrco.pdf>.

VESTING, Thomas. **Gentleman, Gestor, Homo Digitalis – A transformação da subjetividade jurídica na modernidade**, trad. Ricardo Campos e Gercélia Mendes. São Paulo: Contraconcorrente, 2022.

VIEIRA, Ariza Fabiana Vieira; MARTINS, Lilian Al-Chueyr Pereira. A scala naturae de Aristóteles no tratado De Generatione Animalium. In **Filosofia e História da Biologia**, vol. 5, n. 1. São Paulo: Universidade de São Paulo, 2010.

ZUBOFF, Shoshana. **A Era do Capitalismo da Vigilância – A disputa por Um Futuro Humano na Nova Fronteira do Poder**. Lisboa: Relógio D'Água, 2019.

WEBER, Max. **Economia e sociedade: Fundamentos da sociologia compreensiva**, vol. I. Brasília: Ed. UnB, 2000.

Eficácia Diagonal da Proteção de Dados Pessoais

Oscar Valente Cardoso [283]

Resumo

O artigo aborda a eficácia diagonal dos direitos fundamentais, com foco específico na proteção de dados pessoais em contextos marcados por desigualdades entre as partes. Por meio de uma pesquisa teórica e análise crítica, o estudo examina como normas legais e as decisões judiciais reconhecem e corrigem essas assimetrias, a fim

[283] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

de promover a proteção dos mais vulneráveis nas relações privadas de tratamento de dados pessoais. O objetivo principal é o de demonstrar que a aplicação da eficácia diagonal é indispensável para assegurar o equilíbrio nas relações assimétricas, especialmente em cenários como consumo, trabalho e tratamento de dados pessoais. A metodologia baseia-se em uma abordagem teórica, focada na análise de conceitos jurídicos e na interpretação de normas jurídicas sobre a eficácia diagonal dos direitos fundamentais. Os resultados indicam que a eficácia horizontal dos direitos fundamentais é insuficiente para abordar os desafios impostos pelas desigualdades informacionais e estruturais existentes nas relações entre agentes e titulares de dados pessoais, o que demanda a aplicação de mecanismos jurídicos que priorizem a transparência, o consentimento válido e a responsabilidade dos agentes. Conclui-se que a eficácia diagonal é necessária para garantir a dignidade da pessoa humana, a liberdade e a autonomia informacional dos titulares, com a promoção de uma proteção adequada dos dados nos meios físico e digital.

Palavras-chave: Eficácia diagonal, direitos fundamentais, proteção de dados pessoais, vulnerabilidade informacional, assimetria de poder.

Abstract

The article examines the diagonal effectiveness of fundamental rights, focusing specifically on the protection of personal data in contexts marked by power imbalances between parties. Through theoretical research and critical analysis, the study explores how legal norms and judicial decisions identify and address these asymmetries to protect the most vulnerable individuals in private data-processing relationships. The primary goal is to demonstrate that diagonal effectiveness plays an essential role in ensuring balance in asymmetric relationships, particularly in areas such as consumer transactions, labor relations, and personal data processing. The methodology relies on a theoretical approach, centered on the analysis of legal concepts and the interpretation of legal norms concerning the diagonal effectiveness of fundamental rights. The findings reveal that the horizontal effectiveness of fundamental rights falls short in addressing the challenges posed by informational and structural inequalities in relationships between data controllers and data subjects. This gap underscores the need for legal mechanisms that emphasize transparency, valid consent, and accountability. The article concludes that diagonal

effectiveness is crucial for safeguarding human dignity, freedom, and informational autonomy, while ensuring robust protection of personal data in both physical and digital environments.

Keywords: Diagonal effectiveness, fundamental rights, personal data protection, informational vulnerability, power asymmetry.

Introdução

A proteção de dados pessoais é um dos temas mais relevantes no cenário jurídico contemporâneo, especialmente diante das crescentes desigualdades informacionais existentes nas relações privadas. O avanço tecnológico e a ampliação do uso de dados pessoais em diversas esferas - como consumo, trabalho e serviços digitais - evidenciam a necessidade de mecanismos jurídicos que assegurem o respeito aos direitos fundamentais, entre os quais está a proteção de dados pessoais. A questão é particularmente complexa em relações marcadas por assimetrias de poder, nas quais os titulares de dados se encontram em posições de vulnerabilidade frente a agentes dotados de maior conhecimento, recursos e capacidade de processamento.

Nesse contexto, a eficácia diagonal dos direitos fundamentais é uma resposta jurídica a essas assimetrias, ao proporcionar uma proteção diferenciada ao titular vulnerável. Diferentemente da eficácia horizontal, que parte do pressuposto de igualdade entre particulares, a eficácia diagonal reconhece a necessidade de mecanismos que corrijam desequilíbrios e assegurem a efetividade dos direitos fundamentais em relações privadas assimétricas. Nesse contexto, normas legais como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (RGPD) na União Europeia, bem como as decisões

judiciais que interpretam e aplicam tais normas aos casos concretos, desempenham um papel relevante na operacionalização da eficácia diagonal.

A pesquisa desenvolvida no presente artigo é justificada pela necessidade de aprofundar a compreensão da eficácia diagonal como instrumento de proteção em cenários de desigualdade informacional, especialmente nas relações contratuais que embasam as atividades de tratamento de dados pessoais. A análise fundamenta-se em um problema central: como o ordenamento jurídico pode garantir a aplicação prática do direito fundamental à proteção de dados pessoais em relações privadas marcadas por assimetrias? Esse problema se torna ainda mais relevante diante da crescente digitalização das relações sociais e econômicas, que amplia as operações de tratamento de dados pessoais de maneira intensiva e, por vezes, abusiva.

O objetivo geral do artigo é demonstrar que a aplicação da eficácia diagonal é indispensável para corrigir desigualdades e promover o equilíbrio nas relações privadas que envolvem dados pessoais, a fim de garantir a dignidade, a liberdade e a autonomia informacional dos titulares. Para atingir esse objetivo, o artigo adota uma abordagem teórica e crítica, com a análise de conceitos jurídicos e de normas legais relacionadas à eficácia diagonal dos direitos fundamentais.

A estrutura do artigo está dividida em tópicos que refletem o desenvolvimento lógico da pesquisa. A primeira seção delimita as concepções das eficácias horizontal e vertical dos direitos fundamentais. O segundo item desenvolve os aspectos conceituais da eficácia diagonal dos direitos fundamentais. Na sequência, o terceiro tópico contextualiza a eficácia diagonal dos direitos fundamentais, diferenciando-a especialmente da eficácia horizontal. A quarta seção analisa de forma específica a eficácia diagonal da proteção de dados pessoais e, ao fim, o quinto item explica as razões pelas quais a eficácia horizontal não é suficiente para essa tutela.
Dessa forma, o presente estudo busca não apenas aprofundar a compreensão sobre a eficácia diagonal, mas também oferecer subsídios teóricos e práticos para assegurar a tutela adequada do direito fundamental à proteção de dados pessoais.

1. Eficácia Horizontal e Vertical dos Direitos Fundamentais

A eficácia dos direitos fundamentais no ordenamento jurídico pode ser analisada sob duas perspectivas distintas, mas complementares: a vertical e a horizontal.
Esses conceitos refletem a forma como os direitos fundamentais incidem nas relações jurídicas, sejam elas entre o indivíduo e o Estado, ou entre particulares. Entender essa distinção é importante para compreender a amplitude e o alcance da proteção conferida pelos direitos fundamentais[284].

[284] Sobre as duas eficácias: CANARIS, Claus-Wilhelm. **Direitos fundamentais e direito privado**. Coimbra: Almedina, 2009, p. 52-56.

A eficácia vertical é a forma mais tradicional (e originária) de observância dos direitos fundamentais, que incidem diretamente sobre as relações entre o indivíduo e o Estado. Nesse modelo, os direitos fundamentais são concebidos como limites ao exercício do poder estatal, a fim de proteger o cidadão contra abusos, arbitrariedades e interferências indevidas por parte das autoridades públicas, bem como assegurar o cumprimento de seus direitos, por meio de ações do Estado. Em sua essência, a eficácia vertical reflete o papel dos direitos fundamentais como garantias individuais em face do Estado, que detém o monopólio do poder coercitivo. Para esse fim, leva em consideração as desigualdades existentes entre o Poder Público e os particulares[285].

Historicamente, esse modelo foi consolidado com o Constitucionalismo clássico, que se baseava na concepção de que os direitos fundamentais deveriam restringir a atuação estatal para proteger a liberdade individual. Por exemplo, o direito à liberdade de expressão impede o Estado de censurar opiniões e o direito à propriedade limita a possibilidade de desapropriações arbitrárias sem a devida indenização.

A eficácia vertical é especialmente visível nos deveres impostos ao Estado para garantir condições mínimas de dignidade e igualdade aos cidadãos. Por exemplo, o direito à educação pública gratuita impõe ao Estado o dever de criar e manter instituições de ensino acessíveis a todos. Caso falhe nesse dever, os cidadãos podem invocar diretamente esse direito fundamental para exigir a sua concretização.

Em outro exemplo, Lucas, um cidadão brasileiro, descobre que seus dados pessoais foram expostos por uma entidade pública em uma página governamental na internet, sem o seu consentimento. Entre os dados divulgados estão seu número de CPF, endereço residencial e informações sobre benefícios recebidos de programas sociais. Ao perceber que a sua privacidade foi comprometida e os seus dados pessoais expostos, Lucas contrata um advogado para ingressar com uma demanda judicial contra a pessoa jurídica de direito público, com fundamento nos direitos fundamentais à privacidade e à proteção de dados pessoais, garantidos pela Constituição e regulados no Código Civil e na Lei Geral de Proteção de Dados Pessoais.

Nesse caso, a relação jurídica entre Lucas e o ente público caracteriza-se como uma situação de eficácia vertical dos direitos fundamentais. A divulgação indevida de seus dados por uma entidade estatal representa uma violação direta do direito à privacidade (artigo 26º da Constituição portuguesa e art. 5º, X, da Constituição brasileira) e do direito à proteção de dados pessoais (artigo 35º da Constituição portuguesa e art. 5º, LXXIX, da Constituição brasileira). Lucas, como indivíduo, está em posição de desigualdade em relação ao Estado, que possui o controle de seus dados e recursos tecnológicos superiores aos dele.

É possível constatar ainda no caso o papel do Estado como garantidor dos direitos fundamentais, ao exigir que ele não apenas respeite, mas também proteja

[285] Acerca do conceito e extensão da eficácia vertical: DIMOULIS, Dimitri; MARTINS, Leonardo. **Teoria geral dos direitos fundamentais**. 5. ed. São Paulo: Atlas, 2014, p. 102-103.

ativamente os direitos dos indivíduos. Nesse sentido, a eficácia vertical dos direitos fundamentais assegura que as práticas governamentais estejam alinhadas às normas constitucionais, especialmente no contexto da transformação digital e da proteção de dados pessoais.

A eficácia horizontal, por sua vez, refere-se à aplicação dos direitos fundamentais nas relações entre particulares. Por essa razão, também é denominada de "eficácia privada" ou ainda, na doutrina alemã, de "efeitos perante terceiros" (Drittwirkung), para se referir à extensão da eficácia dos direitos fundamentais para outras pessoas além do Estado, que se divide em Mittelbare Drittwirkung (incidência dos princípios e valores extraídos dos direitos fundamentais para a resolução de conflitos entre particulares) e em Unmittelbare Drittwirkung (incidência direta das normas de direitos fundamentais para a resolução de conflitos entre particulares). Esse modelo reconhece que os direitos fundamentais não devem se limitar às relações com o Estado, mas também devem orientar as relações privadas, garantindo que princípios como dignidade, igualdade e liberdade sejam respeitados em todas as esferas da convivência humana[286].

A evolução do entendimento sobre a eficácia horizontal foi impulsionada pelo reconhecimento de que as violações de direitos fundamentais também podem ocorrer em contextos privados.

Por exemplo, João reside em um condomínio no Brasil que decidiu implementar um sistema de controle de acesso com o uso de dados biométricos, como a impressão digital e o reconhecimento facial, para aumentar a segurança. O síndico informa que todos os moradores devem obrigatoriamente fornecer seus dados biométricos para o cadastro no sistema, sem esclarecer como esses dados serão armazenados, protegidos ou eventualmente descartados (por exemplo, quando um morador se mudar em definitivo para outro local). Preocupado com a possibilidade de mau uso ou vazamento de seus dados, João questiona a medida, mas é informado de que sua recusa o impediria de acessar as áreas comuns do condomínio.

Por isso, João decide buscar auxílio jurídico, com a alegação de que seu direito fundamental à proteção de dados pessoais, assegurado pela Constituição e pela LGPD, está sendo violado. Ele argumenta que o condomínio, como entidade privada, não pode obrigá-lo a fornecer dados biométricos sem garantir transparência sobre seu uso, tampouco demonstrar a implantação medidas de segurança adequadas, e sem permitir uma forma diferenciada de acesso que não exija a coleta de dados pessoais sensíveis.

---

[286] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018, p. 393-402. Também sobre o assunto: CANOTILHO, J. J. Gomes. **Direito constitucional e teoria da Constituição**. 7. ed. Coimbra: Almedina, 2003, p. 1286-1290. Ainda: DIMOULIS, Dimitri; MARTINS, Leonardo. **Teoria geral dos direitos fundamentais**. 5. ed. São Paulo: Atlas, 2014, p. 103-110.

Nesse caso, pretende-se a eficácia horizontal, pois um direito fundamental de João está sendo aplicado em uma relação entre particulares: o morador e o condomínio. O tribunal pode determinar que o condomínio ofereça alternativas ao uso de dados biométricos, como o uso de cartões de acesso, além de exigir que as operações de tratamento de dados estejam em conformidade com as normas da LGPD.

Embora a eficácia vertical e horizontal sejam distintas, na prática elas frequentemente se entrelaçam.

Por exemplo, a violação de direitos fundamentais por uma empresa privada pode demandar a intervenção do Estado, por meio do Judiciário, para restaurar o equilíbrio das relações. Da mesma forma, o Estado tem o dever de regular as relações privadas de maneira a evitar violações sistemáticas de direitos fundamentais.

As interseções entre esses dois modelos são particularmente evidentes em contextos de regulação econômica e social. Por exemplo, o Estado é responsável por legislar para proteger os consumidores contra práticas abusivas de empresas, a fim de assegurar que os direitos fundamentais sejam respeitados nas relações de consumo. Nesse sentido, a eficácia horizontal dos direitos fundamentais muitas vezes depende de uma atuação ativa do Estado, o que reforça sua dimensão vertical.

2. Eficácia Diagonal dos Direitos Fundamentais: Aspectos Conceituais

Além da eficácia vertical e horizontal, o conceito de eficácia diagonal dos direitos fundamentais surge para abordar um contexto específico: as relações entre particulares que apresentam uma assimetria de poder significativa, como aquelas que envolvem empregadores e empregados, ou fornecedores e consumidores.

Essa concepção amplia a discussão sobre a aplicação dos direitos fundamentais, ao reconhecer que as diferenças estruturais de poder podem gerar situações de vulnerabilidade, que exigem uma abordagem diferenciada.

A eficácia diagonal dos direitos fundamentais se aplica às relações jurídicas entre particulares, quando existir um desequilíbrio entre as partes, que coloque uma delas em posição de desvantagem em relação à outra. Esse modelo reconhece que, nesses casos, a simples aplicação da eficácia horizontal (que presume um nível de igualdade entre as partes) pode ser insuficiente para assegurar a proteção efetiva dos direitos fundamentais[287].

[287] Sobre o assunto: "Dessa forma, a eficácia diagonal é a união dos conceitos de eficácia vertical (relação cidadão/Estado – relação de poder) e eficácia horizontal (relação particular/particular – relação paritária) na aplicação dos direitos fundamentais à relação entre particulares na qual se observa disparidade de poder entre eles" (ALVARENGA, Rúbia Zanotelli de; CUNHA, Cristie Helena; AMARAL, Jéssica Maria Sousa Gurgel de. A eficácia diagonal dos direitos fundamentais como uma limitação ao poder empregatício: uma análise

O termo "diagonal" simboliza a relação assimétrica, na qual uma parte exerce maior poder econômico, social ou político, e a outra depende desse poder, o que cria uma situação de vulnerabilidade. Esse tipo de eficácia visa garantir que os direitos fundamentais sejam aplicados como instrumentos de equilíbrio, a fim de proteger os mais vulneráveis nas relações privadas.

Um exemplo clássico está na discriminação no ambiente de trabalho, em que empregadores podem violar o direito à igualdade ao adotar práticas discriminatórias com base em gênero, raça ou orientação sexual (entre outros critérios). Nessa situação, os direitos fundamentais têm diagonal horizontal, pois incidem diretamente sobre a relação contratual entre empregador e empregado, caracterizada pelo desequilíbrio.

Outro exemplo está na relação entre consumidores e fornecedores de produtos ou serviços. Se uma operadora de telefonia inserir cláusulas abusivas em seus contratos, a eficácia diagonal permite que o direito fundamental à proteção do consumidor, previsto no art. 5º, XXXII, da Constituição brasileira seja aplicado, para corrigir o desequilíbrio e assegurar a justiça contratual.

Ana, uma usuária de uma plataforma de comércio eletrônico, descobre que a empresa compartilhou seus dados pessoais com terceiros sem o seu consentimento e sem indicar outra base legal válida, o que resultou no envio de propagandas invasivas e ligações indesejadas para a consumidora. Além disso, Ana percebeu que os termos e condições de uso da plataforma não são claros sobre como os dados dos usuários são tratados (e se poderiam ser compartilhados). Sentindo-se lesada, ela decidiu processar a empresa, com a alegação de que a prática violou o seu direito fundamental à proteção de dados pessoais.

Aqui, o conflito ocorre em uma relação entre particulares: Ana, enquanto consumidora, e a plataforma digital, enquanto fornecedora de serviços. Contudo, o desequilíbrio entre as partes caracteriza a eficácia diagonal dos direitos fundamentais, o que permite à consumidora invocar diretamente a Constituição e a LGPD, para exigir que a empresa respeite os seus direitos. O tribunal pode determinar que a plataforma cesse o compartilhamento não autorizado de dados, implemente políticas de transparência sobre o tratamento de dados e indenize Ana pelos danos causados.

3. Distinções entre Eficácia Horizontal e Diagonal

A eficácia horizontal e a eficácia diagonal dos direitos fundamentais se distinguem, em essência, pelo tipo de relação jurídica que regulam e pelo reconhecimento (ou não) de desigualdades estruturais entre as partes envolvidas. Essas diferenças revelam nuances importantes sobre como os direitos fundamentais permeiam as

da aplicação do princípio da não discriminação na fase pré-contratual das relações de emprego. **Revista de Direito do Trabalho**, São Paulo, nº 211, p. 253-268, maio/jun.2020). Ainda: CONTRERAS, Sérgio Gamonal. **Cidadania na empresa e eficácia diagonal dos direitos fundamentais**. São Paulo: LTr, 2011, p. 33-34.

relações privadas, ampliando a sua aplicação para além do contexto público-estatal.

A eficácia horizontal dos direitos fundamentais regula as relações entre particulares em posição de igualdade jurídica inicial. Nesse contexto, os direitos fundamentais são aplicados diretamente para equilibrar conflitos e proteger interesses legítimos, mas sem presumir ou considerar desigualdades entre as partes. Trata-se de uma aplicação genérica e uniforme, que reconhece os direitos de todos os envolvidos, mas sem necessariamente adotar medidas específicas para proteger uma parte em situação de vulnerabilidade ou de inferioridade.

Essa eficácia se manifesta com frequência em relações contratuais, nas quais os direitos fundamentais podem ser invocados para equilibrar interesses, desde que não haja uma disparidade inicial entre as partes. Desse modo, o objetivo é criar um espaço de convivência harmônica e respeitosa, para proteger valores essenciais, sem considerar vulnerabilidades adicionais.

Por sua vez, a eficácia diagonal reconhece explicitamente a existência de uma desigualdade estrutural ou de poder entre as partes envolvidas na relação jurídica. Diferentemente da eficácia horizontal, que parte do pressuposto de igualdade formal, a eficácia diagonal busca corrigir os desequilíbrios que podem comprometer os direitos fundamentais de uma parte, especialmente quando esta estiver em situação de vulnerabilidade ou dependência (desigualdade material).

Essa eficácia é comum em relações de trabalho e de consumo (entre outras), nas quais uma das partes (empregador e fornecedor) tem maior poder econômico, social ou institucional em relação à outra (empregado e consumidor). No contexto trabalhista, por exemplo, a relação entre empregador e empregado é marcada por uma disparidade natural de poder, pois o empregador detém os meios de trabalho e de subsistência do trabalhador. Nessas circunstâncias, a aplicação dos direitos fundamentais exige uma proteção diferenciada para a parte mais frágil, como no caso de assédio moral ou discriminação.

A eficácia diagonal busca garantir que os direitos fundamentais sejam não apenas reconhecidos formalmente, mas também efetivados de maneira prática de acordo com a situação material, isto é, considerando o contexto da relação e as circunstâncias de vulnerabilidade de uma das partes. Isso significa que as normas constitucionais devem ser interpretadas e aplicadas de forma a proteger o lado mais fraco e a reduzir as desigualdades materiais inerentes à relação.

De forma comparativa, três características diferenciam cada uma destas duas eficácias das normas de direitos fundamentais:

(a) Igualdade: na eficácia horizontal há uma igualdade material inicial, ou seja, as partes são presumidas iguais em termos de poder e capacidade de negociação. Já na eficácia diagonal, existe o reconhecimento explícito de que uma das partes se encontra em situação de desvantagem, em virtude da desigualdade material existente entre elas, o que exige maior proteção;

(b) Relações jurídicas: a eficácia horizontal regula relações privadas gerais, como disputas entre vizinhos ou entre parceiros comerciais. Já a eficácia diagonal é

aplicada a relações privadas assimétricas, como aquelas entre empregadores e empregados, ou fornecedores e consumidores;
(c) Objetivo: a eficácia horizontal busca garantir a igualdade formal na aplicação dos direitos fundamentais. Já a eficácia diagonal tem como foco corrigir desequilíbrios estruturais e promover a igualdade material, a fim de proteger as partes mais vulneráveis.

Em síntese, enquanto a eficácia horizontal pressupõe uma igualdade inicial entre as partes e regula as relações privadas de maneira geral, a eficácia diagonal reconhece explicitamente a existência de uma desigualdade entre os envolvidos. O foco principal da eficácia diagonal é o de proteger os mais vulneráveis e corrigir os desequilíbrios de poder que podem comprometer os direitos fundamentais.

Por exemplo, em um conflito horizontal, como uma disputa entre vizinhos sobre barulho excessivo, os direitos fundamentais (como o direito à privacidade e à inviolabilidade do domicílio) são aplicados de forma direta, sem considerar desigualdades econômicas ou sociais. O foco da eficácia horizontal, nesse caso, é assegurar que ambos os lados sejam tratados de maneira igualitária, com base nos direitos previstos na Constituição ou em normas legais específicas.

Já em um contexto diagonal, como um caso de assédio moral no trabalho, a aplicação dos direitos fundamentais leva em conta a posição de dependência do empregado em relação ao empregador, o que exige uma proteção adicional.

Embora diferentes, as eficácias horizontal e diagonal não são excludentes. Ao contrário, elas se complementam para ampliar o alcance e a proteção dos direitos fundamentais.

A eficácia horizontal atua como uma base geral, para garantir que os direitos fundamentais sejam aplicáveis às relações privadas de forma uniforme. Por sua vez, a eficácia diagonal atua como uma camada adicional de proteção, a fim de adaptar a aplicação dos direitos fundamentais para lidar com desigualdades materiais.

Essa complementaridade é fundamental para assegurar que os direitos fundamentais cumpram sua função de promover a dignidade da pessoa humana, proteger as liberdades e observar a igualdade (formal e material) em todas as esferas sociais, seja no plano individual, seja no contexto coletivo.

Ao reconhecer tanto a igualdade quanto as vulnerabilidades, o sistema jurídico amplia a capacidade dos direitos fundamentais de transformar realidades e de atingir a sua eficácia.

4. A Eficácia Diagonal da Proteção de Dados Pessoais

A eficácia diagonal dos direitos fundamentais encontra sua expressão prática na existência de normas legais e decisões judiciais que os reconhecem e atuam para corrigir desigualdades em relações privadas.

Esses meios têm o objetivo de operacionalizar a proteção dos mais vulneráveis, com a promoção do equilíbrio em contextos em que uma das partes detém maior poder econômico, social ou institucional.

Por meio dessas normas e interpretações, busca-se garantir que os direitos fundamentais existam não apenas formalmente, mas também sejam efetivamente aplicados para proteger a dignidade e os direitos daqueles que se encontram em situações de desvantagem.

Para esse fim, as normas legais estabelecem regras específicas de proteção para indivíduos em relações jurídicas assimétricas.

Nesse contexto está a proteção de dados pessoais, que se destaca como uma das ocorrências mais significativas da eficácia diagonal dos direitos fundamentais na atualidade. Em um mundo cada vez mais digitalizado, as relações privadas frequentemente envolvem desequilíbrios acentuados entre aqueles que tratam os dados (controladores ou operadores na LGPD e responsáveis pelo tratamento e subcontratantes no RGPD) e os titulares desses dados.

Esses desequilíbrios decorrem, principalmente, do poder econômico e tecnológico detido por grandes corporações, plataformas digitais e instituições financeiras, em contraste com a posição de vulnerabilidade informacional das pessoas.

A proteção de dados pessoais, na eficácia diagonal, visa justamente corrigir essa disparidade, ao garantir que o titular mantenha controle e autonomia sobre os seus dados pessoais, mesmo em relações marcadas por assimetria de poder. Essa correção do desequilíbrio é realizada por meio de normas legais específicas e de interpretações que reconhecem o impacto desproporcional que o tratamento inadequado ou irregular dos dados pode ter sobre os indivíduos, especialmente em contextos como consumo, trabalho e acesso a serviços essenciais.

A eficácia diagonal na proteção de dados pessoais parte do reconhecimento de que o titular está em uma posição de vulnerabilidade diante dos agentes que tratam os seus dados. Essa vulnerabilidade é multifacetada, pois abrange aspectos como o *desconhecimento técnico* sobre as operações de tratamento de dados, a *falta de transparência* por parte dos agentes de tratamento e a *desigualdade de poder* na relação contratual entre agente e titular (via de regra, definida por meio de termos e condições de uso com cláusulas excessivas, ininteligíveis e não lidas previamente pelo titular, que se limita a aderir à relação com um clique na tela de seu dispositivo eletrônico).

Por exemplo, ao consentir com o tratamento de seus dados ao realizar o cadastro em um aplicativo digital, o titular frequentemente não compreende plenamente as implicações de suas escolhas, o que o deixa em uma posição de *vulnerabilidade informacional*. Essa situação exige uma proteção legal diferenciada, que assegure a transparência e evite abusos, a fim de corrigir os desequilíbrios inerentes à relação.

A desigualdade de poder existente na relação contratual entre agente e titular é um dos elementos centrais que justificam a tutela diferenciada

proporcionada pela eficácia diagonal dos direitos fundamentais na proteção de dados pessoais. Essa assimetria decorre não apenas da disparidade econômica e tecnológica entre as partes, mas também de um desequilíbrio informacional, no qual o agente controlador ou responsável pelo tratamento dos dados detém maior conhecimento, domínio e capacidade de utilização dos dados (e das informações extraídas dele) em benefício próprio, enquanto o titular frequentemente é colocado em uma posição de passividade.

Em muitos casos, a relação contratual é definida por meio de contratos de adesão (especialmente nas relações de consumo), nos quais o titular dos dados não tem espaço para negociar as cláusulas ou os termos do tratamento de seus dados. Esses contratos, usualmente apresentados em formatos digitais, possuem cláusulas padronizadas, extensas e redigidas em linguagem técnica, o que dificulta ou impossibilita sua compreensão integral pelo titular. Como consequência disso, o consentimento dado para o tratamento de dados é frequentemente viciado pela falta ou insuficiência de informações, já que o titular aceita os termos sem entender completamente o alcance das permissões que concede ao contratado.

Esse cenário cria a vulnerabilidade informacional, na qual o titular não tem condições de avaliar, de maneira efetiva, os riscos e as implicações do tratamento de seus dados pessoais. Essa vulnerabilidade se manifesta de diferentes formas, especialmente no desconhecimento técnico (o titular não compreende os processos tecnológicos envolvidos no tratamento de dados, como os algoritmos de perfilamento), a falta de transparência (os agentes de tratamento não fornecem informações claras e acessíveis sobre como os dados serão tratados e com quem serão compartilhados, deixando o titular sem capacidade de questionar ou intervir) e a assimetria na decisão (a relação contratual é estruturalmente desequilibrada, com o titular sendo compelido a aceitar os termos impostos para acessar serviços essenciais, como aplicativos de mobilidade, plataformas de comunicação ou de serviços financeiros).

Essa combinação de fatores coloca o titular em uma posição de dependência e subordinação em relação ao agente de tratamento, na qual ele não apenas cede seus dados, mas também abdica, frequentemente de forma inconsciente, de parte de sua autonomia informacional. Essa autonomia, essencial para a dignidade humana e para a liberdade individual, é comprometida quando o titular não tem controle sobre como seus dados serão tratados.

Além disso, a vulnerabilidade informacional é agravada pelo uso cada vez mais sofisticado de tecnologias de *Big Data* e inteligência artificial, que permitem que os agentes de tratamento utilizem os dados para criar perfis detalhados e prever comportamentos futuros dos titulares. Essas práticas, embora possam ser legais, ampliam a desigualdade de poder, pois o titular não possui as ferramentas ou o conhecimento necessário para monitorar ou limitar o uso de seus dados e informações.

A eficácia diagonal na proteção de dados pessoais busca corrigir esse desequilíbrio, ao estabelecer regras específicas de transparência, consentimento e responsabilidade civil. Por exemplo, a exigência de que os controladores ou responsáveis pelo tratamento forneçam políticas de privacidade claras e compreensíveis é uma medida essencial para reduzir a vulnerabilidade informacional.

Nesse contexto, as normas previstas em leis como o Regulamento Geral de Proteção de Dados (RGPD), na União Europeia, e a Lei Geral de Proteção de Dados Pessoais (LGPD), no Brasil, operam como instrumentos de eficácia diagonal, ao estabelecer deveres para os agentes de tratamento de dados que visam proteger os direitos dos titulares e buscar o equilíbrio na relação existente entre eles.

Esses dispositivos regulatórios não apenas reconhecem a assimetria existente entre agentes e titulares, mas também impõem medidas para corrigi-la, como os direitos à portabilidade dos dados, à revogação do consentimento e à informação clara e acessível, os quais permitem ao titular retomar parte do controle sobre seus dados, a fim de equilibrar a relação contratual.

Contudo, a proteção efetiva exige mais do que a existência de normas legais; é necessário que essas normas sejam interpretadas e aplicadas de uma forma que reconheça as desigualdades existentes nessa relação. Nesse sentido, decisões judiciais que invalidam cláusulas abusivas em contratos de adesão ou que fixam indenizações por vazamentos de dados pessoais são exemplos práticos de como a eficácia diagonal pode atuar para proteger o titular e reforçar a sua autonomia informacional.

As decisões judiciais desempenham um papel relevante na concretização da eficácia diagonal dos direitos fundamentais, ao aplicar as normas legais em situações concretas, a fim de adaptá-las às desigualdades específicas presentes em cada caso. Essa função interpretativa permite que o Judiciário vá além da aplicação literal das normas, para reconhecer os desequilíbrios de poder e adotar medidas que garantam a proteção efetiva da parte vulnerável.

Por exemplo, ao declarar nula uma cláusula abusiva que exonera a empresa de eventual responsabilidade civil por vazamentos de dados pessoais, os tribunais protegem não apenas os titulares diretamente afetados, mas também estabelecem precedentes para futuras relações contratuais. Essa atuação não apenas resolve o caso, mas desestimula práticas desleais e incentiva agentes de tratamento a adotar medidas mais robustas de segurança e transparência, o que contribui para o fortalecimento das normas de proteção de dados pessoais no âmbito privado.

5. A Insuficiência da Eficácia Horizontal da Proteção de Dados Pessoais

Embora a eficácia horizontal dos direitos fundamentais seja relevante na regulação das relações jurídicas entre particulares, é insuficiente para abordar adequadamente as complexidades e desigualdades inerentes ao tratamento de dados pessoais.

A eficácia horizontal parte do pressuposto de uma relação de igualdade inicial entre as partes, com a incidência dos direitos fundamentais de maneira uniforme, sem necessariamente considerar as disparidades de poder e vulnerabilidades que caracterizam muitas dessas relações. Por sua vez, o tratamento de dados pessoais frequentemente ocorre em contextos assimétricos, nos quais o titular dos dados está em uma posição de desvantagem diante do agente de tratamento.

Essa insuficiência decorre de duas razões principais. Primeiro, a *assimetria de poder* existente entre os titulares de dados e os agentes que os tratam não é plenamente abordada pela eficácia horizontal. Grandes corporações, plataformas digitais e instituições financeiras possuem acesso a recursos tecnológicos, informações e capacidades que superam em muito as dos indivíduos, o que criando uma desigualdade informacional, que a aplicação horizontal dos direitos fundamentais não consegue corrigir.

Em segundo lugar, a eficácia horizontal não é projetada para lidar com o *impacto sistêmico* que o tratamento inadequado de dados pode ter na sociedade. A violação dos direitos de um titular, como um vazamento de dados, pode gerar consequências amplas e coletivas (e, até mesmo, irreversíveis), que exigem uma abordagem mais específica e adequada.

Por exemplo, em uma relação contratual entre um consumidor e uma plataforma de comércio eletrônico, a aplicação da eficácia horizontal garantiria que ambas as partes fossem tratadas com base nos direitos fundamentais, como a proteção da privacidade. No entanto, ao ignorar a desigualdade de poder existente entre o consumidor e a empresa que comercializa produtos na plataforma, a eficácia horizontal pode não ser suficiente para proteger o consumidor contra práticas abusivas, como cláusulas contratuais que permitem o compartilhamento de dados ou que impõem o consentimento como um meio exclusivo de acesso a determinados serviços. Nesse contexto, a eficácia diagonal se torna necessária, para adotar medidas específicas que reconheçam a vulnerabilidade do consumidor titular dos dados e obriguem a plataforma a fornecer informações claras e obter o consentimento de forma válida (sem a imposição de técnicas de "tudo ou nada" para a coleta de dados).

Assim, a eficácia horizontal, por si só, é insuficiente para proteger adequadamente o direito fundamental à proteção de dados pessoais em situações que envolvem partes excessivamente desiguais. A proteção efetiva dos dados pessoais exige uma abordagem mais abrangente, que considere tanto as relações privadas assimétricas (eficácia diagonal) quanto as interações entre o indivíduo e o Poder Público (eficácia vertical), a fim de garantir que os direitos fundamentais sejam aplicados de forma adequada e eficaz.

Considerações finais

A eficácia diagonal dos direitos fundamentais é indispensável no enfrentamento das desigualdades que marcam as relações privadas em diversos contextos, especialmente no tratamento de dados pessoais.

Como visto, na proteção de dados pessoais é preciso ir além da eficácia horizontal dos direitos fundamentais e adotar uma abordagem diagonal. A eficácia diagonal reconhece e corrige as desigualdades, impõe deveres específicos aos agentes de tratamento, a fim de proteger os titulares vulneráveis. A eficácia vertical também pode desempenhar um papel importante nessa relação, especialmente quando o Estado atua como regulador ou como o próprio agente de tratamento de dados pessoais.

As decisões judiciais desempenham um papel relevante, ao interpretar e adaptar as normas às especificidades de cada caso, indo além da aplicação literal para reconhecer e corrigir os desequilíbrios existentes. O papel das normas legais, como o RGPD na União Europeia e a LGPD no Brasil, embasam essa atuação, ao estabelecer normas que buscam equilibrar as relações entre agentes e titulares.

Ademais, a proteção efetiva dos direitos fundamentais na esfera privada exige uma abordagem integrada que inclua a evolução contínua das normas e a atuação judicial. Assim será possível assegurar que os direitos fundamentais não apenas existam formalmente, mas também sejam efetivados de maneira prática, especialmente com a proteção adequada dos dados pessoais.

Referências

ALVARENGA, Rúbia Zanotelli de; CUNHA, Cristie Helena; AMARAL, Jéssica Maria Sousa Gurgel de. A eficácia diagonal dos direitos fundamentais como uma limitação ao poder empregatício: uma análise da aplicação do princípio da não discriminação na fase pré-contratual das relações de emprego. **Revista de Direito do Trabalho**, São Paulo, nº 211, p. 253-268, maio/jun.2020.

CANARIS, Claus-Wilhelm. **Direitos fundamentais e direito privado**. Coimbra: Almedina, 2009.

CANOTILHO, J. J. Gomes. **Direito constitucional e teoria da Constituição**. 7. ed. Coimbra: Almedina, 2003.

CONTRERAS, Sérgio Gamonal. **Cidadania na empresa e eficácia diagonal dos direitos fundamentais**. São Paulo: LTr, 2011.

DIMOULIS, Dimitri; MARTINS, Leonardo. **Teoria geral dos direitos fundamentais**. 5. ed. São Paulo: Atlas, 2014.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

II
LEGISLAÇÃO E JURISPRUDÊNCIA COMENTADA

Videovigilância em Contexto Laboral
Comentário ao Acórdão do TRE de 26 de setembro de 2024

Pedro Martins Proença
Manuel David Masseno

Resumo

Na Era Digital, os avanços tecnológicos têm revolucionado as dinâmicas de controlo e gestão no ambiente laboral, permitindo às organizações desenvolverem métodos sofisticados de supervisão e avaliação do desempenho dos respetivos trabalhadores. Apesar de contribuírem para a produtividade e segurança no local de trabalho, as novas tecnologias de vigilância trouxeram implicações éticas e legais significativas. Diante deste contexto, o presente artigo visa comentar, em termos sintéticos, o Acórdão (AC) proferido no âmbito do processo 1442/23.9T8STR.E1, a 26 de setembro de 2024, pelo Tribunal da Relação de Évora (TRE). Com efeito, o TRE pronunciou-se sobre questões relacionadas com a admissibilidade da captação de imagens de videovigilância como meio de prova, que fundamentaram a ação de despedimento de uma funcionária. O objetivo deste comentário consiste em trazer a debate um conjunto de temáticas envoltas à videovigilância na esfera laboral, que não tem permanecido consensual a nível de jurisprudência e tem gerado dificuldades na articulação com a Proteção de Dados e outras matérias do Direito.

Palavras-chave: Portugal, videovigilância, laboral, CNPD, RGPD, despedimento.

Abstract

In the Digital Age, technological advancements have revolutionized the dynamics of control and management within the workplace, enabling organizations to develop sophisticated methods for monitoring and evaluating employee performance. While these surveillance technologies enhance productivity and security in the workplace, they have also introduced significant ethical and legal implications. The present article aims to, briefly, discuss the ruling issued in Case 1442/23.9T8STR.E1, on 09/26/2024, by the Évora Court of Appeal. The Court addressed issues related to the admissibility of capturing video surveillance images as evidence, which supported the dismissal of an employee. The objective of this commentary is to bring to the table a range of topics surrounding workplace video surveillance, an area that remains contentious in jurisprudence and has posed challenges in alignment with Data Protection and other legal issues.

***Keywords*:** Portugal, CNPD, GDPR, *video surveillance, labour, dismissal.*

Introdução

A videovigilância, também designada por *Closed-circuit Television* (CCTV), consiste na instalação de um sistema de recolha de imagens por meio eletrónico, seja ele analógico, digital ou híbrido, fixo ou móvel, por um período limitado ou indefinido. Os seus objetivos primários são o de utilizar o seu efeito dissuasor para proteger pessoas e bens, podendo também servir para fins probatórios. Esses sistemas, por vezes capazes de recolher registos de som e analisar os dados captados com recurso a diversas tecnologias incorporadas, podem ser considerados uma forma de controlo da atividade laboral à distância.

Tem sido alvo de discussão e vasta análise se os dados resultantes da utilização de meios de videovigilância à distância têm uma equivalência jurídica aos

restantes dados pessoais[288], com reservas quanto à proteção e salvaguarda dos direitos que possam perigar. De acordo com Francisco Marques, a videovigilância é uma operação de tratamento de dados pessoais, no qual estes sistemas são um meio bastante atrativo para garantir a segurança de pessoas e bens, mas também são passíveis de limitar os direitos, pelo que a sua utilização deve ser objeto de delicadas ponderações (Marques, 2021). Na mesma linha de pensamento, Teresa Coelho Moreira considera esses tipos de recursos, disponibilizados tanto para empregadores quanto para trabalhadores, como algo positivo, embora reconheça que o seu uso possa violar determinados direitos fundamentais dos trabalhadores (Moreira, 2012).

Consequentemente, as imagens recolhidas por sistemas de videovigilância constituem dados pessoais, ou pelo menos são suscetíveis de constituir, desde que recolham imagens de pessoas, objetos, ou equipamentos, que permitam, ainda que de forma indireta, a identificação concreta de indivíduos. Por outras palavras, não é necessário que integrem imagens explícitas de pessoas: basta que permitam identificar ou localizar indivíduos, *v.g.* imagens que permitam identificar uma viatura, através da matrícula ou de outra caraterística que atribua a propriedade ou utilização a determinada pessoa (Alves, 2020)[289].

Em determinadas ocasiões, o Comité Europeu para a Proteção de Dados (CEPD) assinala que as imagens captadas por sistemas de videovigilância podem enquadrar-se na categoria de dados pessoais especiais, tais como titulares de dados identificáveis a participar numa manifestação. Denota, também, que o tratamento de categorias especiais de dados requer uma vigilância reforçada e contínua de certas obrigações, por exemplo um elevado nível de segurança e uma avaliação de impacto, quando necessário (CEPD, 2020). Outrossim, os videogramas podem constituir dados biométricos (art.º 4.º, n.º 14 do RGPD). Para que isso aconteça é indispensável que os dados sejam tratados para identificar uma pessoa de forma inequívoca.

2. O conteúdo do Acórdão

[288] Constituem dados pessoais qualquer "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular", art.º 4, n.º 1 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados (Regulamento Geral de Proteção de Dados), o RGPD.

[289] Fora do escopo do RGPD ficam as câmaras que não captam imagem, vulgo "câmaras falsas", apesar de poderem gerar pressão nos indivíduos e, consequentemente, afetarem o direito geral de personalidade (Engelhardt & Durmus, 2020).

O AC de 26 de setembro de 2024 do Tribunal da Relação de Évora (TRE)[290], cujo Relator foi o Des.dor Mário Branco Coelho, debruça-se, essencialmente, sobre a apreciação de indícios de facto e elementos de Direito quanto à legitimidade da captação de imagens por videovigilância como meio de prova em contexto laboral. Utilizando esse elemento probatório, a Ré "R.", uma sociedade comercial de exploração de supermercados, terá despedido a funcionária "A." pelas suas condutas durante o exercício das respetivas funções.

Em síntese, o caso inicia-se com uma ação movida por "A." contra a sua antiga entidade patronal, no Juízo do Trabalho de Santarém, impugnando o seu despedimento por motivos de ilicitude. Seguindo os trâmites processuais, não havendo conciliação na audiência de partes, a entidade empregadora foi chamada a apresentar o articulado de motivação de despedimento. Não concordando com a motivação de "R.", a Autora apresentou contestação e deduziu reconvenção, ao qual "R." respondeu. Posteriormente, realizou-se o julgamento, com a produção da prova requerida pelas partes, ao que foi proferida sentença, julgando a ação procedente, declarando a ilicitude do despedimento e condenando a Ré a indemnizar a Autora. Inconformada com a decisão, a Ré recorreu. Cumpriu ao TRE apreciar e decidir da matéria de facto, procedendo à audição da prova gravada e à visualização dos registos de vídeo que instruem o procedimento disciplinar.

Cingindo-nos ao tema central do nosso comentário, o TRE começou por reforçar a incoerência da sentença, quando esta menciona que as imagens captadas pelo sistema de videovigilância devem serem consideradas nulas, por não terem cumprido os requisitos legais. Enquanto, decidiu-se levar à factualidade provada os factos resultantes das imagens extraídas pelas câmaras que o Tribunal visualizou na audiência final.

Destarte, a Relação refere não ser mais necessário pedir autorização ou notificar a Comissão Nacional de Proteção de Dados (CNPD) para se instalar um sistema de videovigilância no local de trabalho, visto que o RGPD e respetiva lei de execução revogaram tacitamente essa obrigatoriedade. Numa análise particularmente feliz, o TRE indica que art.º 5.º, n.º 2 do RGPD consagrou o "princípio da auto-responsabilidade", na medida em que tem de ser o responsável a garantir a observação dos princípios relativos a dados pessoais[291].

Assim, a Relação considerou que a instalação de placas informativas da existência de sistemas de vigilância, aliada à dupla natureza criminal e disciplinar do processo, legitimaram a utilização dos meios de videovigilância por parte da Ré. Ou seja, desde que os videogramas pudessem ser usados no âmbito de um processo penal, cumprindo os prazos estabelecidos na lei, poderiam ter efeitos para apuramento de responsabilidade disciplinar, sem que a entidade patronal fosse obrigada a aguardar pela conclusão do processo criminal.

[290] Disponível em *https://www.dgsi.pt*.

[291] Também Anabela Luna de Carvalho (Carvalho, 2021) menciona que o RGPD fez com que se passasse de um regime de autorização prévia para uma solução – regra de autorresponsabilização e de autodisciplina no tratamento.

Perante os factos, o TRE reconheceu a justa causa de despedimento e concedeu provimento ao recurso interposto pela empregadora, revogando a sentença recorrida por improcedente na sua totalidade.

3. A videovigilância em contexto laboral

3.1. Videovigilância no panorama transnacional, considerações breves

Antes de analisar a dicotomia entre os direitos dos trabalhadores e empregadores em matéria de videovigilância, há que enquadrar esta temática no panorama jurídico transnacional. Fazendo a ponte entre os limites da vigilância eletrónica e a proteção de dados, existe um conjunto de instrumentos internacionais, designadamente do Conselho da Europa, como a *Convenção Europeia dos Direitos Humanos*, de 1950 (art.º 8.º), alinhada com a *Declaração Universal dos Direitos Humanos*, de 1948 (art.º 12.º), a *Convenção para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais*, de 1981, ou a *Convenção de Budapeste sobre o Cibercrime*, de 2001.

Na União Europeia, a *Carta dos Direitos Fundamentais* enfatiza a proporcionalidade nas restrições ao exercício dos direitos e liberdades no que concerne à proteção de dados pessoais, da vida privada e familiar, do domicílio e das comunicações (art.º 7.º).

A maioria dos Estados-Membros já regulavam a videovigilância no local de trabalho antes da entrada em vigor do RGPD (Riso & Litardi, 2024) e, entretanto, foram adaptando a sua legislação às exigências das especificidades desse regulamento. Em alguns destes países, os sindicatos e as comissões de trabalhadores estão envolvidas no processo de autorização para instalação de CCTV no local de trabalho.

Por exemplo, na Eslovénia, a Lei de Proteção de Dados de 2023[292] destaca que as entidades patronais devem consultar os sindicatos representativos e a comissão de trabalhadores antes de implementar a videovigilância (Riso & Litardi, 2024).

Enquanto em Itália o art.º 4.º do Estatuto dos Trabalhadores[293] estabelece que "os sistemas audiovisuais e outros instrumentos a partir dos quais deriva a possibilidade de controle remoto da atividade dos trabalhadores, podem ser utilizados exclusivamente para necessidades organizacionais e produtivas, para a segurança do trabalho e para a proteção dos bens da empresa e podem ser instalados sob o acordo coletivo estipulado pela representação sindical unitária ou pelos representantes da empresa"[294], ficando excluídos de autorização pelo n.º 2 desse artigo as ferramentas que possam permitir que a sua operação seja controlada pelos próprios funcionários (Conno, 2022).

---

[292] *Zakon o varstvu osebnih podatkov* (ZVOP-2).
[293] *Statuto dei Lavoratori (Legge 300 del 1970)*.
[294] Na ausência de tal acordo, a videovigilância poderá ser instalada com autorização prévia da sede territorial do *Ispettorato Nazionale del Lavoro* (Perino, 2024).

Se em Portugal é proibido, por princípio, a captação de som no horário de trabalho, e a utilização de sistemas de videovigilância por parte dos empregadores para avaliar o desempenho dos seus funcionários, no Direito Espanhol é reconhecida a possibilidade desses controlos existirem mediante certos requisitos legais, para garantir a segurança e o cumprimento das obrigações a que os funcionários estão sujeitos[295-296].

3.2. Videovigilância no ordenamento jurídico português

Numa situação idêntica à apresentada, o CCTV poderia servir para garantir a segurança e o bem-estar do próprio trabalhador. Nesse sentido, o legislador constitucional não dissociou a liberdade da segurança, no art.º 27.º da *Constituição da República Portuguesa* (CRP), criando, desta forma, normas que se pretendem indissociáveis, sem que simultaneamente configurem direitos absolutos (Alves, 2019).

A CRP assegura o direito de reserva da vida privada no n.º 1 do art.º 26.º, a ser conjugado com o art.º 80.º do *Código Civil* (CC), o qual apenas poderá ser restrito quando for necessária a prossecução de interesses legítimos e dentro dos limites do princípio da proporcionalidade[297]. De igual relevância, o art.º 32.º, n.º 8.º, da CRP, trata da validade constitucional da prova, estatuindo que "são nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações". Em concordância com o art.º 32.º da CRP, também o art.º 126.º do *Código de Processo Penal* prevê que "sejam nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas" (n.º 1), "obtidas mediante intromissão na vida privada [...] sem o consentimento do respetivo titular" (n.º 3).

Neste panorama, é importante sublinhar que o direito à imagem está inscrito no art.º 79.º do CC e CRP. Por sua vez, no *Código Penal*, art.º 199.º, são criminalizadas as gravações e fotografias ilícitas, prevendo a punição de quem "fotografar ou filmar outra pessoa, mesmo em eventos em que tenha legitimamente participado". Não é permitida a visualização das imagens, quando não tenha ocorrido uma infração penal que atente contra pessoas e bens, e estas só podem ser comunicadas no termos da lei processual penal.

Em Portugal, a Lei n.º 10/91, de 29 de abril, não previa no seu âmbito de aplicação tratamento de som e imagem, o qual só foi salvaguardado após a Diretiva 95/46/CE, nos *Considerandos* 14 e 17. A Lei n.º 67/98, de 26 de outubro, Lei da Proteção de Dados Pessoais, dava suporte ao conceito de "dado pessoal" no seu art.º 3.º, al. a), em muito semelhante ao disposto no apelidado Pacote de Proteção

[295] *Artículo 20.3, Estatuto de los Trabajadores.*
[296] *Artículo 89, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos.*
[297] Para Miguel Teixeira de Sousa, em Processo Civil, o "carácter lícito ou ilícito da prova não depende de qualquer juízo de proporcionalidade entre os interesses conflituantes das partes", sendo que a prova "ilicitamente obtida através da intromissão na privacidade fica sempre sujeita ao binómio ilicitude/exclusão de ilicitude" (Sousa, 2020).

de Dados, que engloba o RGPD e a Diretiva *Law Enforcement*[298], sem descurar as Leis n.º 58/2019 e n.º 59/2019 de 8 de agosto, que asseguram, respetivamente, a execução na ordem jurídica interna portuguesa do RGPD e a transposição da Diretiva supramencionada.

O regime do exercício da atividade de segurança privada é regulado pela Lei n.º 34/2013, de 16 de maio. Nos termos do seu art.º 31.º, havendo alvará ou licença para o exercício dos serviços de vigilância, poderiam ser utilizados equipamentos eletrónicos de vigilância, com o objetivo de proteger pessoas e bens, desde que sejam ressalvados os direitos e interesses constitucionalmente protegidos e confinados à propriedade do responsável. A gravação de imagem e som só deve ser conservada pelo prazo de 30 dias, findo o qual será, em regra geral, destruído, no prazo máximo de 48 horas.

No entanto, a videovigilância encontra-se espalhada por um conjunto de outros regimes jurídicos setoriais, daí ser enganadora a remissão disposta no n.º 1 do art.º 19.º, da Lei n.º 58/2019 (Marques, 2021): "os sistemas de videovigilância cuja finalidade seja a proteção de pessoas e bens asseguram os requisitos previstos no artigo 31.º da Lei n.º 34/2013, de 16 de maio, com os limites definidos no número seguinte". Exemplo dessa pluralidade é a Lei n.º 95/2021, de 29 de dezembro, que aborda a utilização e acesso a câmaras de vídeo pelas forças e serviços e pela Autoridade Nacional de Emergência e Proteção Civil. Outros dos exemplos que aferem a dispersão normativa deste assunto são a utilização de videovigilância pela *Estradas de Portugal*, agora *Infraestruturas de Portugal*, e pelas concessionárias rodoviárias[299]; no âmbito da utilização em táxis[300]; e ainda com recurso a dispositivos aéreos não tripulados (*drones*)[301].

3.3. Videovigilância no contexto laboral português

Um dos aspetos mais problemáticos da relação laboral é a salvaguarda da esfera pessoal no tempo e local de trabalho (Redinha, 2004). A privacidade no local de trabalho é uma parte importante dos direitos de autonomia dos indivíduos na nossa sociedade e, se não for respeitada, pode ter um impacto profundo no senso de dignidade, liberdade e autonomia dos empregados (Moreira & Andrade, 2016).

As progressivas introduções de novas tecnologias no local de trabalho, com as consequentes e significativas ameaças ao direito à reserva da intimidade da vida privada do trabalhador, já reclamavam a atenção legislativa do *Código do Trabalho*

[298] A Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.
[299] Lei n.º 51/2006, de 29 de agosto; Decreto-Lei n.º 207/2005, de 29 de novembro.
[300] Lei n.º 33/2007, de 13 de agosto.
[301] Despacho n.º 3478/2022, de 24 de março.

(CT) (Festas, 2004). O CT, como aprovado pela Lei n.º 99/2003, de 27 de agosto (CT/03), tipificava que as câmaras de videovigilância não podiam incidir regularmente sobre os trabalhadores durante a atividade laboral e as imagens não podiam ser utilizadas para o controlo da sua atividade e aferição da produtividade (art.º 20.º), salvo para proteção de segurança e bens ou quando a natureza da atividade o justifique. A previsão da norma revelou-se inovadora, garantindo ao trabalhador a reserva da vida privada e assegurando-lhe o direito à imagem (Salazar, 2017).

Consagrados no CT/03 estão outras normas que garantem: a "Liberdade de expressão e de opinião" (art.º 15.º); a "Reserva da intimidade da vida privada" (art.º 16.º); a "Proteção de dados pessoais" (art.º 17.º); a "Integridade Física e Moral" (art.º 18.º); e "Testes e exames médicos" (art.º 19.º).

Com as alterações ao CT pela Lei n.º 7/2009, de 12 de fevereiro (CT/09), tais direitos de personalidade passaram a constar essencialmente dos art.ºs 14.º a 22.º. Além de ter sido adicionado ao art.º 20 o dever de informação do empregador aos trabalhadores aquando utilização de meios de vigilância, foram acrescentados ao CT os "Dados biométricos" (art.º 18.º) e a "Utilização dos meios de vigilância a distância" (art.º 21.º). Este último artigo faz referência à necessidade de autorização da CNPD - que ainda se mantém vigente e será mais adiante alvo do nosso escrutínio - para utilização de meios de vigilância à distância, à questão da proporcionalidade, à conservação e destruição dos dados pessoais, e à obrigatoriedade de um parecer da comissão de trabalhadores. Porém, no CT ficou por legislar a admissão da videovigilância como meio de prova para efeitos de despedimento[302].

Relativamente ao tratamento de dados biométricos dos trabalhadores, que pode pôr em causa os direitos e liberdades dos titulares[303], o CNPD desaconselha a interconexão destes dados com sistemas de videovigilância (CNPD, 2018), não obstante de ser considerado legítimo o tratamento em âmbito controlo de assiduidade e para controlo de acessos às instalações do empregador. Nestes casos, deve assegurar-se que apenas se utilizam representações dos dados biométricos e que o respetivo processo de recolha não permita a reversibilidade dos referidos dados[304], respeitando sempre o princípio da minimização: "[…] mesmo nos casos em que o artigo 9.º, n.º 1 (do RGPD), não se aplica, o responsável pelo tratamento deve sempre tentar minimizar o risco de captação de imagens que revelem outros dados sensíveis (para além do artigo 9.º)" (CEPD, 2020).

Por sua vez, com a Lei n.º 58/2019, foi reforçado que as câmaras não podem incidir sobre o interior de áreas reservadas aos trabalhadores, designadamente áreas

---

[302] Para despedir um trabalhador, a questão da admissibilidade da utilização dos registos obtidos pelos meios de vigilância à distância ficou omissa pelo legislador no CT, justificando um regime especial que precisasse a utilização desse meio de prova para fundamentar o despedimento (Salazar, 2017).

[303] Do tratamento de dados biométricos "emergem riscos acrescidos para os direitos e liberdades dos titulares dos dados, ao serem procedimentos automatizados, quase sempre com recurso a bases de dados geridas por sistemas
de IA — Inteligência Artificial" (Masseno, 2023).

[304] Art.º 28.º da Lei n.º 58/2019.

de refeição, vestiários, ginásios, instalações sanitárias, zonas exclusivamente afetas ao seu descanso, conforme o disposto no seu art.º 19.º, n.º 2, al. d). Em adição ao mencionado, as imagens não podem ser captadas de forma oculta[305], e têm sempre por base as regras genéricas aplicadas ao tratamento de todos os dados pessoais, mais concretamente os princípios de licitude, lealdade e transparência (art.º 5.º do RGPD).

3.4. Comentário ao Acórdão

Inicialmente, no que toca à configuração de justa causa de resolução do contrato do trabalhador e à sua utilização como meio de prova de ilícitos disciplinares, na Jurisprudência havia um entendimento discordante com o presente AC. Designadamente, o Tribunal da Relação de Lisboa, no AC de 19 de novembro de 2008, processo n.º 7125/2008-4, cujo Relator foi o Des.dor Ramalho Pinto[306], enaltece a necessidade de consentimento do trabalhador para a captação de imagens e parte do pressuposto que a videovigilância não deve ser utilizada como meio de prova em sede de procedimento disciplinar, por constituir uma abusiva intromissão na vida privada e violar o direito à imagem do funcionário. Portanto, a nosso ver, numa situação hipotética de desvio ilícito de produtos, análoga ao caso apresentado, um trabalhador estaria beneficiado perante a lei em relação a um outro individuo sem vínculo contratual, violando o princípio da igualdade (art.º 13.º da CRP).

Na opinião sufragada por David Festas, estranho seria que a videovigilância não pudesse fundamentar uma atuação contra aqueles que, pelas funções que desempenham (os trabalhadores), mais poderão atentar contra as finalidades que a instalação visa defender (Festas, 2004). Nesse sentido, nos anos subsequentes houve um entendimento generalizado, partilhado com o presente AC, que "as imagens gravadas e outros dados pessoais registados através da utilização de sistemas de vídeo, ou outros meios tecnológicos de vigilância à distância, podem ser utilizados para efeitos de apuramento de responsabilidade disciplinar, na medida em que o sejam no âmbito do processo penal"[307].

O AC faz referência às atribuições e competências do CNPD, presentemente definidas no art.º 57.º do RGPD e no art.º 6.º da Lei 58/2019, bem como à desnecessidade atual da autorização dessa entidade para instalar sistemas de videovigilância[308], devendo "entender-se que o art.º 21.º n.º 1 do Código do Trabalho está tacitamente revogado pelo citado art.º 5.º n.º 2 do RGPD.". Ora. a discussão em

[305] As gravações ocultas são ilícitas, mesmo que não sejam utilizadas, divulgadas ou até destruídas no imediato (Sousa, 2020).
[306] Disponível em *https://www.dgsi.pt*.
[307] Art.º 28.º, n.ºs 4 da Lei n.º 58/2019.
[308] A própria CNPD faz referência que "com o novo regulamento europeu de proteção de dados, já não é necessário pedir autorização ou fazer alguma notificação à CNPD para ter um sistema de videovigilância" (CNPD, s.d.).

torno desse tópico tem gerado sérias dissensões, fruto dos problemas de interpretação do RGPD com a Lei 58/2019 e da falta de revogação expressa do art.º 21.º aludido.

Consequentemente, a eventual necessidade de autorização prévia por parte da CNPD deveria verificar-se de acordo com o disposto no n.º 4 do art.º 19.º da Lei 58/2019 e não com o art.º 21.º do CT (Mota & Sampaio, 2019). Quer isto dizer que a CNPD continuaria a ter de autorizar a captação de som sempre que os trabalhadores estejam presentes nas instalações. Inclusive, na matéria de facto provada no caso em epígrafe, a transcrição de que houve "informação concretamente não apuradas por não serem audíveis" deixam reservas relativamente ao facto de os sistemas de videovigilância estarem a captar som (se era impercetível, ou inexistente).

De qualquer forma, a revogação da autorização do CNPD não significa que os demais pressupostos previstos no CT e no RGPD possam ser postergados. O n.º 4 do art.º 21 do CT aponta para a autorização do CNPD acompanhada de um parecer da comissão de trabalhadores: "o pedido de autorização a que se refere o n.º 1 deve ser acompanhado de parecer da comissão de trabalhadores ou, não estando este disponível 10 dias após a consulta, de comprovativo do pedido de parecer". Assim, considero que uma eventual revogação expressa do n.º 1 não deveria deixar de fora as estruturas de representação coletiva. Para além disso, a entidade responsável pelo tratamento tem ainda de comprovar o efetivo cumprimento desses pressupostos, ficando a admissibilidade da valoração das correspondentes imagens como meio de prova dependente da alegação e prova do cumprimento de tais requisitos[309].

No seu local de trabalho, um trabalhador provavelmente não espera, na maioria dos casos, ser controlado pelo seu empregador (CEPD, 2020). Ora, o AC em análise não refere se a trabalhadora estava devidamente informada da existência das câmaras de videovigilância e se a entidade empregadora conseguiu provar esse facto para além da mera afixação da sinalização: "foram cumpridos os requisitos do art.º 31.º da Lei 34/2013, de 16 de maio, estando o sistema sinalizado através de placas informativas existentes no local". Aliás, o TRE nem sequer menciona a Portaria n.º 273/2013, de 20 de agosto, art.º 115.º, que exige que os avisos sejam colocados no perímetro exterior do local ou zona objeto de vigilância (n.º 4) e repetidos no interior do local ou zona objeto de vigilância (n.º 5). O não cumprimento das exigências de afixação poderia contribuir para uma eventual falta de perceção da trabalhadora para o facto de estar a ser vigiada na empresa, ou em que zonas isso aconteceria. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando os dados pessoais forem tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional (*Considerando* 47 do RGPD).

[309] AC da Relação de Lisboa, de 14 de dezembro de 2023, processo 17630/22.2T8LSB.L1-4, sendo Relatora a Des.dora Maria José Pinto, disponível em *https://www.dgsi.pt*.

Conquanto a Doutrina não tenha feito ressalvas a cenários em que o trabalhador tenha de consentir ser filmado no seu local de trabalho[310], isso não está totalmente descartado, desde que seja cumprido o art.º 7.º do RGPD: "se o responsável pelo tratamento quiser basear-se no consentimento, tem o dever de se certificar de que cada titular dos dados que entra na área que está sob videovigilância deu o seu consentimento" (CEPD, 2020). Assim, por via do consentimento, os trabalhadores ficariam impedidos de invocar, depois, a ilicitude das lesões respetivas, numa espécie de concretização do brocardo *volenti non fit injuria*[311]. Porém, consideramos também que o consentimento do trabalhador poderia colocar em causa o princípio de igualdade na admissibilidade da prova, comparativamente a outra pessoa sem vínculo laboral.

Adicionalmente, à luz do RGPD, estamos perante um desequilíbrio da relação entre o empregador e o trabalhador[312]. Por isso, o consentimento do trabalhador não seria efetivamente livre, o que é uma condição essencial para que o tratamento seja considerado válido. Nesse seguimento, com o regime jurídico atual, o titular dos dados tem o direito de se opor ao tratamento dos dados pessoais que lhe digam respeito, fazendo-o cessar, o que dificultaria a implementação destes tipos de sistemas de controlo à distância.

Por outro lado, o tratamento de dados dos trabalhadores é necessário para a execução do contrato de trabalho entre o empregador e o trabalhador, sendo esta uma das fontes de licitude (Alves, 2020), e para o cumprimento de obrigações jurídicas a que o empregador esteja sujeito, como, por exemplo, quando tenha de fornecer dados dos salários às autoridades fiscais[313] (Pinheiro & Gonçalves, 2018).

A videovigilância poderia, eventualmente, ter sido utilizada como meio de prova para o despedimento, com base no interesse legítimo da entidade patronal, conforme disposto no art.º 6.º, n.º 1, alínea f) do RGPD. Segundo o CEPD (CEPD, 2024), existem um conjunto de pontos cumulativos necessários para legitimar esse interesse: "*i)* a busca de um interesse legítimo por parte do responsável pelo tratamento ou por um terceiro; *ii)* a necessidade de processar dados pessoais para os fins do(s) interesse(s) legítimo(s) perseguido(s) (ou seja, o processamento de dados pessoais deve ser "necessário" para esses fins); *iii)* os interesses ou as liberdades e direitos fundamentais dos titulares dos dados em questão não podem prevalecer sobre o(s) interesse(s) legítimo(s) do responsável pelo tratamento ou de um terceiro".

---

310 Em matéria de consentimento, Teresa Coelho Moreira (Moreira, 2021) adverte para o conteúdo dúbio manifestado no art.º 28.º, n.º 3, da Lei n.º 58/2019: "deveria ter-se alterado a redação e colocado que "salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais: se do tratamento não resultar uma vantagem jurídica ou económica para o trabalhador" (sublinhado nosso).

311 Também neste sentido, temos o AC do Tribunal da Relação de Coimbra, de 20 de junho de 2021, processo 302/19.2T8MGL.C1, sendo Relatora a Des.dora Sílvia Pires, disponível em *https://www.dgsi.pt*.

312 Art.º 6.º, n.º 1, al. a) e o art.º 9.º, n.º 2, al. a) do RGPD.

313 Art.º 6.º, n.º 1, al. b) e c) do RGPD.

Em síntese, não obstante o art.º 88.º do RGPD ter permitido aos Estados-membros a aprovação de normas especiais a nível laboral, como as efetivadas no art.º 28.º da Lei n.º 58/2019, o legislador europeu teve em conta a colisão de normas dos Estados, garantindo o equilíbrio entre interesses das partes envolvidas, sem que os titulares dos dados enfrentarem um risco sério à sua privacidade.

Resultante das particularidades introduzidas pelo agora referido art.º 88.º, o próprio n.º 2, do art.º 79.º, do CC prevê que para "exigências de polícia ou de justiça", entre outras, não é necessário o consentimento da pessoa retratada, independentemente do seu vínculo laboral. Embora o consentimento seja, em regra, exigível pelo CC - com a ressalva das exceções mencionadas -, poderá já não ser assim ao abrigo do RGPD devido aos fundamentos de licitude anteriormente descritos. No caso do CC, os tribunais têm assumido a presunção de consentimento ou consentimento tácito, ao passo que no RGPD o consentimento tácito não é suficiente. Podendo mesmo considerarem-se as regras do CC em matérias de direitos da personalidade afastada pelo RGPD (Cordeiro, 2023).

Quanto à matéria de proporcionalidade em sentido estrito (não poderão adotar-se medidas excessivas, desproporcionadas para alcançar os fins pretendidos)[314], achamos que seria relevante analisar em que medida a necessidade da Recorrente em lograr a proteção de pessoas e bens justifica uma plenitude de meios de vigilância, que permitem uma descrição minuciosa, algo exacerbada, de todas as movimentações dos trabalhadores no ceio da empresa (*v.g.* "saiu do bombeado, onde tinha deixado o porta-combis antes de ir ao carro vestir as calças de frio"). Até porque não foi aferido se o local onde se praticaram os factos fazia parte das instalações onde é obrigatório a presença desses sistemas[315].

Mesmo em circunstâncias que imponham à Ré a instalação de videovigilância, não só é necessário demonstrar e comprovar o cumprimento dos princípios atrás identificados, como também ponderar entre o interesse legítimo da empresa ou entidade pública e os direitos das pessoas. Além do mais, o responsável pelo tratamento só deve comunicar as imagens no âmbito de processo judicial devidamente identificado, em cumprimento de despacho fundamentado da autoridade judiciária competente (Alves, 2020); fornecer as gravações às pessoas abrangidas pelas imagens, salvo se estiverem a ser utilizadas no âmbito de investigação criminal; e fazer cumprir a segurança, a confidencialidade dos dados e limite de tempo de armazenamento estabelecido na lei, respeitando os princípios da minimização e da finalidade.

4. Algumas conclusões e perspetivas futuras

O núcleo da disputa do recurso que deu origem a este AC estava centrado na questão de as imagens de videovigilância poderem ser legalmente usadas para

[314] Citado pelo AC n.º 634/93 do Tribunal Constitucional, processo n.º 94/92, tendo por Relator o Cons.º Luís Nunes de Almeida, disponível em *https://www.tribunalconstitucional.pt*.
[315] Art.º 8.º da Lei n.º 46/2019, de 8 de julho.

comprovar condutas inadequadas no ambiente de trabalho, que resultem em processo-crime e disciplinar, com respetivo despedimento.

Na Jurisprudência é unânime o entendimento quanto à videovigilância implicar restrições aos direitos, liberdades e garantias dos trabalhadores. Em circunstâncias cuja finalidade esteja restrita à proteção de pessoas e bens, ultimamente tem prevalecido a orientação em cujos termos os videogramas podem considerados como meios de prova, desde que se cumpram os pressupostos legais e sejam primariamente utilizados para fins penais. O que revela um maior equilíbrio entre os direitos dos trabalhadores, das próprias empresas e da manutenção do Estado de Direito.

Contudo, com a entrada em vigor do RGPD, ficaram em aberto algumas questões acerca da articulação de outros regimes, como o CT e o CC. Em qualquer caso, que vai continuar a existir a necessidade de uma interpretação de toda a legislação laboral à luz do RGPD.

Futuramente, com a proliferação de novos dispositivos e tecnologias digitais de recolha e manipulação de dados, passará a existir um enorme risco para a privacidade dos trabalhadores. Isso levará, cada vez mais, o responsável pelo tratamento a tomar em consideração tecnologias respeitadoras da privacidade, utilizando, por exemplo, filtros de *pixalização*[316], ou até a evitar a instalação de câmaras rotativas que abranjam áreas de vigilância proibida.

A meu ver, se o legislador português quiser continuar a exigir a proteção do trabalhador face ao controlo da sua performance por meios de videovigilância, terá de reforçar as suas recomendações ou a imposição de medidas para minimizar o risco de violação de privacidade, já que a instalação desproporcional destes sistemas, mesmo que as finalidades estejam devidamente fundamentadas, não exclui completamente o controlo das suas ações e eventuais danos às relações laborais.

À semelhança do que ocorre em alguns países da União Europeia, consideramos que o envolvimento de sindicatos, comissões de trabalhadores, ou de outras estruturas de representação coletiva, no processo de autorização de CCTV em locais de trabalho, poderia ser uma adição valiosa na garantia dos direitos laborais. Aí sim, em caso de desacordo, a CNPD poderia exercer a última palavra.

Agradecimentos

O meu sincero agradecimento ao Prof. Manuel David Masseno pela orientação enquanto docente e pelo constante empenho no fortalecimento da ligação entre o Direito e a Engenharia Informática.

316 Designadamente, a *Préposé fédéral à la protection des données et à la transparence,* entidade responsável na Suíça por aconselhar, educar e garantir a proteção de dados pessoais nesse território, recomenda, caso a vigilância seja "absolutamente necessária", o emprego de filtros de *pixalização* nas faces, para proteger a privacidade dos trabalhadores que estão a ser filmados em tempo real (FDPIC, 2024).

Bibliografia

Alves, L. D. (2020). Proteção de Dados Pessoais no Contexto Laboral - O Direito à Privacidade do Trabalhador. Coimbra: Almedina. ISBN: 978-972-40-8612-5, pp. 38-44.

Alves, L. D. (2019). A videovigilância e a compressão da privacidade. In *Anuário da Proteção de Dados 2019*, pp. 137-155. Disponível em: https://cedis.novalaw.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf

Carvalho, A. L. de (2021). A videovigilância no local de trabalho. Os limites da proteção de dados na jurisprudência laboral. Os desafios do Teletrabalho. In *DataVenia - revista jurídica digital*, 9(12), pp. 141-174. Disponível em: https://datavenia.pt/ficheiros/edicao12/datavenia12_p141_174.pdf

Comissão Nacional de Proteção de Dados (s.d.), "Áreas temáticas: Videovigilância". Disponível em https://www.cnpd.pt/organizacoes/areas-tematicas/videovigilancia/

Comissão Nacional de Proteção de Dados (2018). Parecer n.º 20/2018 sobre Proposta de Lei n.º 120/XIII. Disponível em: https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/120328

Comité Europeu para a Proteção de Dados (2024). Diretrizes 1/2024 sobre o processamento de dados pessoais baseados no artigo 6(1)(f) do RGPD. Disponível em: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_pt

Comité Europeu para a Proteção de Dados (2020). Diretrizes 3/2019 sobre o tratamento de dados pessoais através de dispositivos de vídeo. Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_de vices_pt.pdf

Conno, A. D. (2022). *Controllo a distanza dei lavoratori e strumenti informatici*. In *Altalex - Quotidiano di informazione giuridica*. Disponível em: https://www.altalex.com/documents/news/2022/03/04/controllo-a-distanza-dei-lavoratori-e-strumenti-informatici

Cordeiro, A. B. M. (2023). Direitos de personalidade e dados pessoais: o que sobra para o Código Civil? In Revista de Direito Civil, VIII(1), 45-63. Disponível em: https://www.revistadedireitocivil.pt/artigos/direitos-de-personalidade-e-dados-pessoais-o-que-sobra-para-o-codigo-civil

Engelhardt, J. & Durmus, E. (2020). Are there information duties for camera dummies? In *NOTOS-Xperts*. Disponível em: https://notos-xperts.de/assets/Uploads/Elements/FileList/Information-duties-for-camera-dummies-NOTOS-Xperts.pdf

Federal Data Protection and Information Commissioner (2024), *Monitoring employees: video surveillance in the workplace*. Disponível em https://www.edoeb.admin.ch/en/video-surveillance-in-the-workplace

Festas, D. (2004). O direito à reserva da intimidade da vida privada do trabalhador no Código do Trabalho. In *Revista da Ordem dos Advogados*, II. Disponível em: https://www.oa.pt/Conteudos/Artigos/detalhe_artigo.aspx?idsc=45841&ida=47185

Masseno, M. D. (2023). Da vigilância biométrica no Ordenamento da União Europeia (Para fins de segurança em espaços acessíveis ao público). In Fonseca, Isabel Celeste (Org.) - *Cidades inteligentes e direito, governação digital e direitos: desafios futuros globais*. Coimbra: GESTLEGAL, ISBN: 9789895374540, pp. 275-296. Disponível

em:
https://repositorium.sdum.uminho.pt/bitstream/1822/91367/1/Ebook%20Cidades%20Inteligentes.pdf

Marques, F. P. (2021) In Cordeiro, M. (Org.) - *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*. Editora Almedina. ISBN: 978-972-40-9289-8, pp. 596-598.

Moreira, T. C. (2021). Proteção de dados e emprego público. In AA.VV. *Direito à Informação Administrativa e Proteção de Dados. Lisboa: Centro de Estudos Judiciários*, pp. 33-50. Disponível em: https://cej.justica.gov.pt/LinkClick.aspx?fileticket=4qCUnhbJfM8%3d&portalid=30

Moreira, T. C. (2012). Novas Tecnologias: um admirável mundo novo do trabalho? In *Revista de Direito e Garantias Fundamentais*, 11, pp. 15-52. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/209/115

Moreira, T. C. & Andrade, F. P. (2016). Personal Data and Surveillance: The Danger of the "Homo Conectus. In *Ambient Intelligence and Smart Environments*, 21, pp. 115.124. Disponível em: https://ebooks.iospress.nl/volumearticle/45165

Mota, J., & Sampaio, A. (2019). Regulamento Geral de Proteção de Dados em Portugal – alguns apontamentos à sua lei de execução. In *Actualidad Jurídica Uría Menéndez*, 53, pp. 142-148.
Disponível em: https://www.uria.com/documentos/publicaciones/6855/documento/port01.pdf.

Perino, L. (2024). Videosorveglianza in azienda: norme e adempimenti. In *NT+ Diritto*. Disponível em: https://ntplusdiritto.ilsole24ore.com/art/videosorveglianza-azienda-norme-e-adempimenti-AF4blohC

Pinheiro, A. & Gonçalves, C. (2018). In Pinheiro, A. (Org.) - *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina. ISBN: 978-972-40-7786-4, pp. 212-227.

Redinha, M. R. (2004). Os Direitos de Personalidade no Código do Trabalho: Actualidade e Oportunidade da sua Inclusão. In AA.VV. *A Reforma do Código do Trabalho – Centro de Estudos Judiciários*. Coimbra, Coimbra Editora. ISBN 972-32-1290-0, 161-171. Disponível em: https://sigarra.up.pt/fdup/pt/pub_geral.show_file?pi_doc_id=6296

Riso, S., & Litardi, C. (2024). *Employee monitoring: A moving target for regulation*. In *European Foundation for the Improvement of Living and Working Conditions*.

Disponível em: https://www.eurofound.europa.eu/en/resources/article/2024/employee-monitoring-moving-target-regulation

Salazar, H. (2017). A utilização pelo empregador dos registos obtidos através dos meios de vigilância à distância como meio de prova para despedir o trabalhador: síntese de uma discussão jurisprudencial. In Lambelho, A., Mendes, J. B. & Dinis, M. (Org.). *Atas do IX Congresso Internacional de Ciências Jurídico-Empresariais: O Direito do Trabalho e as Empresas*. Leiria: Instituto Politécnico de Leiria, 2183-5330, pp. 80-96. Disponível em: https://iconline.ipleiria.pt/bitstream/10400.8/4538/1/Atas_IX_CICJE.pdf

Sousa, M. T. (2020). Provas ilicitamente obtidas por particulares. In *Revista da Faculdade de Direito da Universidade de Lisboa*, LXI(2), pp. 15-52. Disponível em: https://www.fd.ulisboa.pt/wp-content/uploads/2021/10/Miguel-Teixeira-de-Sousa.pdf

Considerações sobre o Regulamento dos Serviços Digitais - Regulamento (UE) 2022/2065 de 19 de outubro de 2022

Renata Guilardi de Oliveira Castro [317]

[317] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Introdução

Os serviços prestados normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário, são definidos, nos termos da Diretiva (UE) 2015/1535, como "serviços da sociedade de informação".

Dentre eles, se destacam os serviços intermediários, que podem ser, conforme o artigo 3.º, g, do Regulamento dos Serviços Digitais: de "simples transporte" (transmissão de informações prestadas por um destinatário do serviço ou na concessão de acesso a uma rede de comunicações), de «armazenagem temporária» (transmissão de informações prestadas por um destinatário do serviço, que envolve a armazenagem automática, intermédia e temporária dessas informações efetuada apenas com o objetivo de tornar mais eficaz a transmissão posterior das informações a outros destinatários, a pedido destes) ou de «alojamento virtual» (armazenagem de informações prestadas por um destinatário do serviço e a pedido do mesmo).

Esses serviços fazem parte da vida dos cidadãos europeus e são essenciais para a economia da União, por isso a importância do Regulamento dos Serviços Digitais, no sentido de evitar a propalação de conteúdos ilegais e de desinformação (*fake news)* na rede de comunicações, bem como os riscos sociais dela decorrentes, sejam através das redes sociais ou das plataformas em linha.

1. Objeto da Resolução

O objetivo do Regulamento dos Serviços Digitais é promover um comportamento responsável e diligente por parte dos prestadores de serviços intermediários (empresas que disponibilizam informações, a pedido do destinatário do serviço que as forneceu, a um número potencialmente ilimitado de terceiros), a fim de garantir um ambiente em linha seguro, previsível e fiável, assegurando os direitos fundamentais dos cidadãos da União, como a liberdade de expressão, a liberdade de empresa e a defesa do consumidor.

Por outro lado, o Regulamento dos Serviços Digitais não pode responsabilizar os prestadores de serviços digitais de forma objetiva quando algum tipo de conteúdo digital é divulgado pelos destinatários, pois a União Europeia almeja a expansão de novos serviços no mercado interno da União Europeia, o que é essencial para se manter competitiva na era digital, e onerar as empresas pode ser um óbice.

Entende-se por conteúdos ilegais "quaisquer informações que, por si só ou em relação a uma atividade, incluindo a venda de produtos ou a prestação de serviços, não estejam em conformidade com o direito da União ou com o direito de qualquer um dos Estados-Membros que seja conforme com o direito da União,

independentemente do objeto ou da natureza precisa desse direito;" (artigo 3.º, h, do Regulamento dos Serviços Digitais).

Para atingir esse objetivo, é essencial um quadro normativo harmónico entre os Países-Membros, para evitar a fragmentação do mercado interno, garantir condições de concorrência equitativas no mercado interno, segurança jurídica e promover a interoperabilidade.

Assim, o Regulamento dos Serviços Digitais define em que situações os prestadores de serviços intermediários não podem ser responsabilizados por conteúdos ilegais fornecidos pelos destinatários do serviço, todavia, as isenções de responsabilidade não se aplicarão quando o prestador de serviços intermediários criar, editar ou distribuir conteúdos sob responsabilidade editorial, desempenhando um papel ativo, ou seja, quando tiver conhecimento ou controle sobre os conteúdos ilegais, ou ainda, se colaborar intencionalmente com um destinatário para facilitar atividades ilegais.

Essas regras variam conforme o tipo de atividade: "simples transporte", "armazenagem temporária" ou "alojamento virtual".

No caso de "simples transporte" o prestador não é responsável desde que (artigo 4.º do Regulamento dos Serviços Digitais):

a) *Não esteja na origem da transmissão;*
b) *Não selecione o destinatário da transmissão; e*
c) *Não selecione nem modifique as informações objeto da transmissão.*

No caso de "armazenagem temporária", o prestador do serviço não é responsável desde que que (artigo5.º do Regulamento dos Serviços Digitais):

a) *Não modifique as informações:*
b) *Respeite as condições de acesso às informações;*
c) *Respeite as regras relativas à atualização das informações, indicadas de forma amplamente reconhecida e utilizada pelo sector;*
d) *Não interfira com a utilização legítima da tecnologia, tal como amplamente reconhecida e utilizada pelo sector, aproveitando-a para obter dados sobre a utilização das informações; e*
e) *Atue com diligência para suprimir ou bloquear o acesso às informações que armazenou, logo que tome conhecimento efetivo de que as informações foram suprimidas da rede na fonte de transmissão inicial, de que o acesso às mesmas foi bloqueado, ou de que uma autoridade judiciária ou administrativa ordenou essa supressão ou desativação de acesso.*

No caso de "alojamento virtual", o prestador do serviço não é responsável desde que que (artigo 6.º do Regulamento dos Serviços Digitais):

a) *Não tenha conhecimento efetivo da atividade ou conteúdo ilegal e, no que se refere a uma ação de indemnização por perdas e danos, não tenha conhecimento de factos ou de circunstâncias que evidenciem a ilegalidade da atividade ou do conteúdo; ou*

b) *A partir do momento em que tenha conhecimento da ilicitude, atue com diligência no sentido de suprimir ou desativar o acesso aos conteúdos ilegais.*

Apesar de os prestadores de serviços intermediários não terem a obrigação geral de controlar as informações que transmitem ou armazenam, nem de procurar ativamente factos ou circunstâncias que indiquem ilicitudes, eles têm obrigações de diligência para um ambiente em linha transparente e seguro.

Assim, após receberem uma decisão de atuação, ou uma decisão de prestação de informações específicas sobre um ou mais destinatários individuais específicos do serviço, emitida pelas autoridades judiciárias ou administrativas nacionais competentes, os prestadores de serviços intermediários devem informar, sem demora injustificada, à autoridade que emitiu a ordem, ou qualquer outra autoridade especificada na ordem, da sua receção e do seguimento que lhe foi dado, especificando se e quando a ordem foi executada.

Eles também informam o destinatário do serviço em causa da decisão recebida e do seguimento que lhe foi dado. As informações comunicadas ao destinatário do serviço incluem a exposição dos motivos, as possibilidades de reparação existentes e uma descrição do âmbito territorial da ordem.

Para evitar que as plataformas em linha de muito grande dimensão e os motores de pesquisa em linha de muito grande dimensão influenciem a segurança em linha, a formação da opinião pública e o comércio em linha, o Regulamento impõe regras específicas para essas empresas, como, por exemplo, avaliação dos riscos sistémicos decorrentes da conceção, do funcionamento e da utilização dos seus serviços e criação de meios para atenuar esses riscos.

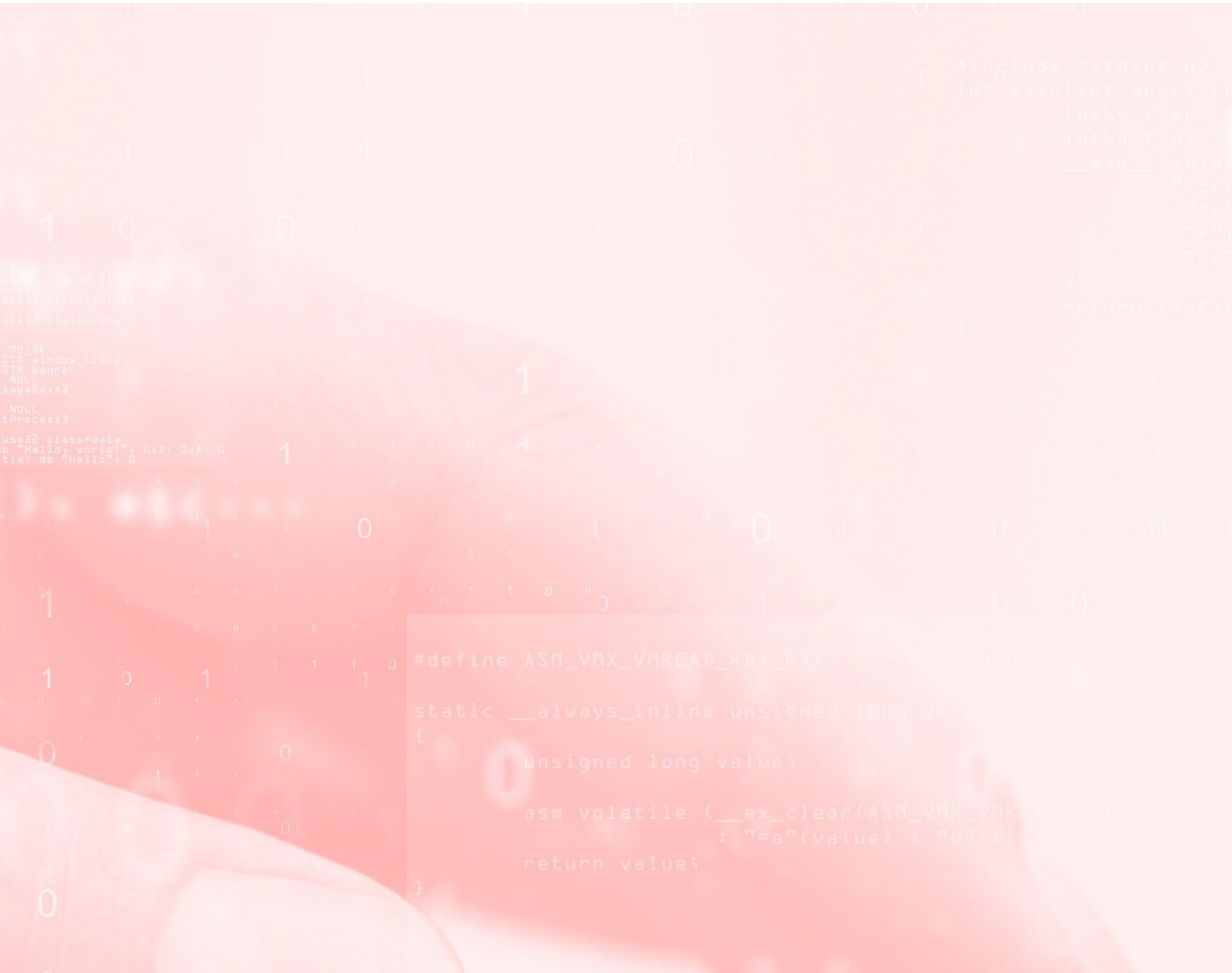
Para viabilizar as comunicações das autoridades dos Estados-Membros, da Comissão e do Comité Europeu dos Serviços Digitais, os prestadores de serviços intermediários devem designar um ponto único de contacto. A Comissão e o Comité, junto com os coordenadores dos serviços digitais, têm a função de fiscalizar o cumprimento do Regulamento, bem como contribuem para a elaboração de códigos de conduta para contribuir para a sua correta aplicação, que incluem a questão da publicidade em linha.

Por esse ponto único de contacto, os destinatários do serviço poderão comunicar direta e rapidamente com os prestadores de serviços intermediários e poderão ter acesso às informações atualizadas sobre as decisões acerca de conteúdos ilegais.

Conclusão

Tanto a Carta dos Direitos Fundamentais da União Europeia quanto os princípios gerais do direito da União fundamentam e justificam o Regulamento dos Serviços Digitais, nomeadamente o direito à liberdade de expressão e de informação, e a liberdade e o pluralismo dos meios de comunicação social.

Portanto, os órgãos competentes para efetivar e fiscalizar o cumprimento do Regulamento devem, no caso de conflito entre direitos fundamentais, buscar o equilíbrio entre eles, conforme o princípio da proporcionalidade, tendo em conta os seus objetivos principais.



III
OUTROS ESTUDOS

Blockchain como Pilar para um Sistema Global de Propriedade Intelectual: Uma Abordagem Descentralizada e Universal

João Mateus [318]

Cristina Maria de Gouveia Caldeira [319]

Resumo

O presentee estudo constitui as primeiras reflexões de um projeto de investigação que explora a aplicação da tecnologia blockchain como um pilar para a criação de um sistema global de Propriedade Intelectual (PI) que seja descentralizado, transparente e universalmente acessível. O projeto desenvolve-se no âmbito da linha de investigação "Propriedade Intelectual, Direito da Saúde e Inovação", que constitui um eixo central da investigação produzida no Privacy and Data Protection Centre, uma unidade de investigação da Universidade Europeia.

A proposta central é utilizar blockchain para superar os desafios dos sistemas tradicionais de registo de PI, como fragmentação jurisdicional, altos custos e dificuldades na proteção internacional. Através de um modelo baseado em blockchain, os autores sugerem um registo descentralizado de PI, utilizando timestamps e chaves criptográficas para garantir a autoria e a criação de obras de forma imutável. Além disso, propõe o uso de contratos inteligentes para automatizar o licenciamento e a gestão de royalties, garantindo transações seguras e transparentes. O estudo também aborda como a blockchain pode verificar a autenticidade e combater a falsificação de produtos protegidos por PI. Com ênfase nos benefícios, como redução de custos, maior acessibilidade e eliminação de intermediários, o estudo discute as implicações e desafios para a implementação, incluindo questões regulatórias e de escalabilidade. Um estudo de caso hipotético

318 Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

319 Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

ilustra o funcionamento prático do sistema proposto, destacando os impactos positivos potenciais.

Palavras-chave: tecnologia blockchain, Propriedade Intelectual (PI), modelo baseado em blockchain, contratos inteligentes, licenciamento, royalties

Abstract

This study constitutes the first reflections of a research project that explores the application of blockchain technology as a pillar for the creation of a global Intellectual Property (IP) system that is decentralized, transparent and universally accessible. The project is developed within the scope of the research line "Intellectual Property, Health Law and Innovation", which constitutes a central axis of the research produced at the Privacy and Data Protection Centre, a research of the Universidade Europeia. The central proposal is to use blockchain to overcome the challenges of traditional IP registration systems, such as jurisdictional fragmentation, high costs and difficulties in international protection. Through a blockchain-based model, the authors suggest a decentralized IP registry, using timestamps and cryptographic keys to guarantee the authorship and creation of works in an immutable way. In addition, it proposes the use of smart contracts to automate licensing and royalty management, ensuring secure and transparent transactions. The study also addresses how blockchain can verify the authenticity and combat counterfeiting of IP-protected products. With an emphasis on benefits, such as cost reduction, greater accessibility and elimination of intermediaries, the study discusses the implications and challenges for implementation, including regulatory and scalability issues. A hypothetical case study illustrates the practical operation of the proposed system, highlighting potential positive impacts.

Keywords: blockchain technology, Intellectual Property (IP), blockchain-based model, smart contracts, licensing, royalty

Introdução

A Propriedade Intelectual (PI) desempenha um papel crucial na proteção das criações humanas, incentivando a inovação e o desenvolvimento econômico global. No entanto, os sistemas tradicionais de registro e proteção de PI enfrentam desafios significativos, como a fragmentação entre jurisdições, altos custos e a complexidade na proteção internacional. Esses obstáculos dificultam o acesso e a eficácia do sistema para muitos criadores e empresas, especialmente em mercados emergentes.A tecnologia blockchain surge como uma solução promissora para esses desafios, oferecendo um sistema de registro global, descentralizado e universalmente reconhecido.

Com características como transparência, segurança e imutabilidade, a blockchain tem o potencial de transformar a gestão de PI ao eliminar intermediários e reduzir custos. Este artigo explora como a blockchain pode ser aplicada ao contexto da Propriedade Intelectual, propondo um modelo que aproveita suas capacidades para criar um sistema mais eficiente e acessível.O objetivo deste artigo é apresentar um modelo baseado em blockchain para o registro e gestão de PI, destacando suas vantagens e abordando os desafios de implementação. A proposta inclui o uso de registros descentralizados, smart contracts para licenciamento automatizado e mecanismos para verificar a autenticidade e combater a falsificação. Ao explorar essas soluções, o artigo visa demonstrar como a blockchain pode oferecer um novo paradigma para a proteção e gestão de Propriedade Intelectual, beneficiando criadores e empresas em todo o mundo.

1.1. Contexto e Relevância

A Propriedade Intelectual (PI) é um pilar fundamental da economia global moderna, incentivando a inovação e a criatividade ao proteger os direitos de inventores, artistas e empresas. No mundo atual, onde a tecnologia e a informação são motores essenciais de crescimento econômico, a PI desempenha um papel vital na promoção do desenvolvimento econômico, cultural e social. Ela garante que os criadores possam obter o reconhecimento e os benefícios financeiros de suas invenções e obras, estimulando assim um ciclo contínuo de inovação.

Entretanto, o sistema tradicional de proteção de PI enfrenta desafios significativos, ao mesmo tempo que a IA, a robótica e o uso de tokens não fungíveis/Non-fungible Tokens (NFT), apresentam-se como algo inovador, que deve ser acompanhado de novos contornos jurídicos à escala planetária.

Considerando a relevância da criação para a sociedade, o Código do Direito de Autor e Direitos Conexos (CDADC) atribui a titularidade da obra ao criador intelectual, pertencendo-lhe o direito de autor sobre a sua criação (art. 11.º CDADC). O art. 12.º do mesmo Código estabelece que «O direito de autor é reconhecido independentemente de registo, depósito ou qualquer outra formalidade.». O artigo 2.º da Convenção de Berna para a Proteção das Obras Literárias e Artísticas (Acto

de Paris de 24 de Julho de 1971), na versão de 28 de Setembro de 1979, estabelece que, «1) Os termos 'obras literárias e artísticas' compreendem todas as produções do domínio literário, científico e artístico, qualquer que seja o seu modo ou forma de expressão, tais como: os livros, folhetos e outros escritos;"

A tecnologia digital tem cada vez mais impacto no auxílio à disseminação das criações intelectuais, obras cujos suportes vão além do meio físico. Nesse contexto inscrevem-se as obras audiovisuais, as quais apresentam-se como criações acessíveis a um número muito amplo de pessoas, mas igualmente expostas a riscos que se prendem com a pirataria e o plágio, sendo necessário apurar se os instrumentos jurídicos tradicionais respondem aos desafios do presente. Importa ainda compreender se o software pode ser protegido pelo direito de autor e o que será necessário para cumprir o critério da originalidade. Impõe-se então familiarizar-se com a máquina e procurar entender se a IA pode criar ou auxiliar na produção das obras intelectuais.

Considerando o ambiente digital e atendendo ao impacto na propriedade intelectual, levou o Tribunal de Justiça, no acórdão de 16 de Julho de 2009, Processo C-5/08[320], a sublinhar que,

> «6) Sem uma harmonização a nível comunitário, as actividades legislativa e regulamentar a nível nacional, já iniciadas, aliás, num certo número de Estados- -Membros para dar resposta aos desafios tecnológicos, podem provocar diferenças significativas em termos da protecção assegurada e, consequentemente, traduzir-se em restrições à livre circulação dos serviços e produtos que incorporam propriedade intelectual ou que nela se baseiam, conduzindo a uma nova compartimentação do mercado interno e a uma situação de incoerência legislativa e regulamentar. O impacto de tais diferenças e incertezas legislativas tornar-se-á mais significativo com o desenvolvimento da sociedade da informação, que provocou já um aumento considerável da exploração transfronteiras da propriedade intelectual. Este desenvolvimento pode e deve prosseguir. (…) Um sistema rigoroso e eficaz de protecção do direito de autor e direitos conexos constitui um dos principais instrumentos para assegurar os recursos necessários à produção cultural europeia, bem como para garantir independência e dignidade aos criadores e intérpretes. (22) O objectivo de apoiar adequadamente a difusão cultural não deve ser alcançado sacrificando a protecção estrita de determinados direitos nem tolerando formas ilegais de distribuição de obras objecto de contrafacção ou pirataria. (31) Deve ser salvaguardado um justo equilíbrio de direitos e interesses entre as diferentes categorias de titulares de direitos, bem como entre as diferentes categorias de titulares de direitos e utilizadores de material protegido. […].

[320] Acórdão do Tribunal de Justiça (Quarta Secção) 16 de Julho de 2009, Processo C-5/08. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62008CJ0005

O caminho percorrido pelo Direito europeu em matéria de propriedade intelectual, e em particular da tutela dos direitos de autor, permite-nos observar que a Diretiva (UE) 2019/790, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos direitos de autor e direitos conexos no mercado único digital integrou os vetores principais do direito de autor na era digital, pronunciadas pelo Tribunal de Justiça da União Europeu. Porém, a fragmentação entre as diferentes jurisdições cria complexidade e ineficiências, tornando o processo de registo e proteção caro e demorado. Além disso, a falta de um sistema universalmente reconhecido pode levar a disputas legais e incertezas sobre a titularidade e a autenticidade das criações, prejudicando tanto os criadores quanto os consumidores.

Diante desse cenário, há uma necessidade crescente de um sistema mais eficaz e universal para a gestão da Propriedade Intelectual. Um sistema que não só simplifique os processos de registo e proteção, mas que também ofereça maior transparência, segurança e acessibilidade a criadores de todo o mundo. A tecnologia blockchain, com suas características de descentralização e imutabilidade, apresenta-se como uma solução potencial para esses desafios, prometendo revolucionar a forma como a PI é gerida e protegida em escala global.

1.2. Desafios Atuais

Os sistemas tradicionais de registo de Propriedade Intelectual (PI) enfrentam uma série de desafios que limitam sua eficácia e acessibilidade. Entre os principais problemas, destacam-se:

1. **Fragmentação entre Jurisdições**: A PI é regida por leis nacionais, o que significa que os direitos de proteção variam de um país para outro. Essa fragmentação cria complexidade para os criadores que desejam proteger suas invenções ou obras em múltiplos mercados. A necessidade de cumprir com diferentes requisitos legais e procedimentos administrativos em cada jurisdição pode ser um processo moroso e complicado.

2. **Custos Elevados**: O registo e a manutenção de direitos de PI podem ser caros, especialmente para pequenas empresas e inventores individuais. As taxas de registo, juntamente com os custos de tradução, assessoria jurídica e gestão de portfólios de PI em várias jurisdições, podem representar um obstáculo significativo para muitos criadores.

3. **Dificuldades na Proteção Internacional**: A proteção eficaz da PI em âmbito internacional é um desafio devido à falta de harmonização entre as leis de diferentes países. Isso pode levar a conflitos de direitos, onde uma invenção

ou obra é protegida em um país, mas não em outro, expondo os criadores a riscos de infração e litígios.

4. **Tempo e Burocracia**: O processo de obtenção de direitos de PI pode ser demorado, com longos períodos de espera para o exame e aprovação de pedidos. A burocracia envolvida pode desmotivar os inovadores e atrasar o tempo de colocação de novos produtos ou tecnologias no mercado.

Esses desafios destacam a necessidade urgente de reformar os sistemas de PI para torná-los mais eficientes, acessíveis e capazes de atender às necessidades de um mercado globalizado. A busca por soluções inovadoras, como a adoção de tecnologias emergentes, é crucial para superar essas limitações e promover um ambiente mais favorável à inovação e ao crescimento econômico.

1.3. Objetivo do Estudo

O objetivo deste estudo é propor um modelo inovador para a gestão e registo de Propriedade Intelectual (PI) que aproveita a tecnologia blockchain. Este modelo visa superar as limitações dos sistemas tradicionais ao oferecer uma solução que seja descentralizada, transparente e universalmente acessível.

A proposta centra-se em criar uma plataforma de registo de PI que opere em uma rede blockchain, permitindo que todos os participantes tenham acesso igual e seguro às informações. A descentralização elimina a dependência de uma autoridade central, reduzindo custos e burocracia, e aumentando a eficiência do processo de registo.

Além disso, a transparência inerente à tecnologia blockchain assegura que todas as transações e registos de PI sejam verificáveis e imutáveis, proporcionando maior confiança e proteção contra fraudes. A universalidade do modelo proposto facilita a proteção internacional de direitos de PI, permitindo que criadores e empresas registrem suas invenções e obras de forma simplificada e uniforme em múltiplas jurisdições.

Em suma, este estudo procura apresentar um caminho viável para modernizar o sistema de registo de PI, promovendo um ambiente mais inclusivo e dinâmico para a inovação global.

Fundamentos da Tecnologia Blockchain

1.4. Conceito de Blockchain

A blockchain é uma tecnologia de registo distribuído que permite a partilha segura de informações entre múltiplas partes sem a necessidade de uma autoridade central. Funciona como um livro-razão digital, onde as transações são registadas de forma cronológica e imutável.

Estrutura da Blockchain

Blocos: A blockchain é composta por uma série de blocos, cada um contendo um conjunto de transações. Cada bloco possui um identificador único chamado de "hash", que é gerado a partir das informações contidas nesse bloco.

1. **Hashing**: O hashing é um processo criptográfico que transforma os dados de um bloco em uma sequência de caracteres de comprimento fixo. Este hash serve como uma impressão digital do bloco, garantindo que qualquer alteração nos dados resulte em um novo hash, tornando as fraudes facilmente detectáveis.
2. **Consenso Descentralizado**: A blockchain opera em uma rede de computadores (nós) que trabalham juntos para validar e registar transações. O consenso descentralizado refere-se ao processo pelo qual esses nós concordam sobre o estado atual da rede. Os algoritmos de consenso, como Proof of Work (PoW) ou Proof of Stake (PoS), asseguram que todos os nós tenham uma cópia idêntica da blockchain, mantendo a integridade e segurança dos dados.

1.5. Prova de Imutabilidade e Segurança

Os negócios de arte atraem cada vez mais investidores, que procuram investir em obras de arte, utilizando os tokens não fungíveis (NFT)/Non-fungible Tokens (NFT), tokens que certificam as obras, ou qualquer objeto quantitativamente limitado. O mercado dos NFT consolidou-se, com benefício para o setor cultural que encontrou nos NFTS um novo fôlego financeiro para a produção digital. Quer tratando-se de arte fungível, quer de arte digital, ao adquirir um NFT, o titular adquire o registo certificado de originalidade, designadamente de pinturas, fotografias, desenhos, músicas, jogos, escultura ou bem imobiliário, transformando-o em ativo digital.

Mas, os negociadores de arte passaram a olhar para a blockchain, sendo esta conhecida pela sua natureza imutável e segura, o que a torna uma tecnologia confiável para o registo de transações e dados. Vejamos como a imutabilidade e a segurança são asseguradas:

Imutabilidade dos Registos

1. **Ligação de Blocos**: Cada bloco na blockchain contém um hash do bloco anterior, criando uma cadeia ininterrupta. Se alguém tentasse alterar os dados de um bloco, o hash desse bloco mudaria, quebrando a ligação com o bloco seguinte e tornando a alteração evidente para todos na rede.
2. **Distribuição Descentralizada**: A blockchain é armazenada em múltiplos nós distribuídos por toda a rede. Qualquer tentativa de alteração de um bloco em um nó específico seria detectada e rejeitada pelos outros nós, preservando a integridade da cadeia.

Segurança dos Dados

1. **Hashing**: O hashing garante que qualquer alteração nos dados de um bloco resulte em um hash completamente diferente. Isso não só ajuda a manter a integridade dos dados, mas também facilita a detecção de alterações não autorizadas.
2. **Criptografia Assimétrica**: A blockchain utiliza criptografia assimétrica para garantir a segurança das transações. Cada utilizador possui um par de chaves: uma chave pública, que é partilhada com outros, e uma chave privada, que é mantida em segredo. As transações são assinadas digitalmente com a chave privada do remetente, garantindo que apenas o proprietário dessa chave possa autorizar a transação.
3. **Algoritmos de Consenso**: Mecanismos como Proof of Work (PoW) e Proof of Stake (PoS) asseguram que as transações sejam validadas de forma segura e que todos os nós concordem sobre o estado da blockchain. Estes algoritmos dificultam ataques, como o "ataque de 51%", onde um agente mal-intencionado tenta controlar a maioria da rede para alterar transações.

Em conjunto, esses elementos criam um sistema robusto onde os dados são protegidos contra alterações não autorizadas, garantindo a confiança e segurança dos registos na blockchain.

1.6. Casos de Uso Atuais

A tecnologia blockchain está a ser aplicada em vários domínios, trazendo inovação e eficiência. Aqui estão alguns exemplos de como a blockchain já está a ser utilizada:

1.6.1 Criptomoedas

- **Exemplo**: Bitcoin e Ethereum são as criptomoedas mais conhecidas que utilizam a tecnologia blockchain.
- Para as criptomoedas, a blockchain atua como um livro de contas digital que regista todas as transações de forma segura e descentralizada. Cada transação é verificada por uma rede de computadores (nós) e, uma vez validada, é adicionada a um bloco que, por sua vez, é adicionado à cadeia

de blocos. Este processo garante que as transações sejam transparentes, seguras e imutáveis.

O funcionamento das criptomoedas com blockchain é um processo fascinante que combina criptografia, descentralização e consenso para permitir transações seguras e transparentes. Vamos aprofundar nos principais aspetos desse funcionamento:

Estrutura e Funcionamento

1. **Descentralização**: Ao contrário das moedas tradicionais, que são geridas por bancos centrais, as criptomoedas operam numa rede descentralizada de computadores (nós). Cada nó mantém uma cópia completa da blockchain, que é o registo de todas as transações realizadas na rede.
2. **Criptografia**: A segurança das transações é garantida através de técnicas criptográficas. Cada transação é assinada digitalmente com a chave privada do remetente, garantindo que apenas o proprietário legítimo pode autorizar a transferência de fundos.
3. **Blocos e Mineração**:
    - As transações são agrupadas em blocos. Cada bloco contém um conjunto de transações e uma referência criptográfica ao bloco anterior, formando uma cadeia.
    - A mineração é o processo pelo qual novos blocos são adicionados à blockchain. Os mineiros usam poder computacional para resolver problemas matemáticos complexos, conhecidos como "provas de trabalho". O primeiro mineiro a resolver o problema valida o bloco e é recompensado com novas unidades da criptomoeda, como bitcoins.
4. **Consenso**: O mecanismo de consenso mais comum é o Proof of Work (PoW), mas existem outros, como Proof of Stake (PoS). Estes mecanismos garantem que todos os nós da rede concordem sobre o estado atual da blockchain, evitando fraudes e duplo gasto.
5. **Imutabilidade e Transparência**: Uma vez que um bloco é adicionado à blockchain, as suas transações tornam-se imutáveis. Qualquer tentativa de alterar uma transação exigiria a revalidação de todos os blocos subsequentes, o que é computacionalmente inviável. Além disso, todas as transações são públicas e podem ser verificadas por qualquer participante da rede.

Transações com Criptomoedas

- **Iniciação**: O utilizador cria uma transação especificando o valor a ser transferido e o endereço público do destinatário.
- **Assinatura**: A transação é assinada digitalmente com a chave privada do remetente.
- **Propagação**: A transação é transmitida para a rede, onde aguarda validação.
- **Validação e Confirmação**: Os mineiros validam a transação ao incluí-la num bloco. Após a validação, a transação é considerada confirmada e é adicionada à blockchain.

Vantagens das Criptomoedas

- **Segurança**: A utilização de criptografia avançada torna as transações extremamente seguras.
- **Transparência**: Todas as transações são registadas publicamente na blockchain.
- **Descentralização**: Elimina a necessidade de intermediários, como bancos, reduzindo custos e aumentando a eficiência.
- **Acessibilidade**: Qualquer pessoa com acesso à internet pode participar na rede de criptomoedas.

A combinação destes elementos faz das criptomoedas uma inovação poderosa no mundo financeiro, oferecendo uma alternativa às moedas tradicionais e abrindo novas possibilidades para transações digitais.

1.6.2 Redes de Abastecimento

- **Exemplo**: Empresas como a IBM e a Walmart utilizam blockchain para gerir e otimizar as suas cadeias de abastecimento.
- **Como Funciona**: A blockchain permite o rastreamento de produtos ao longo de toda a cadeia de abastecimento, desde a origem até ao consumidor final. Isto assegura a autenticidade dos produtos, aumenta a transparência e reduz a possibilidade de fraudes e erros.

O uso da tecnologia blockchain nas redes de abastecimento tem o potencial de transformar significativamente a forma como as empresas gerem e monitorizam o fluxo de bens e informações.

Funcionamento da Blockchain nas Redes de Abastecimento

1. **Rastreabilidade e Transparência**:
    - Cada etapa do processo de abastecimento, desde a produção até a entrega final, pode ser registada num bloco da blockchain. Isso permite que todas as partes envolvidas tenham acesso a um registo imutável e transparente de cada transação e movimento de mercadorias.
    - A rastreabilidade é melhorada, pois cada produto pode ser seguido desde a origem até o destino final, facilitando a identificação de problemas ou ineficiências.
2. **Descentralização**:
    - A blockchain elimina a necessidade de um intermediário central para gerir os dados da cadeia de abastecimento. Todos os participantes da rede têm acesso a uma cópia atualizada da blockchain, garantindo que todos veem a mesma informação em tempo real.
3. **Imutabilidade e Segurança**:
    - Uma vez que uma transação é registada na blockchain, ela não pode ser alterada. Isso garante a integridade dos dados e reduz o risco de fraudes.
    - A segurança é reforçada pela criptografia, que protege as informações sensíveis e garante que apenas os participantes autorizados possam aceder aos dados.
4. **Contratos Inteligentes**:
    - Os contratos inteligentes são programas autoexecutáveis armazenados na blockchain que são acionados quando determinadas condições são cumpridas. Eles podem automatizar processos como pagamento e reabastecimento, reduzindo a necessidade de intervenção manual.
    - Por exemplo, um contrato inteligente pode liberar o pagamento automaticamente quando um produto é entregue e verificado.

Benefícios da Blockchain nas Redes de Abastecimento

- **Eficiência Operacional**: A redução de intermediários e a automação de processos através de contratos inteligentes podem diminuir custos e tempos de processamento.
- **Melhoria na Gestão de Inventário**: Com dados precisos e em tempo real, as empresas podem gerir melhor os seus inventários, evitando excessos ou faltas de stock.
- **Confiança e Colaboração**: A transparência da blockchain aumenta a confiança entre os parceiros da cadeia de abastecimento, incentivando uma colaboração mais estreita.

- **Redução de Riscos**: A capacidade de rastrear produtos de forma precisa ajuda a mitigar riscos associados a recalls e fraudes.
- **Sustentabilidade e Conformidade**: As empresas podem verificar e demonstrar a sustentabilidade das suas práticas ao longo da cadeia de abastecimento, garantindo a conformidade com as regulamentações e os padrões éticos.

Exemplos de Aplicação

- **Indústria Alimentar**: A blockchain pode ser usada para rastrear a origem dos alimentos, garantindo a segurança e a autenticidade dos produtos.
- **Setor Farmacêutico**: Ajuda a garantir que os medicamentos são autênticos e que foram armazenados e transportados em condições adequadas.
- **Indústria Automobilística**: Facilita a gestão de peças e componentes, assegurando que são genuínos e que cumprem os padrões de qualidade.

A implementação da blockchain nas redes de abastecimento oferece uma abordagem inovadora para enfrentar os desafios tradicionais, proporcionando maior eficiência, segurança e transparência em toda a cadeia.

1.6.3 Smart Contracts

- **Exemplo**: Plataformas como Ethereum permitem a criação e execução de smart contracts.
- **Como Funciona**: Smart contracts são contratos autoexecutáveis com os termos do acordo escritos diretamente no código. A blockchain garante que, uma vez que as condições pré-definidas sejam cumpridas, o contrato é automaticamente executado sem a necessidade de intermediários. Isto aumenta a eficiência e reduz os custos associados à execução de contratos tradicionais.

Os contratos inteligentes, ou *smart contracts*, são uma das aplicações mais inovadoras da tecnologia blockchain. Eles representam uma evolução significativa na forma como os contratos podem ser criados e executados, oferecendo uma abordagem automatizada e segura para a gestão de acordos. Vamos explorar em detalhe como funcionam e quais são os seus benefícios.

O que são Smart Contracts?

- **Definição**: Um contrato inteligente é um programa de computador que executa automaticamente ações pré-definidas quando certas condições são satisfeitas. Estes contratos são armazenados na blockchain, o que garante a sua imutabilidade e segurança.
- **Execução Automática**: Quando as condições estipuladas no contrato são cumpridas, o contrato inteligente executa automaticamente as ações

acordadas, como transferir fundos ou liberar um ativo. Isso elimina a necessidade de intervenção humana para validar ou executar o contrato.

Como Funcionam?

1. **Codificação do Contrato**:
    - Os termos do contrato são traduzidos em código de programação. Este código define as regras e penalidades do acordo, assim como as condições sob as quais o contrato será executado.
2. **Descentralização e Imutabilidade**:
    - Uma vez que o contrato inteligente é implantado na blockchain, ele não pode ser alterado. Isso garante que todas as partes envolvidas confiem que o contrato será executado exatamente como programado.
    - A blockchain oferece um registo público e distribuído, garantindo que todos os participantes têm acesso à mesma versão do contrato.
3. **Condições de Execução**:
    - Os contratos inteligentes monitorizam eventos externos ou dados fornecidos por oráculos (fontes de dados externas confiáveis) para determinar quando as condições do contrato foram atendidas.
    - Assim que as condições são verificadas, o contrato executa automaticamente as ações estipuladas, como transferir criptomoedas de uma conta para outra.

Benefícios dos Smart Contracts

- **Eficiência e Velocidade**: A automação dos processos reduz o tempo necessário para executar contratos, eliminando atrasos associados a processos manuais.
- **Redução de Custos**: Ao eliminar intermediários, como advogados ou notários, os contratos inteligentes reduzem significativamente os custos de transação.
- **Segurança**: A natureza criptografada e descentralizada da blockchain protege os contratos inteligentes contra fraudes e alterações não autorizadas.
- **Transparência e Confiança**: Todas as partes têm acesso ao contrato e às suas condições, garantindo total transparência e aumentando a confiança entre os participantes.
- **Precisão**: A eliminação de erros manuais e a execução automática garantem que os contratos são cumpridos com precisão.

Exemplos de Aplicação

- **Setor Imobiliário**: Os contratos inteligentes podem automatizar a transferência de propriedade após a verificação do pagamento, simplificando o processo de compra e venda de imóveis.
- **Seguros**: Podem automatizar pagamentos de seguros com base em eventos predefinidos, como condições meteorológicas para seguros agrícolas.
- **Cadeias de Abastecimento**: Facilitam a liberação automática de pagamentos quando mercadorias são entregues e verificadas.
- **Finanças Descentralizadas (DeFi)**: Permitem a execução de operações financeiras complexas, como empréstimos e negociações, sem a necessidade de instituições financeiras tradicionais.

Os contratos inteligentes oferecem uma forma revolucionária de gerir e executar acordos, proporcionando eficiência, segurança e transparência. À medida que a tecnologia blockchain continua a evoluir, espera-se que os contratos inteligentes desempenhem um papel cada vez mais importante em diversas indústrias.

2. Propriedade Intelectual: Desafios e Oportunidades

A cultura digital e o uso das novas tecnologias oferecem um palco de grandes dimensões, com grande facilidade de reprodução e comunicação das criações intelectuais, que se propagam no ciberespaço, continuando a necessitar de novos contornos jurídicos à escala planetária, para melhor enquadrar a titularidade e a originalidade das criações. Sendo a tecnologia uma parte integrante da vida em sociedade, que ao longo da história tem funcionado como instrumento de desenvolvimento da civilização e, como canal de expressão da cultura das sociedades, o tempo dirá se fizemos o melhor uso das novas tecnologias ou se fomos movidos por imperativos tecnológicos, substituindo os criadores humanos, e a manifestação das suas personalidades, como é a nossa tradição.

2.1. Visão Geral da Propriedade Intelectual

A propriedade intelectual stricto sensu compreende o direito de autor e os direitos conexos, bem como a propriedade industrial. A relevância de uma tutela efetiva da propriedade intelectual abrange estes dois planos, segundo a tradição do ordenamento jurídico português. No entanto, esta nomenclatura não é totalmente seguida no plano internacional. Na obra: The Charter of Fundamental Rights of the European Union: A commentary, GONÇALVES & CARVALHO (2024)[321] exploram as diferenças, observando que,

[321] GONÇALVES & CARVALHO (2024). *The Charter of Fundamental Rights of the European Union: A commentary*, Ed: Silveira; Coelho; Costa; Cabral. JusGov/ UMinho Law School. |

> "This is referred to herein in a broad sense, encompassing not only copyright and related right (intellectual property in the strict sense), but also the so-called industrial private rights (industrial property). Copyright and related or neighbouring rights aim to protect literary and artistic creations.18 Industrial private rights protect industrial creations (e.g., inventions and design), distinctive trade signs (e.g., trademarks, logos, designations of origin and geographic indications) and sui generis rights of other intangible assets (e.g., topographies of semiconductor products and traditional knowledge)". (p. 184). Os autores referem ainda que, "The reference to intellectual property (in the broad sense),22 even if it differs from the tradition in our legal system,23 corresponds to the nomenclature adopted both internationally,24 and at the Community25 level under the Anglo-Saxon influence." (p. 185)

A Comissão Europeia (2014), numa comunicação intitulada: Para um consenso renovado sobre a proteção efetiva dos direitos de propriedade intelectual: um plano de ação da UE, faz uma referência à necessária tutela efetiva da propriedade intelectual, face à relevância dos direitos de propriedade intelectual (DPI), e o seu papel no estimulo ao crescimento económico e à inovação na União Europeia.

Nessa comunicação foi apresentado um plano de ação com dez medidas para proteger esses direitos contra violações à escala comercial[322]. No mesmo documento, propõe "novas ferramentas de luta contra a contrafação, como a abordagem «follow the money» («siga o dinheiro») que visa privar os infratores que atuam à escala comercial das receitas que os atraem para tais atividades." [COM(2014) 392, p. 2]. Esta não foi a primeira iniciativa da Comissão. No Livro Verde da Comissão Europeia de 1988, dedicado ao combate à contrafação e à pirataria no mercado interno[323] destaca a importância da luta contra o problema, tendo-se

Escola de Direito da Universidade do Minho, Braga, ISBN: 978-989-35054-8-9.

[322] Comissão Europeia (2014). *Para um consenso* renovado sobre a proteção *efetiva dos direitos de propriedade intelectual: um plano de ação da UE*. COM(2014) 392, Estrasburgo, 1 de julho. https://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2014)0392_/com_com(2014)0392_pt.pdf

[323] Comissão Europeia (1988). *Livro verde o combate à contrafação e à pirataria no mercado interno*. COM(98)569 final. Bruxelas, 15 de outubro. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:51998DC0569&from=MT

dotado de "regulamentação específica para o controlo, na fronteira externa, das mercadorias de contrafacção e piratas." [COM(98)569 final. Bruxelas, p.2]. Mais tarde. A Comissão criou o Plano de Acção da Comissão a Favor do Mercado Único, e em sintonia com este, desenvolveu o Programa de Trabalho da Comissão de combate à fraude, de 1998/1999. [p.2]

Na Comunicação apresentada em 2014, a Comissão admitiu finalmente que as infrações aos DPI, "são um fenómeno insidioso e em constante mutação. Quaisquer que sejam as medidas tomadas para combater estas infrações (…), a distribuição e a venda de produtos que infringem os DPI apresentam uma rentabilidade económica tal que conservam sempre a sua atratividade. Tendo em conta a rapidez com que estas atividades podem ser desenvolvidas e exploradas, é essencial dispor de sistemas de deteção precisos e poder aplicar rapidamente medidas de prevenção." (p. 3)

Em 2024, a Comissão emitiu uma Recomendação sobre as medidas para combater a contrafação e melhorar o respeito dos direitos de propriedade intelectual[324] na qual destaca que o valor alcançado dos produtos protegidos por PI, atrai as redes criminosas, resultando num aumento das mercadorias de contrafação e da pirataria. Refere ainda, que A Estratégia da UE para Lutar contra a Criminalidade Organizada, visa desmantelar essas redes e os seus modelos de negócio. A Comissão enfatizou que o impacto da prática do crime de contrafação, conduz a perdas de receitas para os titulares de direitos de propriedade intelectual («titulares de direitos»), e riscos a saúde pública, ambiente e segurança dos consumidores.[325]

2.2. Problemas no Registo e Proteção

Após uma apresentação dos principais tipos de PI, que inclui quer os direitos de autor e direitos conexos, quer os direitos industriais (patentes, marcas, direitos de autor, designs industriais), pretendemos explorar os problemas atuais com o sistema tradicional de registo, como a falta de um registo universal, a fragmentação jurisdicional e os elevados custos.

2.3. Oportunidades com Blockchain

Discutir as principais oportunidades oferecidas pela blockchain para resolver os desafios existentes, como a criação de um registo global, transparente e acessível.

[324] Comissão Europeia (2024). Recomendação da Comissão relativa a medidas para combater a contrafação e melhorar o respeito dos direitos de propriedade intelectual C(2024) 1739 final, Bruxelas, 19 de março. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=PI_COM:C(2024)1739

[325] Cons. 2 C(2024) 1739 final]

3. Proposta de Modelo Baseado em Blockchain para a Propriedade Intelectual

3.1. Registo Descentralizado de Propriedade Intelectual

Explicar como um sistema de registo descentralizado baseado em blockchain pode funcionar.
Utilização de timestamps e chaves criptográficas para registar a autoria e a criação de obras de forma imutável e verificável globalmente.

3.2. Licenciamento Automatizado com Smart Contracts

Propor o uso de contratos inteligentes para automatizar o licenciamento de obras e a gestão de royalties, explicando como estas transações seriam transparentes e seguras.
Explicar o papel dos smart contracts na transferência de direitos e gestão de PI.

3.3. Verificação de Autenticidade e Combate à Falsificação

Discutir como a blockchain pode ser usada para verificar a autenticidade de marcas, patentes e direitos de autor em tempo real.
Utilização da blockchain para rastrear a cadeia de produção e distribuição de produtos protegidos por PI, ajudando a combater a falsificação.

4. Benefícios e Implicações do Modelo

4.1. Transparência e Imutabilidade

Explicar como a natureza imutável da blockchain garante um registo inviolável, acessível a qualquer pessoa em qualquer parte do mundo.

4.2. Custos Reduzidos e Acessibilidade Global

Abordar como a blockchain pode reduzir significativamente os custos associados ao registo e proteção de PI, especialmente para criadores e empresas em mercados emergentes.

4.3. Descentralização e Confiança

Discutir como a descentralização elimina a necessidade de intermediários, confiando os registos diretamente à rede distribuída, removendo dependências de organismos nacionais.

5. Desafios e Considerações para a Implementação

5.1. Regulação e Harmonização Legal

Discutir as possíveis barreiras legais e regulatórias, como a necessidade de harmonizar as leis de PI globalmente para que um sistema baseado em blockchain possa ser reconhecido.

5.2. Escalabilidade e Performance

Abordar os desafios técnicos, como a escalabilidade da blockchain para lidar com volumes massivos de registos de PI.

5.3. Adoção Global

Discutir os desafios para garantir que o sistema seja amplamente adotado por criadores, empresas e governos em todo o mundo.

6. Estudo de Caso

6.1. Simulação de Registo Global de Propriedade Intelectual

Apresentar um exemplo ou estudo de caso fictício para ilustrar como o sistema proposto funcionaria na prática, desde o registo de uma patente até à gestão dos direitos e licenciamento através de *smart contracts*.

6.2. Análise de Impacto

Discutir os possíveis impactos positivos num cenário real, como a proteção de criadores em países em desenvolvimento ou a redução da burocracia para grandes empresas.

7. Notas finais

Uma nota final, mas não conclusiva, para expressar a relevância do projeto de investigação num momento em que se tornou necessário o recurso às tecnologias para proteger os direitos de propriedade intelectual. De forma galopante o normativismo cede perante a tecnologia e nessa medida falamos de inteligência artificial (IA) e em particular, "da Infraestrutura Europeia de Cadeia de Blocos no Setor dos Serviços", apresentados na Recomendação de 2024. Aí se realça "como os sistemas automatizados de reconhecimento de conteúdos e os algoritmos de aprendizagem automática, podem ser utilizados para reconhecer produtos piratas ou de contrafação ou padrões associados à promoção ou distribuição de tais produtos e têm potencial para se tornarem tecnologias essenciais na luta contra atividades que infringem a PI."[326]. Vimos que a blockchain é uma tecnologia robusta e segura que possibilita a criação de registos digitais confiáveis e transparentes, com aplicações que vão além das criptomoedas, abrangendo áreas como contratos inteligentes, cadeias de abstecimento, gestão de identidade e a Propriedade Intelectual.

[326] C(2024)1739 final, considerando 33.

O projeto que agora se inicia, acompanha a Recomendação da Comissão de 2024, a qual aborda o Autenticador Europeu de Produtos e Serviços de Logística (EBSI-ELSA) do EUIPO, com recurso ao blockchain (cadeia de blocos), apresentado como um programa-piloto para um sistema baseado numa cadeia de blocos que interligaria todas as partes interessadas e os seus sistemas, a fim de garantir a autenticidade do produto ao longo de toda a cadeia de abastecimento e, eventualmente, mais além. Quando as mercadorias estão ligadas à infraestrutura Blockathon, é criado um gémeo digital, que armazena as informações que comprovam a sua autenticidade. Assim, proporciona-se às partes interessadas os meios para transferir uma mercadoria juntamente com o seu equivalente virtual, sendo a este último aposta uma assinatura digital imutável do proprietário da marca. O sistema prevê igualmente a possibilidade de partilhar informações digitais com as partes envolvidas na cadeia logística, incluindo intermediários e autoridades competentes.

Referências

BODO, Bala; GERVAIS, Daniel; QUINTAIS, J. Pedro (2018). **Blockchain and smart contracts: the missing link in copyright licensing?** International Journal of Law and Information Technology, 2018, 26, 311–336 doi: 10.1093/ijlit/eay014.

CASINOA, Fran; DASAKLISB, Thomas K.; PATSAKISA; Constantinos (2019). **A systematic literature review of blockchain-based applications: Current status, classification and open issues.** Telematics and Informatics Volume 36, March 2019, Pages 55-81. Telematics and Informatics | Journal | ScienceDirect.com by Elsevier

GAO, Qiqi; ZHANG, Jiteng (2024) **Artificial Intelligence and the Rule of Law** *in* Artificial Intelligence Governance and the Blockchain Revolution. Institute of Political Science East China University of Political Science Shanghai, China. Ed. Springer. ISBN 978-981-99-9211-9 (eBook) https://doi.org/10.1007/978-981-99-9211-9

HU, Jian; ZHU, Peng; QI, Yong (2022). **A patent registration and trading system based on blockchain.** Volume 201, 1 September 2022, 117094. https://doi.org/10.1016/j.eswa.2022.117094

KHARE et *al*. (2023). **Aryan Artificial Intelligence and Blockchain for Copyright Infringement Detection**. Proceedings of the Second International Conference on Edge Computing and Applications (ICECAA 2023) IEEE Xplore Part Number: CFP23BV8-ART; ISBN: 979-8-3503-4757-9979-8-3503-4757-9 ©2023 IEEE 496 Authorized licensed use limited to: b-on: Universidade Aberta.

KSHETRI, Nir (2018). **Blockchain's roles in meeting key supply chain management objectives, International** Journal of Information Management 39 (2018), 80-89 International Journal of Information Management | ScienceDirect.com by Elsevier

LUO, Liya (2022). **Application of Blockchain Technology in Intellectual Property Protection**. Hindawi Mathematical Problems in Engineering Volume 2022, Article ID 4641559, 12 pages https://doi.org/10.1155/2022/4641559

XIE. Renqiang; TANG, Min (2024). **A digital resource copyright protection scheme based on blockchain cross-chain technology,** Helyion 10 (2024) e 36830 www.cell.com/heliyo

Dados pessoais – "o petróleo do século XXI" – os desafios e as ameaças à luz do cibercrime

Ana Felícia Canilo Santos [327]

Resumo

À medida que as nossas vidas vão estando cada vez mais *online*, à medida que o digital toma poder, com a diminuição do uso dos documentos tradicionais em papel, é compreensível que também os riscos a tal exposição *online*, se imiscuam nos nossos direitos, tradicionalmente consagrados, se assim pudermos chamar.

O grande desafio do Direito será o de perceber como regulamentar e legislar estas alterações. O desafio dos cidadãos será o de transpor a sua vida para o mundo *online*, conseguindo manter intactos os seus direitos.

O tema que aqui nos propomos tratar é, no nosso entender, um tema bastante atual e ambicioso, na medida em que tudo quanto se escreva sobre o mesmo, estará sempre um passo atrás do desenvolvimento das novas tecnologias. Este nosso tema não pretende ser uma análise exaustiva de tudo quanto foi feito, mas sim, fazer uma análise breve, focando nos aspetos principais do que se passou e do que nos levou ao que atualmente vivemos e, por fim, em jeito de conclusão, fazer um pequeno levantamento do que pensamos que seja o futuro do *Cibercrime*, sem esquecer a temática dos *dados pessoais* e como estes têm vindo a consubstanciar uma nova forma de crime.

Palavras-chave: *Dados pessoais; dados sensíveis; cibercrime; criminalidade informática; Hackers.*

[327] Magistrada, Docente da Universidade Europeia e Investigadora do Privacy and Data Protection Centre.

Abstract
As our lives become more and more online and the digital world takes control, with the decrease in the use of traditional paper documents it is understandable that the risks of such online exposure interfere with our traditionally consecrated rights, if we may refer to them like that.
The challenge of Law will be to understand how to regulate and legislate these alterations.The citizens´ challenge will be to transfer their lives to the online world, while managing to keep their rights intact.
The topic we intend to deal here is a very current–and ambitious topic as far as everything written about it will always be one step behind the development of modern technologies. With this work, we do not intend to make an exhaustive analysis of everything that has been done, but rather to make a brief study focusing on the main aspects of what happened and what led us to what we are currently experiencing and, finally, to conclude, make a small survey of what we think is the future of *Cybercrime*, without forgetting the issue of *personal data* and how these have been creating a new form of crime.

Keywords: *Personal data; Sensitive data; Cybercrime; Computer crime; Hackers.*

Lista de Abreviaturas e Acrónimos

Ac.	Acórdão
App.	Application
apud.	Expressão que significa "com", "junto a", "em"
ARPANET	Advanced Research Projects Agency Network
Art.º	Artigo
CD-R	Compact Disk Recordable
CEDH	Convenção Europeia dos Direitos do Homem
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team European Union
cfr.	conforme
CNCSeg	Centro Nacional de Cibersegurança
CNI	Centro Nacional de Inteligência
CNPD	Comissão Nacional de Proteção de Dados Pessoais
COM	Component Object Model
CP	Código Penal Português
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial-of-Service
DGAJ	Direção Geral da Administração da Justiça
DL	Decreto-Lei
DMZ	Demilitarized zone (computing) ou perimeter network
DNS	Domain Naims (Nome de domínio)
DoS	Denial-of-Service
DQ	Decisão-Quadro
DR	Diário da República
DUDH	Declaração Universal dos Direitos do Homem
EBF	The European Banking Federation
EC3	European Cybercrime Center
ed.	edição
EFMS	Fórum Europeu dos Estados Membros
EM	Estados Membros
ENISA	Agência Europeia para a Segurança das Redes e da Informação
ENSI	Estratégia Nacional de Segurança da Informação
EUA	Estados Unidos da América
FTP File	Transfer Protocol
FTTP	Fiber To The Premises
GNS	Gabinete Nacional de Segurança
GPS	Global Positioning System
IAB	Internet Architecture Board

Ibidem	"no mesmo trabalho que o anterior, mesma página"
ICI	Infraestruturas Críticas da Informação
ICT	Information and communications technology
Idem	"mesmo autor"
IDPCC	Instituto de Direito Penal e Ciências Criminais
IDS	Intrusion Detection System
IGF	Internet Governance Forum
I.J.C.	Instituto Jurídico da Comunicação
IP	Internet Protocol
IRIS	Internet Routing in Space
ISOC	Internet Society
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
HIV	Human Immunodeficiency Virus
J-CAT	Joint Cybercrime Action Taskforce
JIC	Juiz de Instrução Criminal
JOCE	Jornal Oficial das Comunidades Europeias
JOUE	Jornal Oficial da União Europeia LC Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro)
LCE	Lei do Comércio Eletrónico (Decreto-Lei n. º7/2004, de 7 de janeiro)
LCI	Lei da Criminalidade Informática (Lei n. º109/1991, de 17 de agosto – revogada)
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales
LPDP	Lei de Proteção de Dados Pessoais (Lei n. º67/98, de 26 de outubro)
LPDPI	Lei de Proteção de Dados Pessoais face à Informática
LPDPT	Lei de Proteção de Dados Pessoais nas Telecomunicações (Lei n. º41/2004, de 18 de agosto)
MP	Ministério Público
n.º	número
NCA	National Crime Agency
NCSD	National Cyber Security Division
op. cit.	Opere citato (mesma obra, página diferente)
OPC	Órgão de Polícia Criminal
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte,
OSCE	Organization for Security and Co-operation in Europe
p.	página
PCSD	Política Comum de Segurança e Defesa
PGDL	Procuradoria-Geral Distrital de Lisboa
PJ	Polícia Judiciária
pp.	páginas

RATs	Remote Access Trojans
ref.	referência
RGPD	Regulamento Geral de Proteção de Dados
SCEE	Sistema de Certificação Eletrónica do Estado
SEA	Syrian Electronic Army
SI	Sistemas de Informação
SIGINT	Sistema de Espionagem Electrónica
SMS	Short Message Service (vulgo mensagens escritas)
SPCI	International Conference on Security, Privacy and Confidentiality Issues in Cyberlaw
SRI	Segurança das Redes e da Informação
ss.	seguintes
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFUE	Tratado sobre o Funcionamento da União Europeia
TIC	Tecnologias da Informação e das Comunicações
TJCE	Tribunal de Justiça das Comunidades Europeias
TUE	Tratado sobre a União Europeia
UE	União Europeia
UNODC	United Nations Office on Drugs and Crime
UNSC	United Nations Security Council
URL	Uniform Resource Locator
USB	Universal Serial Bus
US-CERT	United States - Computer Emergency Readiness Team
v.	ver
VIH	Vírus da Imunodeficiência Humana
vol.	volume
WAAR	Web Application Attack Report
WWW	World Wide Web

Introdução

Com este nosso trabalho, propomo-nos analisar a temática dos *dados pessoais*, vistos à luz do mundo atual e digital em que vivemos. Cada vez mais ouvimos falar de *dados pessoais*, da sua proteção e do valor que estes têm e vão ganhando enquanto moeda de troca, mas será que os cidadãos ditos "comuns" (i.e., leigos em Direito ou sem o conhecimento da matéria em causa), sabem o que está, realmente, em causa? Será que já ouviram falar do RGPD e sabem o que significa? Será que sabem como atuar quando alguém lhes pede uma cópia do Cartão de Cidadão e o que esse simples gesto pode proporcionar à parte que o solicitou e que agora o tem na sua posse? E se passarmos estes gestos do quotidiano, como ir a uma repartição de Finanças, para o mundo digital? O que sucede se uma pessoa consegue aceder à nossa conta das Finanças? E à nossa conta da Segurança Social? E o que acontece se alguém acede às nossas informações médicas e nelas consta uma doença, como HIV (ou VIH, vulgo SIDA)? Escusado será mencionar os perigos de um terceiro aceder à nossa conta bancária e o que isso implicaria.

Mas, recuperando a nossa pergunta inicial, saberá um cidadão comum a importância de proteger os seus dados pessoais, como protege a sua casa ou a sua vida, por exemplo? É esta a análise que aqui nos propomos fazer. Uma análise dos dados pessoais, fazendo uma breve resenha evolutiva até aos dias de hoje; a passagem destes para o mundo tecnológico e os tipos de crimes que a estes instigam e tentar perceber o seu valor de mercado. Por fim, e após aferirmos o valor de mercado dos nossos *dados pessoais*, tentaremos aclarar o título por nós proposto, e perceber se os dados pessoais são ou não "o petróleo do século XXI".

Capítulo I – Dados Pessoais

1.1. Breve evolução histórica

Importa começar este trabalho por fazer uma breve introdução histórica ao *Direito à proteção de Dados Pessoais* e de como estes foram sendo consagrados até aos dias de hoje. Esta breve evolução vai-nos permitir compreender melhor, por um lado, o nível de importância que foi sendo atribuída aos *dados pessoais* e a consagração destes como Direito Fundamental e, por outro, a necessidade que o legislador teve de criar mecanismos de proteção dos mesmos.

Os *dados pessoais* sempre estiveram consagrados, ainda que de forma subjetiva, na Legislação Europeia, o que desde sempre demonstrou a preocupação do legislador sobre esta matéria: "A proteção dos dados pessoais e o respeito pela vida privada são direitos fundamentais europeus. O Parlamento Europeu sempre insistiu na necessidade de alcançar um equilíbrio entre a melhoria da segurança e a preservação dos direitos humanos, incluindo a privacidade e a proteção de dados."[328]

Ainda que de forma subjetiva, diríamos que a primeira vez que se abordou este tema, foi em 1950 na *Convenção Europeia para a Proteção dos Direitos do*

[328] PROTEÇÃO dos Dados Pessoais, do Parlamento Europeu. [Em linha]. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf P. 1. (consult.1 fev.2023).

Homem e das Liberdades Fundamentais (CEDH), de 4 de novembro de 1950, ao consagrar-se o *direito ao respeito pela vida privada e familiar*, conforme se pode ler no seu artigo 8.º: "Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pela sua correspondência.".[329] O ponto fundamental aqui seria a sua correspondência e tudo o que a esta está implícito, mas também o seu domicílio, nomeadamente, morada, nome próprio e nomes dos seus familiares**,** ou pessoas que coabitam naquela mesma residência.

De forma oficiosa, somente em 28 de janeiro de 1981, através da *Convenção 108 do Conselho da Europa, para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais*, foi criado o primeiro instrumento internacional juridicamente vinculativo, adotado no domínio da *proteção de dados*. Este visava "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".[330]

Alguns anos mais tarde, em 2009, encontramos no TFUE, no seu art.º 16.º, a consagração de mais uma referência importante para os *dados pessoais*, ao consagrar no seu n.º 1 que: "Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.".

A *Carta dos Direitos Fundamentais da União Europeia (CDFUE)*, de 7 de junho de 2016, consagra, igualmente, o *Direito à Proteção de dados pessoais*, no seu art.º 8.º, onde o n. º1 mantém a descrição já consagrada no art.º 16.º do TFUE. Já o n.º 2, do art.º 8.º da CDFUE, vai mais além e é mais abrangente naquilo que o legislador pretende defender, nomeadamente, ao definir de que forma os dados recolhidos devem ser tratados e ainda, quais os direitos que são garantidos aos proprietários desses dados: "2. Esses dados 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.".[331]

Em maio de 2018, entraram em vigor novas regras da UE no que dizia respeito à proteção de dados e que vieram reforçar os direitos dos cidadãos, bem como simplificar as regras para as empresas na era digital. O Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que revogou a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), de maio de 2018, veio reforçar a proteção das pessoas singulares no que diz respeito ao tratamento de *dados pessoais* e à livre circulação desses dados. A implementação destas regras

---

[329] Os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia reconhecem o respeito pela vida privada e a proteção dos dados pessoais como direitos fundamentais estreitamente relacionados, mas distintos. *Idem*, p. 2.

[330] *Idem, ibidem.*

[331] [Em linha]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR (consult.1 fev.2023).

visava, e visa atualmente, proteger todos os cidadãos da UE contra as eventuais violações da sua privacidade e dos seus dados, num mundo cada vez mais baseado na partilha e recolha destes, criando simultaneamente um quadro mais claro e mais coerente para as empresas, no que diz respeito à recolha, tratamento e conservação dos dados.[332]

Dos direitos que este Regulamento garante aos cidadãos, destacamos:

- O consentimento claro e positivo do tratamento dos seus dados e o direito de receber informações claras e compreensíveis sobre o mesmo (seja em formato papel, seja nos casos *online*, igualmente com a aceitação expressa do utilizador);
- O direito a ser esquecido (um cidadão pode solicitar que os seus dados sejam apagados de vez);
- O direito a transferir os dados para outro prestador de serviços (por exemplo, ao fazer a mudança de uma operadora de telecomunicação para outra – a chamada portabilidade, através do envio do CVP, código de validação de portabilidade – é possível que haja uma transferência dos dados do consumidor entre ambas, com o consentimento expresso deste);
- O direito de saber se os seus dados foram pirateados.[333]

Estas novas regras aplicam-se, quer às empresas que operam dentro da UE, bem como as que tenham sede fora dela. Para além disso, estas novas regras apresentam uma vertente sancionatória, já que permitem impor medidas corretivas, tais como advertências e ordens, ou coimas às empresas que violem as referidas regras.[334]

Encontramos, ainda em vigor, os seguintes diplomas legais no âmbito da proteção de dados, na UE:

- Diretiva sobre a proteção de dados na aplicação da lei – *a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho*, de 27 de abril de 2016, "relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho".[335] De uma forma resumida, esta Diretiva protege o direito fundamental dos cidadãos à proteção dos seus

[332] De acordo com a investigação realizada para o Parlamento Europeu, a legislação da UE relacionada com a regulamentação dos fluxos de dados contribui anualmente com 51,6 mil milhões de euros para o PIB da União Europeia. PROTEÇÃO dos Dados Pessoais, do Parlamento Europeu. [Em linha]. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf P. 1. (consult.1 fev.2023).

[333] PROTEÇÃO dos Dados Pessoais, do Parlamento Europeu. [Em linha]. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf pp. 2, 3. (consult.1 fev.2023).

[334] *Idem*, p.3 (consult.1 fev.2023).

[335] DIRETIVA (UE) 2016/680 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016. **Jornal Oficial da União Europeia**. [Em linha]. (4.5.2016). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=HR (consult.1 fev.2023).

dados, quando estes forem utilizados pelas autoridades responsáveis pela aplicação da Lei, ao garantir que os *dados pessoais* das vítimas, testemunhas e suspeitos de crimes sejam devidamente protegidos, bem como facilitar a cooperação transfronteiriça na luta contra a criminalidade e o terrorismo.[336]

- A Diretiva relativa à privacidade e às comunicações eletrónicas - *A Diretiva 2002/58/CE do Parlamento Europeu e do Conselho*, de 12 de julho de 2002, relativa ao tratamento de *dados pessoais* e à proteção da privacidade no setor das comunicações eletrónicas, foi alterada pela Diretiva 2009/136/CE, de 25 de novembro de 2009.[337] Esta Diretiva levanta uma questão delicada e amplamente discutida, levada por diversas vezes ao TJUE, tendo sido alvo de uma série de acórdãos[338] sobre a conservação dos dados que determinaram que o Direito da UE obsta à conservação geral e indiscriminada dos dados de tráfego e de localização.[339]
- O Regulamento da UE, relativo ao tratamento de *dados pessoais* por organismos e órgãos da União, nomeadamente O *Regulamento n.º 2018/1725 do Parlamento Europeu e do Conselho*, de 23 de outubro de 2018, relativo à proteção das pessoas singulares, no que diz respeito ao tratamento de *dados pessoais* pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE.[340]

---

[336] Desde 6 de maio de 2022 que se aguarda pelo relatório da Comissão Europeia ao Parlamento Europeu e ao Conselho sobre a avaliação e revisão desta diretiva. PROTEÇÃO dos Dados Pessoais, do Parlamento Europeu. [Em linha]. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf p. 3. (consult.1 fev.2023).

[337] *Idem, ibidem.*

[338] A este respeito e a título de exemplo, destacamos os seguintes casos: - ACÓRDÃO do Tribunal de Justiça nos processos apensos C-793/19 | SpaceNet e C-794/19 | Telekom, Deutschland. COMUNICADO DE IMPRENSA 156/22. Luxemburgo. [Em linha]. (20.9.2022). Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220156pt.pdf (consult.1 fev.2023). E ainda o Processo C-518/07: Acórdão do Tribunal de Justiça (Grande Secção) de 9 de março de 2010 — Comissão Europeia/República Federal da Alemanha (Incumprimento de Estado — Diretiva 95/46/CE — Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados — Artigo 28º, nº 1 — Autoridades nacionais de controlo — Independência — Tutela administrativa exercida sobre essas autoridades). [Em linha]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62007CA0518&qid=1680022484676&from=PT (consult.1 fev.2023).

[339] PROTEÇÃO dos Dados Pessoais, do Parlamento Europeu. [Em linha]. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf , p. 3. (consult.1 fev.2023).

[340] Chamamos a atenção para o nº 2 do artº 101.º deste Regulamento, onde refere que uma exceção à entrada em vigor: "2. No entanto, o presente regulamento é aplicável ao tratamento de dados pessoais pela Eurojust, a partir de 12 de dezembro de 2019." REGULAMENTO (UE) 2018/1725 DO PARLAMENTO EUROPEU E DO CONSELHO, de 23 de outubro de 2018. **Jornal Oficial da União Europeia** [em linha]. (21.11.2018). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R1725&from=PT (consult.1 fev.2023).

1.2. Conceito de *Dados Pessoais*

Depois de analisada a evolução histórica dos *dados pessoais*, importa aferir o que se entende por *dado pessoal* e de que forma este conceito é enquadrado atualmente, quer na nossa esfera jurídica, quer perceber também se existem diferenças nos conceitos ou nas definições que foram transpostas para os ordenamentos jurídicos dos nossos países vizinhos. Por outro lado, importa esclarecer o que não são considerados *dados pessoais*.

Quanto à definição de *dados pessoais*, encontramos no n.º 1 do art.º 4.º do RGPD: "«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados») ;(…)".[341]

Embora similar a este conceito, a definição que cada um dos Países adota, depois, para a sua esfera jurídica interna contempla algumas diferenças, que consideramos curiosas e pertinentes. Vejamos as diferenças que surgem entre a nossa definição de *dado pessoal* e as definições que vigoram, respetivamente, em Espanha e em França, por se tratar de Países que se situam mais próximos de nós. Enquanto na nossa definição surge a informação "relativa a (…)"; no caso Espanhol surge a palavra "sobre": "«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); (…)"[342] e no caso Francês fala-se de informação "referente" ("rapportant"), "1) «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»)[343]. Igualmente nos três conceitos, ao titular desses *dados* é--lhe concedida uma denominação distinta: no caso Português é chamado de "titular dos dados", no caso Espanhol é "el interesado" e no caso Francês de "personne physique identifiable". Curiosamente, apenas no nosso caso se denomina, claramente, como titular dos *dados pessoais*. O termo Espanhol parece-nos ser o mais "perigoso" dos três conceitos e o menos correto de se empregar, já que a denominação de "pessoa interessada" poderá dar azo a más interpretações e a más aplicações, na medida em que nem sempre a pessoa interessada é a titular dos *dados*, assim como nem sempre poderá ter em mente o melhor intuito quanto ao uso desses *dados*, por exemplo no acesso ilegítimo aos mesmos. Por outro lado, imagine-se no caso de uma empresa ou da Administração Pública que, graças à definição contida no RGPD Espanhol, pode alegar um interesse legítimo ou público, respetivamente, para utilizar os *dados pessoais* sem necessidade do consentimento do titular.[344]

---

[341] REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que revoga a Diretiva 95/46/CE (RGPD). **Jornal Oficial da União Europeia**. p. 33. [Em linha]. (4.5.2016). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679 (consult. 3 fev.2023).

[342] REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 201 (RGPD), pág. 33 **Diario Oficial de la Unión Europea**. [Em linha]. (4.5.2016). Disponível em: https://www.boe.es/doue/2016/119/L00001-00088.pdf (consult. 3 fev.2023).

[343] RÈGLEMENT (UE) 2016/679 du Parlement Européen et du **C**onseil, du 27 avril 2016, pág. 33. **Journal Officiel de l'Union Européenne**. [Em linha]. (4.5.2016). Disponível em: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=PT (consult. 3fev.2023).

[344] A este respeito v. "**El ciudado ante el RGPD y la nueva LOPDGDD**" *in* CALVO, José López,

Ao conceito de *dado pessoal* e aquilo que segundo este se considera ser uma pessoa identificável, acrescenta ainda o nosso RGPD: "é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;".

De uma forma geral, são considerados *dados pessoais*, aqueles que comummente fornecemos quando nos queremos identificar junto de alguma Entidade ou Organismo, tais como o nosso nome, o número de Cartão de Cidadão, o número de Contribuinte, o número da Segurança Social, a data e o local de nascimento, a filiação, mas também, os nossos dados de localização, ou informações fornecidas através da utilização do nosso Cartão de Crédito (por exemplo, locais onde efetuamos compras, reservas em hotéis, etc.).

Agora que já analisámos o que são *dados pessoais* segundo o RGPD, torna-se mais fácil perceber quais aqueles que o não são. Assim, e por exclusão de partes do exposto no n.º 1 do art.º 4.º, não são considerados *dados pessoais* (e por isso não estão protegidos) todos os dados que não se podem associar a uma determinada pessoa, porque não está identificada, nem pode ser identificável.

Quanto aos *dados sensíveis*, e por entendermos que estes merecem um tratamento especial, abordaremos a sua definição e exemplos no ponto seguinte.

1.3. Conceito de *Dados Sensíveis*

Depois de no ponto anterior termos analisado o conceito de *dados pessoais* e percebermos o que não se insere nessa definição, à luz do RGPD, importa agora debruçarmos-mos sobre os *dados sensíveis*.

Entendeu o legislador (e no nosso entender, fê-lo muito bem), separar a definição de *dados pessoais*, da definição de *dados sensíveis*. Isto porque a mistura destes dois conceitos ou, melhor dizendo, a ausência de uma separação clara entre ambos, daria azo a que todos os *dados* fossem recolhidos, tratados e consagrados da mesma forma e, como iremos ver, a estes (*dados sensíveis*) é-lhes pedida uma especial atenção, já que se referem a questões pessoais e privadas do foro de cada um de nós, que não devem fazer parte do conhecimento público, ou não devem ser solicitadas, pois não identificam e não caraterizam os seus autores e, quando solicitados, podem levar à marginalização dos mesmos. Como refere a Dra. Cristina Caldeira: "Os dados sensíveis merecem uma proteção específica, já que o seu tratamento pode implicar riscos significativos para o direito à reserva da vida privada, com impacto eventual nos direitos e liberdades fundamentais.".[345]

Mas, afinal, o que são *dados sensíveis*?

La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD. pág. 846. febrero 2019. Wolters Kluweer. BOSCH. ISBN: 978-84-9090-345-2

[345] CALDEIRA, Cristina M. G. *in* aula da 7.ª Edição da Pós-Graduação em Proteção de Dados Pessoais, Privacidade e Cibersegurança na EU, (18.10.2022).

Nos termos do RGPD, não existe uma definição concreta de *dados sensíveis* como sucede no caso dos *dados pessoais*. Não obstante, podemos extrair da lista de *dados* presente no n.º 1, do art.º 9.º do RGPD, que pelas suas características especificas, estão proibidos de ser solicitados e chegamos, assim, à uma definição daquilo que o legislador pretendeu salvaguardar como tratando-se de *dados sensíveis*: "1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.".[346]Assim, os seguintes *dados* pessoais são considerados *sensíveis* e estão sujeitos a condições de tratamento específicas:

- *dados* pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas;
- filiação sindical;
- *dados* genéticos, *dados* biométricos tratados simplesmente para identificar um ser humano;
- *dados* relacionados com a saúde;
- *dados* relativos à vida sexual ou orientação sexual da pessoa.[347]

O art.º 9.º contempla, ainda, algumas exceções à solicitação destes *dados*. Estas exceções encontram-se previstas nos números 2, 3 e 4 do referido artigo. Nas alíneas de a) a f) do art.º 6.º (licitude do tratamento), estão previstos igualmente os casos em que, excecionalmente, é lícito o tratamento dos *dados sensíveis*: "1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações".[348]

Capítulo II – Cibercrime

2.1. Breve enquadramento

Antes de passarmos à análise dos utilizadores e dos agentes deste tipo de crime importa, antes de mais, fazer um breve enquadramento sobre a sua definição e características mais importantes.

O *Cibercrime* é o nome genérico pelo qual ficaram conhecidos os crimes informáticos, nomeadamente, os crimes que são perpetrados com recurso ou por intermédio de tecnologias da informação, processamento e comunicação e que ocorrem também no mundo digital, no chamado *Ciberespaço*.

---

[346] REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que revoga a Diretiva 95/46/CE (RGPD). Jornal Oficial da União Europeia. Pág. 38. [Em linha]. (4.5.2016). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679 (consult. 11 fev.2023).

[347] REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que revoga a Diretiva 95/46/CE (RGPD). Jornal Oficial da União Europeia. Pág. 38. [Em linha]. (4.5.2016). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679 (consult. 11 fev.2023).

[348] *Idem,* pág. 36.

Em Portugal, a competência quanto ao *Cibercrime* está dividida entre a Polícia Judiciária e o Ministério Público, sendo este último quem tem competência para decidir. No entanto, também temos casos em que o Órgão de Polícia Criminal e o Juiz de Instrução Criminal podem intervir nos casos mais graves, como por exemplo, escutas telefónicas.

Quanto à Cibercriminalidade, pode ser definida como um vasto conjunto de atividades criminosas que são perpetradas e ocorrem nos meios digitais. No conjunto de crimes que compõem a Cibercriminalidade, encontramos as infrações tradicionais (como a fraude, a falsificação e o roubo de identidade); as infrações relativas aos conteúdos (entre outras, a distribuição de material pedo pornográfico em linha ou o incitamento ao ódio racial) e, por fim, crimes respeitantes exclusivamente a computadores (por exemplo, ataques contra os sistemas informáticos, recusa de serviço e *software* malicioso).

Enquadrados que estão estes dois conceitos, é altura de definirmos os utilizadores e os agentes que encontramos no *Ciberespaço*.

2.2. Utilizadores

Para que possamos compreender os meandros das redes de informação e bem assim, da Internet, precisamos de, primeiro que tudo, definir e descrever os *utilizadores*. Os *utilizadores* somos todos nós, são as pessoas singulares que compõem a sociedade.

O problema que aqui se coloca é quando referimos que *utilizadores* somos todos. Nesse amplo leque de pessoas encontram-se, também, pessoas que, pelas suas características, estão suscetíveis a sofrer mais com estes ataques, na maioria das vezes, sem se aperceberem disso. Falamos aqui das crianças e jovens (para este último conceito iremos considerar os menores de 18 anos).

No primeiro caso, falamos de pessoas que, pela sua idade e imaturidade, não compreendem os riscos que uma atividade na Internet se lhes apresenta. Não obstante, assistimos a um abismal aumento de crianças em idades muito pequenas já com acesso a telemóveis, tablet, computadores, acesso esse facilitado pelos seus responsáveis: progenitores, avós, tios, família mais próxima, como forma de os manter ocupados e quietos durante largas horas, muitas vezes sem qualquer supervisão. Os menores merecem, assim, uma proteção específica no que diz respeito aos seus *dados pessoais*, em particular no que diz respeito ao uso dos seus *dados* para fins comerciais, ou de criação de perfis de usuários. Este ponto leva-nos a uma questão importante que é a da responsabilidade. Quem será o responsável pelas atitudes dos mais novos e pelo fornecimento e partilha dos *dados* que estes possam divulgar, ainda que inconscientemente? Diríamos que, em primeira instância, essa responsabilidade recai nos Pais, ou nos responsáveis legais dos menores já que, como o próprio nome indica, a estes compete a salvaguarda dos interesses dos menores. Assim, é necessária uma especial atenção dos responsáveis pelos menores e que

haja da parte destes um conhecimento ou interesse em saber por onde "navegam" os menores quando utilizam a Internet. Destacamos, por exemplo: ter conhecimento das políticas de *cookies* dos *sítios* informáticos que visualizam, das políticas de privacidade, saber que *dados* são recolhidos, com que intuito ou com que finalidade, ativar sempre que possível o controlo de parentalidade, de forma a permitir que o conteúdo apresentado seja adequado ao menor, etc.; mas perceber, também, um pouco da Legislação em vigor, legislação esta que, precisamente para facilitar o entendimento não só dos Pais, mas de todos, deve ser o mais clara e concisa possível.

Não nos podemos esquecer que a maioria dos *sítios* informáticos estão alojados noutros países, e que, ao consentir na recolha e tratamento dos nossos *dados*, estamos a consentir igualmente no envio desses *dados* para outros países. Neste contexto, deve ter-se devidamente em conta o Regulamento relativo a um mercado único de serviços digitais e as previsões específicas do RGPD.

Como refere a Dra. Graça Canto Moniz, "em larga medida, a legislação sobre proteção de dados pessoais parte de um pressuposto geral: a posição de vulnerabilidade e de desvantagem estrutural das pessoas singulares numa sociedade marcada pela circulação de fluxos informacionais, de várias origens, com vários destinos e finalidades." [349]

No caso dos jovens, a situação é a mesma. No entanto, a presença *online* é muito mais vasta que os primeiros, fomentada pelas diversas aplicações, redes sociais e plataformas *online* para esse efeito e, por isso mesmo, os perigos de tal exposição também aumentam. É neste caso que encontramos situações por vezes graves, que consubstanciam crimes, quer em que os jovens são as vítimas, como também os autores.

Dado que este é apenas um breve trabalho sobre este tema, não conseguimos aqui definir e analisar detalhadamente certas questões como esta. Não obstante, seria pertinente definir e analisar, tal como fizemos para as crianças, quem seriam ou são os responsáveis pelos *dados pessoais* no caso dos jovens, quem é o responsável quando um jovem entra num fórum *online* (para maior de 18 anos), de um jogo de *Playstation*, por exemplo? Ou quando um jovem afirma, num *sítio* de apostas *online*, que tem mais de 18 anos? Ou algo tão simples, como aceitar criar uma conta de uma rede social, tendo apenas 11 ou 12 anos de idade e tem a partir daí ínfimas possibilidades de socializar com milhares de milhões de utilizadores e fazer-se passar por outrem ou, ao contrário, ser vítima das más intenções de outrem?

Pegando precisamente nestas questões, é também no leque de *utilizadores* que encontramos os agentes que aproveitam os meios digitais para perpetrar crimes e obter vantagens sobre os demais. Por haver muito a abordar sobre estes, iremos analisá-los de forma autónoma no ponto seguinte.

2.3. Agentes Estatais

[349] COUNTINHO, Francisco Pereira; MONIZ, Graça Canto - **Anuário da Proteção de Dados**, CEDIS, Centro de I&D sobre Direito e Sociedade, 2018. ISBN: 978-972-99399-4-5, p.12.

Definidos e caracterizados que estão os utilizadores, importa agora traçar o perfil predominante dos agentes, em Portugal, segundo dados estatísticos da PJ de Lisboa.[350]

Ainda antes de passarmos aos dados estatísticos sobre estes agentes, importa primeiro que tudo defini-los. Dentro deste grupo, encontramos dois tipos de agentes: os *Hackers* e os *Crackers*.

Chamamos de *Hacker* a uma pessoa com um elevado conhecimento em sistemas de informática, que utiliza esses dotes para aceder a sistemas de informação sem o consentimento do utilizador. Fá-lo através de técnicas próprias, no intuito de ter acesso à informação confidencial e pessoal do utilizador, para proveito próprio ou de terceiros.

Por outro lado, o *Cracker* é, igualmente, definido como um *Hacker* mas que, ao contrário de simplesmente aceder para proveito próprio ou de terceiro, acede aos sistemas com o intuito de os apagar, modificar, ou introduzir informação distinta da que constava inicialmente, introduzindo também vírus e programas que lhe permitam tornar aquela informação como própria.[351]

Para além das diferenças em termos de conceito, estes dois cibercriminosos distinguem-se, também, pelo âmbito da sua atuação. Enquanto os *Hackers* procuram aceder a sistemas sem autorização, mas adotam uma conduta menos lesiva (se assim pudermos dizer), os *Crackers* têm uma conduta não ética e mais ofensiva, invadindo sistemas com interesses patrimoniais ou danosos. Estes últimos costumam pedir resgates, após acederem às informações dos utilizadores, sob pena de as apagarem ou divulgarem, por exemplo. Não obstante a ação dos *Hackers* ser descrita como menos evasiva em relação aos *Crackers*, importa reforçar que ambos praticam condutas lesivas, puníveis por lei.[352]

Em regra, se tivéssemos de definir as idades dos agentes, encontramos o seguinte perfil de agente cibercriminoso[353], dividido em três grupos:

- Muito novos – entre os 11 a 16 anos;
- Adolescentes – entre os 17 a 25 anos;
- Adultos – entre os 40 e mais anos.

Sobre as idades, não temos dados estatísticos relevantes, pelo que o gráfico infra demonstra apenas a divisão por faixa etária, estando todas ao mesmo nível de incidência.

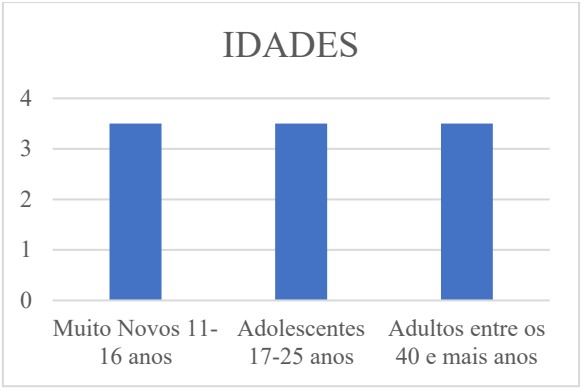
---

[350] Agradecimentos ao Inspetor Chefe da Polícia Judiciária, Dr. Rogério Bravo, pela amável partilha destes dados.

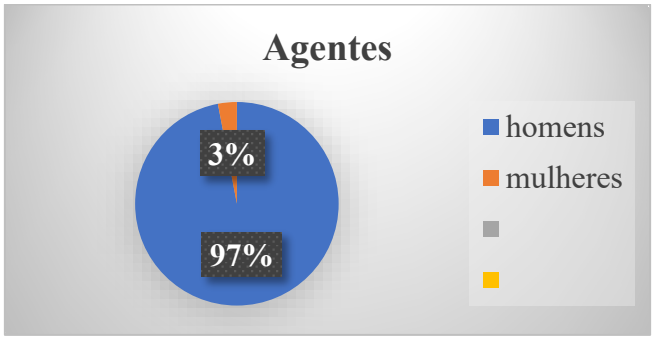
[351] PEREIRA, Joel Timóteo Ramos, **Direito da Internet e Comércio Electrónico**, Quid Juris?, Sociedade Editora, Lisboa, 2001, p.474.

[352] SANTOS, Ana Felícia Canilho - **O Cibercrime: Desafios e Respostas do Direito**, p.84 [em linha], Lisboa: UAL, setembro 2015. Tese de Mestrado em Direito. Disponível em: https://repositorio.ual.pt/handle/11144/2640 (Consult.10 mar.2023).

[353] Por agente cibercriminoso entendemos definir e englobar os dois conceitos, de *Hacker* e *Cracker*, com as diferentes definições já anunciadas no texto.

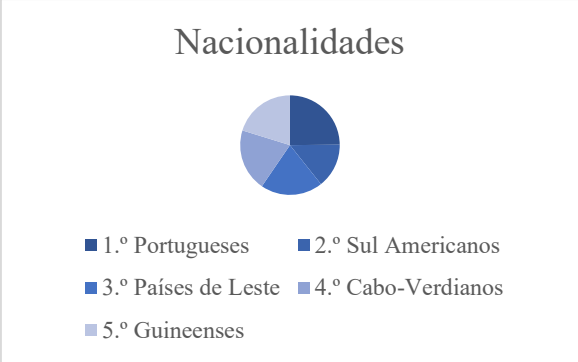


Aliados a estes dados, encontramos uma predominância do género masculino, 97% dos quais são homens, face a apenas 3% de mulheres.



No que diz respeito às mulheres, os dados de que dispomos, dizem respeito a um caso em concreto, em que todas as agentes eram portuguesas, cujas idades rondavam os 21 anos, sendo que uma delas, tinha 32 anos e era a organizadora do grupo. Outro dado interessante que caracteriza as mulheres, é que se inserem em grupos (agentes de cibercrime organizado), como sucedeu neste que aqui analisamos. Ao contrário do que sucede na estatística referente aos homens, que tanto atuam sozinhos, como em grupos organizados.

Também as nacionalidades dos agentes masculinos, no que diz respeito à sua atuação em Portugal, são curiosas e distintas do caso mencionado das mulheres, já que vemos uma predominância de agentes portugueses, seguidos de agentes sul americanos, em terceiro lugar, agentes dos países de leste e, finalmente, Cabo-Verdianos e Guineenses. Referimo-nos como sendo curiosas, na medida em que muitos destes países, no qual se insere Portugal, facilmente se perceberia que não teriam tanto acesso aos meios informáticos, ou que não estivessem tão bem desenvolvidos a nível digital, ou dos conhecimentos para perpetrar estes ataques. Não obstante, as estatísticas demonstram o contrário e vemos uma predominância de agentes oriundos destes países.



De referir ainda que a maioria destes agentes (aqui já no conjunto geral, homens e mulheres), não são licenciados, nem possuem cursos superiores; têm formação ao nível de cursos técnico-profissionais. São, também, pessoas com carências financeiras e provêm ou cresceram em famílias desagregadas, o que lhes traz uma certa marginalização e a necessidade de se afirmarem perante a sociedade. É no cometimento destes crimes que estes agentes se sentem enaltecidos e é no seio de grupos, ou sozinhos, que finalmente sentem que encontraram um propósito, seja a nível de valor, seja de afirmação perante os seus semelhantes. Vemos isso através da análise e estatística dos dados fornecidos pela PJ de Lisboa, onde nas faixas etárias dos 11 aos 16 anos são movidos por ego e ressentimento. Na faixa seguinte, dos 17 aos 25 anos, vemos a predominância ainda do ego e ressentimento, mas é nesta faixa que surgem, depois, outras motivações, como o dinheiro[354], a ideologia, o que lhes permite uma certa emancipação e fazer destas atuações o seu trabalho. Finalmente, na faixa etária mais velha, dos adultos, dos 40 anos em diante, permanece o ressentimento, aliado à obtenção de lucro, à motivação económica. Como se conclui, o ressentimento é o sentimento predominante e, se pudermos dizer, o combustível que os alimenta e instiga ao cometimento destes atos.

Os meios utilizados são, na grande maioria, computadores básicos e telemóveis. E as técnicas utilizadas FTTP[355] são inerentes aos aparelhos que têm e à informação mais divulgada.

[354] Neste âmbito, encontramos 3 tipos predominantes de crimes: furto de identidade, fraude bancária e Ransomware.

[355] FTTP - Fibra para as instalações (FTTP) é um meio de distribuição de cabo de fibra ótica que fornece acesso à Internet diretamente a um usuário ou grupos de usuários de um provedor de serviços de Internet (ISP). É um dos vários termos de topologia de entrega de fibra ótica que, às vezes, são agrupados na categoria geral de "Fibra com x" e abreviados de forma semelhante. [Em linha]. Disponível em: https://definirtec.com/fibra-para-as-instalacoes-fttp/ (consult. 13 mar.2023).

Os ataques mais frequentes, segundo dados estatísticos da PJ, são três: sabotagem[356], acesso ilegítimo[357] e acesso indevido[358]. Paralelamente, temos também o crime como um serviço. Por exemplo, é possível comprar uma *botnet*[359] para realizar um crime.

A proveniência destes ataques é, na sua maioria, realizada no estrangeiro e pode ser complementada em Portugal. Já quanto aos países alvo destes ataques, não se demonstra uma prevalência de uns face a outros, mas, sim, são escolhidos de acordo com as suas vulnerabilidades. Isto é, os agentes atacam aqueles Países que sabem, à partida, que têm vulnerabilidades conhecidas, tornando-os um alvo preferencial pela facilidade com que conseguem cometer aqueles atos.

No ponto seguinte, iremos precisamente avaliar a questão da Cibersegurança e as vulnerabilidades que foram sendo sentidas ao longo dos tempos.

Capítulo III - Cibersegurança

3.1. Conceito

Antes de partirmos para o ponto final e deixarmos algumas considerações sobre o que pensamos que possam ser as medidas adequadas para uma eficaz e segura utilização da Internet por parte dos utilizadores, importa fazer uma breve referência à Cibersegurança, avaliando o que se fez até então, e os momentos em que esta foi posta em causa. Mas comecemos por dar um breve conceito de Cibersegurança.

A par e passo, os Estados têm tentado definir e enquadrar o que se entende por Cibersegurança, à luz das estratégias publicadas e do que também consideram necessário proteger. De entre esses exemplos, destacamos dois conceitos que nos parecem bastante abrangentes e, ao mesmo tempo, concisos.[360] Por exemplo, destacamos a definição da Nova Zelândia, no nosso entender, como uma das mais

---

[356] Sabotagem informática – "o crime tem a ver com entravar ou perturbar o funcionamento do próprio sistema informático ou de comunicação de dados à distância (telemática)." SANTOS, Ana Felícia Canilho - **O Cibercrime: Desafios e Respostas do Direito**, p. 84 [em linha], Lisboa: UAL, setembro 2015. Tese de Mestrado em Direito. Disponível em: https://repositorio.ual.pt/handle/11144/2640 (Consult.10 mar.2023).

[357] Acesso ilegítimo – "Nestes casos, ocorre uma utilização não consentida e abusiva de contas e palavras-passe por parte de terceiros para acederem à Internet." *Idem*.

[358] Acesso indevido, Artigo 47.º da Lei n.º 58/2019, de 08 de agosto, Lei da Proteção de Dados Pessoais.

[359] Botnet - Rede de computadores comprometidos (também conhecidos como *zombies*) controlados por uma pessoa ou organização, que se destina a ser usada para atividades ilícitas. Uma vez criada, a rede de computadores infetados que constituem a "botnet" pode ser ativada sem o conhecimento dos utilizadores dos computadores, a fim de lançar um ciberataque em grande escala, o que geralmente tem o potencial de provocar danos graves, como por exemplo: a perturbação de serviços de sistema de importância pública significativa, ou importantes custos financeiros, ou a perda de *dados pessoais* ou informações sensíveis. SANTOS, Ana Felícia Canilho - **O Cibercrime: Desafios e Respostas do Direito**, p. 248 [em linha], Lisboa: UAL, setembro 2015. Tese de Mestrado em Direito. Disponível em: https://repositorio.ual.pt/handle/11144/2640 (Consult.10 mar.2023).

[360] SANTOS, Ana Felícia Canilho - **O Cibercrime: Desafios e Respostas do Direito**, p.49 [em linha], Lisboa: UAL, setembro 2015. Tese de Mestrado em Direito. Disponível em: https://repositorio.ual.pt/handle/11144/2640 (Consult.10 mar.2023).

completas, ao definir a Cibersegurança como a prática de tornar as redes que constituem o Ciberespaço as mais seguras possível contra intrusões, mantendo a confidencialidade, disponibilidade e integridade de informação, deteção de intrusões e incidentes que ocorram, responder-lhes e recuperar deles.[361] A Espanha, embora não tendo em literatura relevante, uma estratégia definida de Cibersegurança, considera-a como a proteção dos componentes das infraestruturas dos sistemas de informação e comunicação entre ameaças cibernéticas.[362]
Em Portugal, nas palavras do Engenheiro Lino Santos, define que "a atuação da Cibersegurança pretende mitigar os impactos negativos que a tecnologia introduz na Sociedade".[363] Neste sentido, acrescenta ainda o Inspetor-Chefe da PJ, Dr. Rogério Bravo, ao definir a Cibersegurança "como todo o tipo de atividade, a título preventivo ou repressivo, destinado a diminuir os incidentes de segurança e a perceber a sua autoria."[364]

Extraindo o "sumo" de todas estas definições e adotando um conceito só nosso, definiríamos a Cibersegurança como toda a atividade levada a cabo no mundo tecnológico/digital, que não só previne/acautela o acontecimento de eventuais situações, como ajuda os seus utilizadores e entidades, que lidam diretamente com a área da informática, a combater as eventuais situações que desse uso advenham. Desta forma, a definição de Cibersegurança, no nosso entender, tem duas componentes, uma preventiva e uma coerciva, na medida em que tanto é chamada a prevenir eventuais ataques e a dotar os seus utilizadores com o *know how* necessário de como preveni-los, bem como a solucionar e a aplicar medidas quando os ataques já ocorreram.

Ao longo do ponto seguinte, vamos poder perceber as datas e os principais acontecimentos quando e onde a Cibersegurança foi chamada a intervir, ora na eventual iminência de um ataque, ora quando este já tinha ocorrido. Vamos, também, perceber como os ataques e o *modus operandi*[365] dos agentes foram evoluindo ao longo dos anos, até aos dias de hoje.

---

[361] *Idem.*
[362] FREIRE, Vicente - **Cibersegurança e Ciberdefesa: A Inevitabilidade de Adoção de uma Estratégia Nacional**, in Segurança e Defesa, Revista Trimestral, n. º21, maio-agosto 2012.
[363] Engenheiro Lino Santos é, desde 2018, coordenador do Centro Nacional de Cibersegurança. Definição dada na aula de dia 03/01/2023, da 7ª edição da Pós-Graduação em Proteção de Dados Pessoais, Privacidade e Cibersegurança na UE.
[364] Entrevista a Rogério Bravo (Inspetor-Chefe, Polícia Judiciária de Lisboa), no dia 18 de fevereiro de 2014, no âmbito da minha Dissertação de Mestrado. SANTOS, Ana Felícia Canilho - **O Cibercrime: Desafios e Respostas do Direito**, p.122 [em linha], Lisboa: UAL, setembro 2015. Tese de Mestrado em Direito. Disponível em: https://repositorio.ual.pt/handle/11144/2640 (Consult.10 mar.2023).
[365] *Modus operandi* – expressão em latim que significa modo de atuação.

3.2. Evolução da Cibersegurança

Após termos explorado o conceito de Cibersegurança, cumpre-nos agora fazer uma breve passagem pelos pontos chave do surgimento da Cibersegurança ao longo dos tempos, dando ênfase aos acontecimentos mais importantes.

Década de 80, num primeiro momento, na década de 80, não havia um *bem* a proteger, propriamente dito e, por isso, não havia uma ação dolosa, havia sim, uma intenção dos agentes em importunar os utilizadores. Nesta década, a atuação dos agentes caracterizava-se pelo envio sistemático de mensagens de *spam*, de modo a entupir os servidores e as caixas de correio dos utilizadores. Nesta década, a segurança informática era do domínio dos Engenheiros, o que, desde logo, nos demonstra que não havia ainda uma necessidade de o Direito ser chamado a regular e a legislar sobre estas matérias, nem os órgãos de Polícia criminal, nomeadamente, a PJ não era chamada a intervir.

Década de 90 (mais concretamente entre 1996 e 1998), a partir desta década, houve uma expansão da Internet para os Bancos, com a criação dos *sítios* informáticos, a chamada Banca *online*. Assim sendo, surgiram novas formas de atuar no mundo informático e foi a partir daqui que surgiram os crimes de *Blueboxing*[366] *carding*[367], termo que, de um modo geral, se refere à clonagem de cartões, entre outros. Já havia outros tipos de crimes, mas foi nesta altura que surgiram os crimes ligados ao mundo financeiro por meio tecnológico.

Década de 2000: Ano de 2001, entendemos que, embora não tenha ocorrido um ataque diretamente perpetrado por meios informáticos, o meio onde este se desenvolveu e foi planeado, foi através de um meio informático em concreto, por troca de *emails* via conta Gmail (Google). Falamos aqui do atentado de 11 de setembro de 2001 às torres gémeas, comummente conhecidas como World Trade Center. Esta data é importante, pois foi a primeira vez que o mundo se apercebeu que os meios de telecomunicações serviam, ou estariam a ser utilizados como ferramenta de troca de informações e planeamento de ações (ou ataques) em larga escala, e mais, entre países que, à partida, não se assumiria que tivessem

[366] *Blueboxing* – "Os crimes *Blackboxing* e *Blueboxing* são formas de perturbação das telecomunicações. Nestes casos, o agente faz uma interferência nas frequências das linhas telefónicas (*blackboxing*), onde liga estes dispositivos eletrónicos (*blueboxing*), cujo efeito, de entre outros, é o impedimento total ou a diminuição da taxa devida à operadora de telecomunicações. SANTOS, Ana Felícia Canilho, O cibercrime: desafios e respostas do direito, p.122 [em linha], [Em linha]. Lisboa: UAL, setembro 2015. (consult. 10 mar.2023). Dissertação de Mestrado em Direito. Disponível em: https://repositorio.ual.pt/handle/11144/2640

[367] *Carding* - "O Carding consiste numa forma de dados ou de elementos de identificação quer na face quer contidos em bandas magnéticas de cartões de crédito, de débito ou de telecomunicações, bem como a implantação de dados ou de elementos de identificação noutros suportes técnicos." SANTOS, Ana Felícia Canilho, O cibercrime: desafios e respostas do direito, p.122 [em linha], Lisboa: UAL, setembro 2015. (consult. 10 mar.2023). Dissertação de Mestrado em Direito. Disponível em: https://repositorio.ual.pt/handle/11144/2640

acesso a este tipo de comunicações (falamos aqui de Países como o Afeganistão, que em comparação com os EUA, por exemplo, se suporia que não teriam acesso a meios informáticos, ou redes de ligação tão avançados como estes últimos). Foi a partir daqui, no nosso entender, que a necessidade de uma Cibersegurança internacional e eficaz se tornou mais premente.

Ano de 2007, nesse ano e ainda durante a década de 2000, houve um vasto conjunto de ataques contra o Governo, a imprensa, a banca e a grandes empresas contra a Estónia, após a polémica levantada com a retirada da estátua que comemorava os soldados do Exército Vermelho que combateram os nazis na Segunda Guerra Mundial.[368] Uma vez mais, circulava a informação, segundo alegações do Ministério, que estariam a ser utilizados meios informáticos, mais concretamente, *sítios* informáticos russos, para esclarecer como se poderiam realizar ataques. Esta foi uma situação que mobilizou especialistas da OTAN e de vários países da UE que, prontamente se disponibilizaram para verificar a situação, perceber a sua origem e veracidade das alegações, com a exceção da Rússia, que não aceitou cooperar. Apesar das imputações do Governo da Estónia ao Governo Russo, este último negou qualquer relação com aquele ataque e refutou qualquer responsabilidade sobre os ataques ocorridos. Nunca chegou a haver uma confirmação do alegado.

Nos anos seguintes, tivemos um incremento de ataques que, não obstante serem de baixa sofisticação (ou seja, pouco complexos), eram oriundos de todas as partes do mundo, incluindo de Portugal. É a partir daqui que se dá o alargamento da Cibersegurança, o maior já visto, já que daqui em diante se incluiu a parte militar, levando a que muitos países começassem a assumir esta nova forma de cometer crimes, como uma séria ameaça às suas Nações.

Ano de 2011, o mundo volta a receber novas informações de como a vida dos cidadãos estava mais exposta do que se julgava possível. Foi graças às declarações de Edward Snowden[369] e do caso Wikileaks[370], pelo seu fundador Julian Assange, que

---

[368] Para mais informações sobre esta situação, poderá ser consultada a entrevista disponível no *sítio* informático da BBC. [em línea]. (Consult.10 mar.2023). Disponível em: https://www.bbc.com/portuguese/reporterbbc/story/2007/05/070517_estoniaataquesinternetrw

[369] "Edward Joseph Snowden é um analista de sistemas, ex-administrador de sistemas da CIA e ex-contratado da NSA que tornou públicos detalhes de vários programas que constituem o sistema de vigilância global da NSA americana". [. Em línea]. (última consult. 10 mar.2023). Disponível em:
https://pt.wikipedia.org/wiki/Edward_Snowden
Sobre este foram ainda realizados vários filmes e séries.

[370] Wikileaks – "A WikiLeaks assume-se como organização de comunicação sem fins lucrativos. Lançada oficialmente em 2007, abanou o mundo em 2010 com revelações que embaraçaram Governos. Tornou-se objeto de debate e foi alvo de bloqueio por parte de empresas de serviços bancários. Em 2011, chegou a anunciar a suspensão de atividades,

ficámos a conhecer factos e informações que até então apenas estavam sob o conhecimento de quem as trocava. Esta polémica descoberta levantou várias questões, nomeadamente, no âmbito da legalidade. Deverá o cidadão saber que os seus dados são do conhecimento público ou, por outro lado, será que há certos assuntos, sendo a troca de dados, um deles, que devem permanecer em segredo?

Mais grave ainda é quando pensamos que muitos dos dados (e não falamos aqui só de dados pessoais, mas sim de dados em geral, informações confidenciais sobre situações de guerra, ou que motivaram guerras, trocas de informações sobre armamento e pagamentos para financiar esse armamento, coligações, amizades com motivos ulteriores, etc…) que foram dados a conhecer ao mundo, foram a causa de muitos acontecimentos que afetaram a todos e dos quais os seus autores saíram impunes. Muitas destas situações, ao tornarem-se do conhecimento público, deram origem a grandes questões políticas e diplomáticas. Esta situação deixa-nos com uma questão muito importante, admitindo (como pudemos **e** podemos comprovar que isto ocorre), que existe esta troca de informações, devem ser do conhecimento geral, prezando assim pela transparência, ou será que há situações que, pelo seu cariz diplomático, devem ser mantidas em segredo?

A resposta parece-nos complicada de responder. Se, por um lado defendemos a transparência e o sigilo na troca destes dados, também não é menos verdade que o conhecimento de algumas destas informações, ao tornar-se do domínio público, poderiam ter como consequência uma guerra ao nível mundial, numa escala que abrangeria vários Países. No nosso entender, a resposta a esta questão passa por aferir o que é mais importante: se a privacidade das conversações e dos dados nestas contidos, evitando uma possível guerra, ou tornar as conversações e os dados públicos a qualquer custo, ainda que isso traga consequências nacionais e internacionais.

Ano de 2013, é publicada a primeira Resolução, onde vem referido que os Direitos Pessoais também se aplicam no Ciberespaço[371]. Foi graças a esta Resolução que os Estados Membros, no qual se inseriu Portugal[372], definiram que era urgente prevenir e dar respostas às eventuais solicitações na área tecnológica, nomeadamente, as

---

mas, em 2012, voltou a apresentar sinais vitais (…)". **Observatório sobre Crises e Alternativas,** Centro de Estudos Sociais da Universidade de Coimbra. [Em línea]. (última consult. 10 mar.2023). Disponível em: https://www.ces.uc.pt/observatorios/crisalt/index.php?id=6522&id_lingua=1&pag=7868

[371] Estratégia da UE para a Cibersegurança: um ciberespaço aberto, seguro e protegido. Resolução do Parlamento Europeu, de 12 de setembro de 2013, sobre a estratégia da União Europeia para a
Cibersegurança: um ciberespaço aberto, seguro e protegido (2013/2606(RSP)), (2016/C 093/16). [em línea]. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-7-2013-0376_PT.pdf?redirect (consult. 12 mar.2023).

[372] [em línea]. Documento completo, disponível em: https://app.parlamento.pt/webutils/docs/doc.pdf?Path=6148523063446f764c324679626d56304c334e706447567a4c31684a5355786c5a793944543030764e454e425253394562324e31625756756447397a535556564c7a67774d3251785a5459344c54426b595441744e446b7a4e793169596d59354c546b794f5759324e6d49774e445131595335775a47593d&Fich=803d1e68-0da0-4937-bbf9-929f66b0445a.pdf&Inline=true (consult. 12 mar.2023).

perturbações e ataques na *internet*. O objetivo da estratégia era criar e financiar uma rede de Centros especializados nesta matéria, de âmbito nacional de cada Estado, contra a cibercriminalidade, por forma a fomentar a formação e a adoção de medidas preventivas, bem como o desenvolvimento de capacidades no domínio da Cibersegurança. Esta visava, ainda, "garantir um ambiente digital seguro e fiável na UE, através da atuação de todos os Estados-Membros, bem como dos fornecedores de serviços de Internet e dos operadores de infraestruturas."[373]

Ano de 2016, foi outro ano de extrema importância, no que diz respeito à forma como o mundo real (se assim pudermos chamar) e o mundo digital se imiscuíram um no outro. Neste ano, assistimos às eleições mais mediáticas dos últimos anos e atrevemo-nos mesmo a defini-las como as mais importantes e discutidas[374] também. O mundo parou perante a eleição de Donald Trump, enquanto Presidente dos Estados Unidos. Se, por um lado era conhecido como empresário bilionário e figura pública, presença assídua em programas televisivos (um deles da sua autoria) e dono de várias empresas, por outro lado passava despercebido ao mundo político, até à altura da sua candidatura e posterior vitória frente à sua opositora, Hillary Clinton. Referimo-nos ainda como as mais perigosas, porque a partir daqui, ficámos a saber que era possível manipular pessoas e modificar resultados eleitorais através de meios eletrónicos[375]. O projeto Alamo[376], nome pelo qual ficou conhecido, foi uma intervenção de uma empresa de marketing e banco de *dados pessoais*, que atuou através da empresa Facebook, onde sondou e inquiriu milhares de utilizadores, através das suas páginas das redes sociais. Munidos dos *dados pessoais*, dos gostos e opções de cada um, foi possível traçar o perfil dos mesmos e adaptá-los às eleições, fazendo com que a sua opinião favorecesse um candidato, nomeadamente, Donald Trump, em detrimento dos demais. Tudo isto sem que o utilizador soubesse que estava a ser vítima desta atuação.

Já em 2008, Barack Obama tinha usado dados e canais de comunicação digital, para divulgar a sua candidatura a Presidente dos EUA. No entanto, nada teve a ver com a manipulação de votos. Foi considerada apenas uma manobra de

---

[373] [em línea] Disponível em: https://www.anacom.pt/render.jsp?contentId=1156691 (última consult. 12 mar.2023).

[374] Referimos o termo 'discutidas', ao olharmos para estas eleições como responsáveis pelo aumento de candidatos mais intervencionistas e radicais (Donald Trump - EUA, Jair Bolsonaro – Brasil, VOX – Espanha, entre outros…). Esta mudança da democracia, levou ao incremento de crimes de ódio, raciais, xenofobia, homofobia e atentados graves contra a pessoa humana.

[375] Cambridge Analytica, admitiu na época ter mais de 5.000 dados sobre cada cidadão americano. A respeito deste assunto e para mais informações sobre o mesmo, recomendamos a leitura do artigo Cambridge Analytica. Encontramos ainda vários artigos sobre este tema, bem como uma série na plataforma de *streaming* Netflix, "Nada é Privado: O Escândalo da Cambridge Analytica", que retrata bem o que efetivamente sucedeu durante as eleições de 2016, nos EUA.

[376] Para mais informações sobre este projeto. [em línea]. Disponível em: https://www.semantiko.com/blog/project-alamo (consult. 12 mar.2023).

marketing. Não obstante, esta passagem das eleições, nomeadamente das candidaturas e das campanhas eleitorais para o mundo digital permitiu criar um mercado de oportunidades, que foi astutamente aproveitada em 2016.

Ano 2020 , seguindo a ideia anterior e ainda sobre a manipulação das massas, neste caso dos eleitores, observámos outro claro exemplo em 2020. Falamos aqui da saída do Reino Unido da União Europeia, apelidado de Brexit. Embora não hajam dados em concreto a esse respeito, após as entrevistas de Christopher Wylie (ex-consultor de dados da Cambridge Analytica, que já se tinha pronunciado sobre a polémica eleição de Donald Trump), veio novamente a público referir que houve uma manipulação dos eleitores, com base nos seus gostos e preferências, através do cruzamento dos dados por parte da Cambridge Analytica e que permitiu mudar a mentalidade dos Britânicos, de forma a alterar a posição destes e a permitir a saída do Reino Unido da UE.

Anos 2022/2023, a nível Nacional e trazendo de novo à nossa temática a divulgação de dados e informações sigilosas (como trocas de *emails,* trocas de mensagens escritas, vulgo SMS, ou até conversações telefónicas), ao conhecimento do público, damos como exemplo as recentes investigações de inúmeras conversações pessoais e privadas de pessoas influentes, tais como Ministros, Presidentes e demais órgãos políticos, onde Juntas de Freguesia, Câmaras Municipais e grandes empresas como a TAP Portugal se inserem. Estas investigações, que agora estão a ser tornadas públicas e a ser alvo de ações Judiciais, colocam de novo em causa a nossa pergunta anterior. Será que o interesse sobre certos assuntos se sobrepõe à proteção dos *dados pessoais* dos visados, ou será que há exceções, nas quais estes casos se inserem? Esta pergunta, por si só, daria para fazer um longo trabalho sobre os prós e os contras desta temática.

3.2. Apresentação de soluções: consciencialização do utilizador

Antes de concluirmos este nosso trabalho, deixamos algumas considerações que, no nosso entender, farão toda a diferença no dia a dia de cada um de nós e no fomento de uma maior consciencialização por parte do *utilizador*.

Como pudemos verificar ao longo deste trabalho, a privacidade da informação de cada um passa, em primeira instância, por nós próprios, pelo comportamento humano. De nada servirá ter *aplicações* de topo ou ferramentas de bloqueio de *firewalls* e de antivírus se, depois, usamos para todas as nossas *aplicações* e contas a mesma *password* ou, embora possa ser diferente, é fraca ou está acessível a qualquer um (por exemplo, se deixamos na nossa gaveta, ou num *post it* no local de trabalho, todas as nossas *passwords* escritas, ao alcance de qualquer pessoa que ali entre). De igual modo, se deixamos as nossas *aplicações* abertas e nunca, ou raramente, encerramos as sessões quando saímos de uma *aplicação*, ou no local de trabalho, do nosso início de sessão no computador. Igualmente, no caso dos nossos *dados pessoais* e no que pode suceder se deixamos

uma cópia do Cartão de Cidadão com alguém, ou se permitimos que alguém utilize esse nosso Cartão. Na mesma medida em que não daríamos o nosso Cartão Multibanco e o respetivo *código pin* a ninguém, o mesmo devemos aplicar quanto ao nosso Cartão de Cidadão.

Assim, entendemos que as seguintes medidas (daremos uma lista breve, embora existam outras medidas que podem e devem ser tomadas por cada um), podem ser uma boa opção para minimizar a nossa exposição aos riscos associados ao acesso indesejado aos nossos *dados*, quer seja por descuido, por inatenção ou por ação dolosa de terceiros (sem qualquer ordem de importância):

- Primeiro que tudo, questionar sempre. Questionar qual a finalidade do uso dos nossos *dados*; para que necessitam da cópia do Cartão de Cidadão ou do próprio cartão; etc.;
- No seguimento da alínea anterior, saber quais são os nossos direitos e o que devemos e podemos transmitir a uma Entidade, pessoa, *aplicação*, etc. e o que não devemos ou não é necessário.

No âmbito digital:

- Manter atualizados os dispositivos digitais (seja o *software* do computador, seja do telemóvel, já que estes comportam as últimas atualizações ao nível da segurança e as falhas que os fabricantes possam ter detetado, à medida que o produto vai sendo experimentado); igualmente no caso dos *antivírus*;
- Não utilizar redes de *Internet* abertas (as chamadas *free WiFi*) ou partilhadas, especialmente em locais com muitas pessoas, como: aeroportos, centros comerciais, ginásios, etc., já que estas redes ao serem abertas, permitem precisamente a utilização de todos, incluindo de utilizadores mal-intencionados. Evitar especialmente o uso destas redes, ao utilizar aplicações bancárias ou fazer transações;
- Encerrar ou bloquear sempre o nosso computador, tablet, ou aparelho digital, e quando não o estivermos a utilizar, seja em casa, seja no trabalho (de forma a evitar que o acesso ao mesmo fique aberto à intromissão ou utilização de terceiros);
- Ainda no âmbito laboral, é importante separá-lo do nosso tempo de lazer e, por isso, o computador deverá ser usado para o fim a que se destina evitando, sempre que possível, o uso do computador laboral para fins de recreio;
- Utilizar *passwords* fortes e robustas (mínimo de 9 caracteres para utilizadores comuns e 13 para administradores de *aplicações* e *sistemas* – de acordo com a RCM n.º 41/2018), compostas por letras, números e símbolos, e evitar *passwords* simples ou *dados pessoais* (datas de nascimento, nome próprio, ou nomes de familiares, etc.);
- Utilizar *passwords* distintas para cada conta ou utilização que tenhamos (evitar copiar *passwords* profissionais, para lazer e vice-versa);

- Usar autenticação de duas etapas em vez de uma única (*single sign on*), em todas as contas e *aplicações* (se possível) mas, especialmente, em *aplicações* bancárias;
- Não abrir *pens* ou discos externos, cuja proveniência desconhecemos nos computadores laborais ou pessoais;
- Não permitir ligações de *dispositivos* externos à rede interna, sem serem avaliados pela equipa de redes da nossa Entidade laboral ou, no âmbito privado, da nossa casa.
- Entre outras... [377]

Conclusão

O que poderia ter começado como uma ideia utópica, um mundo ligado digitalmente, rapidamente se tornou real. Um espaço onde todos pudessem partilhar as suas experiências, opiniões e frustrações, um álbum de memórias digital dos momentos mais importantes e que partilhamos com os demais, um local que faz de casamenteiro (nas suas diversas aplicações para esse efeito) e até de terapeuta, um local que nos permite a partilha de emoções e fá-lo através das suas diversas aplicações - os meios fundamentais para que ninguém se sinta sozinho. Observando este vasto mundo, seria pertinente perguntar o que sucede a todos estes *dados*, a toda esta informação que criamos e partilhamos? Será que a sua presença na *internet* é efémera, ou será que perdura no tempo e é constante?

Ao investigarmos a fundo estas questões e perante os vários estudos neste sentido, sabe-se agora que estes vestígios digitais, nossos, de cada um, são explorados por uma indústria que rende um bilião de dólares anuais. Achamos que somos o consumidor mas, na realidade, somos a mercadoria.[378] Todas as nossas interações, partilhas, "gostos" ("likes"), pagamentos com Cartões de Crédito, comentários e ativações de localização no nosso telemóvel, entre outras ações que já adotámos para o nosso quotidiano, tudo é recolhido em tempo real e associado à nossa identidade diariamente, dando a qualquer "comprador desses dados", acesso direto às nossas vidas. Munidos dessas informações sobre os nossos perfis, esses mesmos "compradores" (entre eles, sítios informáticos, empresas, marcas, etc.), têm agora na sua posse as nossas preferências, o que lhes permite criar conteúdos exclusivos de acordo e para as características de cada utilizador. A título de exemplo, quantos de nós já pesquisou por uma dada compra ou viagem e, logo de seguida, como que por magia, foi inundado de sugestões em tudo similares à pesquisa que fez? De igual forma, e indo mais longe, quantos de nós já falaram perto,

[377] Retirámos algumas das ideias de entre as soluções apresentadas pelos autores, com as nossas necessárias adaptações e contributos. FRANCISCO, Daniel e FRANCISCO, SANDRA, **RGPD – Regulamento Geral de Proteção de Dados**, p. 145. 2ª ed., Edições Sílabo. ISBN: 978-989-561-283-3.

[378] Existe um ditado em inglês sobe o mercado digital, precisamente neste sentido: "If you're not paying for a product, then you are a product.".

ou ao telemóvel com alguém sobre uma dada compra ou viagem e, uma vez mais, foi inundado de sugestões nesse sentido? A resposta seria, muitas vezes.[379]

A este respeito, e como seria de esperar, as empresas mais ricas são, precisamente, as empresas de tecnologia: Google, Facebook, Amazon, Microsoft, Apple, Tesla (sem ordem cronológica).[380] E a razão pela qual são consideradas as mais poderosas do mundo é, precisamente, porque em 2018, o valor dos *dados pessoais* ultrapassou o valor do petróleo.[381]

Podemos considerar que os *dados pessoais* são o bem mais valioso do mundo. E estas empresas são valiosas, porque têm estado a explorar os *bens*, os *dados pessoais* dos utilizadores, os quais lhes são "entregues", de livre vontade, por todos nós. Já em 2006, o matemático Clive Humby havia dito a seguinte frase: "os dados são o novo petróleo" [382]. Estas empresas que utilizam e lucram com os nossos *dados* são apenas 1/3 dos agentes a quem os nossos *dados* mais interessam. Os outros dois são as plataformas digitais (de certa forma, são e estão incluídas nas próprias empresas) e o terceiro agente é o mercado negro, os agentes criminosos. Assim, a forma como os nossos *dados* são usados e o valor que a estes é atribuído depende, primeiramente, do tipo de agente que a eles tem acesso: se é uma empresa, companhia ou agente criminoso e diretamente ligado ao primeiro ponto, que tipo de intuito tem para com os nossos *dados*.

As plataformas digitais como o Facebook, o LinkedIn, o Youtube ou o Twitter, que permitem que o utilizador crie o seu próprio *conteúdo*, utilizam os *dados* como moeda de troca para aumentar as suas vendas. Desta forma, e fazendo uso dos nossos *dados*, aumenta o público-alvo que assiste aos nossos conteúdos, mas

---

[379] A este respeito, tudo é influenciado pelos *cookies* (pequeno arquivo que fica armazenado no computador do utilizador e guarda todas as informações importantes sobre a sua navegação) presentes nos *sítios* informáticos que servem, precisamente, para recolher os nossos gostos e criar o nosso *perfil* de utilizador. Mas também os algoritmos, uma vez mais criados pelos *sítios* informáticos e pelas *contas* que criamos nas *aplicações* como o *Instagram* e o *Facebook*, entre outras, que adaptam as publicações e as recomendações que surgem nas nossas *páginas pessoais* ao nosso *perfil*.

[380] Lista referente a 2020 [Em linha]. Disponível em: https://www.forbes.com/the-worlds-most-valuable-brands/#20cc116a119c (consult. 17 mar.2023). Lista referente a 2023. [Em linha]. Disponível em: https://forbes.com.br/forbes-money/2023/01/as-10-marcas-mais-valiosas-do-mundo-em-2023/
(consult. 17 mar.2023).

[381] [Em linha]. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (consult. 17 mar.2023).

[382] "Data is the new oil" – podemos, inclusive, encontrar esta frase na sua página pessoal da rede social LinkedIn. [Em linha]. Disponível em: https://uk.linkedin.com/in/clivehumby?challengeId=AQFjVBQdJdGMzgAAAYbw-5reO8FuqTlAedCKzCYSjgFScbOgXAaHvbeNSL51ACV0Ab4KxlCi8TzsivYtQE6yfC50XitsPPJJow&submissionId=0115b10a-9b4a-4d17-e299-38bb3057b230&challengeSource=AgH9t7Vd6V8hMgAAAYbw-9sMk3gFsypGN0SsPo0x4smG-Fnk-8eIKTT3VN_FL9M&challegeType=AgHujh2VNVMWaQAAAYbw-9sP9ri4JQ-xCNYPOJviFzx8laNowP69NS4&memberId=AgEPt3w6GcpzOAAAAYbw-9sTkgB2KXB7fJrs-DJR7PnhVMM&recognizeDevice=AgFNtyCsdQupkQAAAYbw-9sWJwOVKUCPyO1_OC6OURGsxdjzWbDg (consult. em: 17 mar.2023).

também aumenta a percentagem dos nossos *dados* a que essas empresas têm acesso e que elas próprias partilham com terceiros.[383]

As empresas funcionam de forma semelhante aos anteriores, com uma pequena singularidade. A estas interessa saber qual o tipo de utilizador que somos e, por isso, necessitam saber mais *dados* específicos sobre nós, de forma a criar um perfil o mais detalhado possível para que, depois, possam perceber a quem "vender" esses *dados*. Os *dados* certos podem definir preferências pessoais, afiliações, orientações sexuais, dinâmica familiar, política e muito mais, para garantir que a mensagem certa chegue ao público certo no momento certo. (A este respeito, relembramos o que falámos no ponto 3.2. do Cap. III, sobre as eleições nos EUA em 2016 e o perfil exato que com estes *dados* se cria de um utilizador e os fins para os quais estes *dados* podem ser usados). Para as empresas, os *dados* são uma oportunidade de entender melhor as necessidades, os desejos e os pontos problemáticos de um público e, mais especificamente, como eles podem ajustar os seus produtos, serviços e mensagens, para atender melhor a esses pontos.[384]

Finalmente, os agentes criminosos acedem (contrariamente aos anteriores exemplos), com uma intenção dolosa, criminal e fazem-no através de diversos meios: acesso ilegítimo, roubo de identidade, entre outros, sendo que o motivo principal de tal acesso é, em última instância, a obtenção de lucro (como tivemos oportunidade de constatar ao analisar o perfil dos cibercriminosos), através da venda desses *dados* a quem oferecer mais dinheiro ou, atualmente, *criptomoedas*. Assim, encontramos no mercado negro, todo o tipo de informação pessoal que se possa imaginar. De igual modo, encontramos vários tipos de compradores para os nossos *dados*, como por exemplo outros agentes criminosos singulares, ou em organizações criminosas e ainda Governos de países estrangeiros. O valor de venda desses *dados* depende, primeiro de tudo, do intuito do agente que os vende (se é a obtenção de maior ou menor margem de lucro); se é algum motivo pessoal (chantagem ou extorsão) e, por isso, o intuito é também o de causar dano à imagem de uma pessoa (por exemplo, na divulgação de um vídeo de cariz sexual), etc. É difícil, por isso, apurar um valor concreto que é dado, ou pelo qual são vendidos os *dados* no mercado negro, tanto podemos encontrar dois milhões de *dados pessoais* de Portugal à venda na *dark web* por $10USD, noutros casos estavam à venda por duas centenas de USD e agora, *criptomoedas*.[385]

Em face do exposto e analisados os tópicos que nos pareceram mais importantes de abordar ao longo deste breve trabalho (muito mais ficou por explorar), concluímos que os *dados pessoais* são o petróleo do século XXI. Não geram guerras, por enquanto, porque tal valor é ainda uma matéria-prima em bruto,

---

[383] A este respeito, em 2020, LinkedIn Marketing Solutions arrecadou mais de 3 bilhões de dólares de receita, ao fornecer aos anunciantes acesso aos seus mais de 700 milhões de usuários. De igual modo, o YouTube obteve uma receita de 6.9 bilhões de dólares em publicidade no mesmo período. Tradução livre. [Em linha]. Disponível em: https://www.invisibly.com/learn-blog/how-much-is-data-worth/ (consult. em: 17 mar.2023).

[384] Tradução livre. [Em linha]. Disponível em: https://www.invisibly.com/learn-blog/how-much-is-data-worth/ (consult. em: 17 mar.2023).

[385] Exemplos fornecidos pelo Inspetor-Chefe da PJ, Dr. Rogério Bravo.

apenas do conhecimento das entidades que os exploram, como as plataformas digitais, as empresas e os agentes criminosos, como pudemos abordar, anteriormente, relativamente à qual os utilizadores, todos nós enquanto proprietários desses *dados*, os disponibilizamos sem a devida consciência do seu valor e da sua importância. Para que possamos assistir a um vídeo, a uma notícia ou, simplesmente, consultar um *sítio* informático, aceitamos a política de *cookies*, ou aceitamos os termos e as condições sem, muitas das vezes, lermos o que este *sítio* irá recolher a nosso respeito e fazemo-lo quase de forma automática, porque já sabemos que sem aquela aceitação não podemos ver o que queremos ver. Estratégia brilhante, diríamos nós.

É difícil de antever qual será o futuro dos nossos *dados pessoais*, pois esta previsão está diretamente ligada a uma série de condicionantes: De que forma as pessoas vão tratar os seus *dados* doravante, nomeadamente, no que diz respeito ao uso e à partilha dos mesmos com terceiros? De que forma os vão proteger ou, pelo menos, tornarem-se mais conscientes que esses necessitam de proteção, como se de uma extensão da sua vida se tratasse (e cuja presença *online* se irá prolongar mesmo após a nossa morte)? De que forma o Direito e o legislador se vão adaptar a esta nova realidade e à constante necessidade de consagrar e proteger os *dados pessoais*? Quais as mudanças necessárias ao RGPD e à eventual criação de outros diplomas deste cariz já que, contrariamente ao que sucede no "*mundo real*", o "*mundo digital*" não é estático e está em constante mudança, pelo que as Leis a aplicar nesse âmbito têm que se adaptar às suas constantes evoluções.

Gostaríamos que este nosso breve trabalho, identificado logo no título e desenvolvido nos capítulos que o compõem, clarifique a temática sobre a qual nos propusemos debruçar, e possa contribuir para a consciencialização por parte de cada titular dos *dados pessoais*, todos nós afinal, sobre a importância de os perceber, nomeadamente, sobre a que se referem, quando falamos em *dados pessoais*, com que finalidade são usados e por quem, o seu valor de mercado, etc. É nosso propósito que cada indivíduo, depois de compreender estes pontos, tenha a preocupação de proteger os seus *dados pessoais* porque, como concluímos, são um *bem* valioso, altamente lucrativo e que, por isso, nem sempre são utilizados por terceiros com as melhores intenções.

Bibliografia

ACUÑA, Concepción Campos, **Aplicación práctica y adaptación de la protección de datos en el ámbito local.** Novedades tras el RGPD y la LOPDGDD. 2ª Ed. enero 2019. Wolters Kluweer. BOSCH. ISBN Papel: 978-84-7052-472-1

CALVO, José López, **La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD**. febrero 2019. Wolters Kluweer. BOSCH. ISBN: 978-84-9090-345-2

COUTINHO, Francisco Pereira; MONIZ, Graça Canto, **Anuário da Proteção de Dados**, CEDIS, Centro de I&D sobre Direito e Sociedade, 2018. ISBN: 978-972-99399-4-5.

COUTINHO, Francisco Pereira; MONIZ, Graça Canto, **Anuário da Proteção de Dados de 2020**, CEDIS, Centro de I&D sobre Direito e Sociedade. junho, 2020. ISSN 2184-5468. [Em linha]. Disponível em: http://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2020/07/ANUARIO-2020-Eletronico.pdf

FRANCISCO, Daniel e FRANCISCO, SANDRA, **RGPD – Regulamento Geral de Proteção de Dados,** 2ª ed., Edições Sílabo. ISBN: 978-989-561-283-3.

FREIRE, Vicente - Cibersegurança e Ciberdefesa: A Inevitabilidade de Adoção de uma Estratégia Nacional, in Segurança e Defesa, Revista Trimestral, n. º21, maio-agosto 2012.

GOMES, Mário M. Varges, O Código da Privacidade e da Protecção de Dados Pessoais na Lei e na Jurisprudência (Nacional e Internacional), Colecção direito das novas tecnologias, CENTROATLANTICO.PT, Portugal, 2006, ISBN: 989-615-022-2.

PEREIRA, Joel Timóteo Ramos, **Compêndio Jurídico da Sociedade da Informação**, *Quid Juris*? Sociedade Editora, Lisboa, outubro, 2004. ISBN: 978-972-724-225-2.

PINHEIRO, Alexandre Sousa (Coord.), **Comentário ao Regulamento Geral de Proteção de Dados**, Ed: Edições Almedina, Coimbra, dezembro 2018. ISBN: 978-972-407-782-6.

SOUSA, Constança Urbano de, O **Espaço de Liberdade, Segurança e Justiça da UE: Desenvolvimentos Recentes**, Departamento de Direito, EDIUAL, Universidade Autónoma Editora, maio 2014. ISBN: 978-989-8191-61-8.

VENÂNCIO, Pedro Dias, **Lei do Cibercrime**, Anotada e Comentada, Coimbra Editora, grupo Wolters Kluwer, Portugal, 2010. ISBN: 978-972-32-1906-7.

VERDELHO, Pedro, **Cibercrime e Segurança Informática**, in Polícia e Justiça, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n. °6, julho-dezembro 2005.
VERDELHO, Pedro; BRAVO, Rogério (*et. al.*), **Leis do Cibercrime**, Vol. I, CENTROATLANTICO.PT, Portugal, 2003. ISBN: 972-8426-69-0.

MONOGRAFIA COMPLETA
- SANTOS, Ana Felícia Canilho - **O Cibercrime: Desafios e Respostas do Direito**, Lisboa: Universidade Autónoma de Lisboa, abril 2016. Tese de Mestrado em Direito. [Em linha]. Disponível em: https://repositorio.ual.pt/handle/11144/2640 .

Legislação Nacional e Internacional:

CARTA Direitos Fundamentais da União Europeia. **Jornal Oficial da União Europeia.** [Em linha]. (7.6.2016). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR (última consult. 12 mar.2023).

CONSTITUIÇÃO da República Portuguesa, Ed.: Almedina. 8ª edição: reimpressão 2022. ISBN: 978-989-400-772-2.

CONVENÇÃO Europeia dos Direitos Humanos. **Jornal Oficial da União Europeia.** [Em linha]. (Roma, 4.11.1950). Disponível em: https://www.echr.coe.int/documents/convention_por.pdf (última consult. 12 mar.2023).

CONVENÇÃO Nº. 108, 1981. Protocolos 2001 e 2018, do Parlamento Europeu. **Jornal Oficial da União Europeia.** [Em linha]. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf

DIRETIVA ePrivacy 2002/58, 12 de julho, *relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas* (Directiva relativa à privacidade e às comunicações electrónicas). (Lei original dos cookies). **Jornal Oficial das Comunidades Europeias.** [Em linha]. (31.7.2002). Disponível em:https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_pt.pdf

DIRETIVA (UE) 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à *proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados*, e que revoga a Decisão-Quadro

2008/977/JAI do Conselho. **Jornal Oficial da União Europeia.** [Em linha]. (4.5.2016.) Disponível em:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=PT

DIRETIVA (UE) 2016/681, do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave. **Jornal Oficial da União Europeia.** [Em linha]. (4.5.2016). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0681&from=FR

ESTRATÉGIA da UE para a Cibersegurança: um ciberespaço aberto, seguro e protegido Resolução do Parlamento Europeu, de 12 de setembro de 2013, sobre a estratégia da União Europeia para a Cibersegurança: um ciberespaço aberto, seguro e protegido (2013/2606(RSP)), (2016/C 093/16). **Jornal Oficial da União Europeia.** [em linha]. (9.3.2016). Disponível em:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013IP0376&qid=1590705521117&from=EN (última consult. 12 mar.2023).

LEI n.º 10/91, de 29 de abril de 1991, referente à Lei da Proteção de Dados Pessoais face à Informática, Diário da República, I Série A, n.º 98, 29.4.1991, alterada pela Lei n.º 28/94, de 29 de agosto.

LEI n.º 109/91, de 17 de agosto, aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, Diário da República, I Série A, n. º188, de 17.8.1991.

LEI n.º 67/98, de 26 de outubro, referente à Lei da Proteção de Dados Pessoais e à Livre Circulação desses dados, transpõe para a ordem jurídica portuguesa a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

RECOMMENDATION of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) [C (80)58/FINAL, as amended on 11 July 2013 by C (2013)79]. [Em linha]. (11.7.2013). Disponível em: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf .

REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva

95/46/CE (Regulamento Geral sobre a Proteção de Dados**). Jornal Oficial da União Europeia**. [Em linha]. (4.5.2016). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679

REGULAMENTO (UE) 2018/1725 DO PARLAMENTO EUROPEU E DO CONSELHO de 23 de outubro de 2018, *relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados*, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n. º1247/2002/CE. **Jornal Oficial da União Europeia** [Em linha]. (21.11.2018). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R1725&from=PT

RESOLUÇÃO do Parlamento Europeu, de 12 de setembro de 2013, sobre a agenda digital para o crescimento, a mobilidade e o emprego: passar a uma velocidade superior (2013/2593(RSP)). (2016/C 093/17). **Jornal Oficial da União Europeia.** [Em linha]. (4.5.2016). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013IP0376&qid=1590705521117&from=EN

TRATADO da União Europeia, (versão consolidada). **Jornal Oficial da União Europeia.** (7.6.2016). [Em linha]. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF

TRATADO sobre o Funcionamento da União Europeia (versão consolidada). **Jornal Oficial da União Europeia.** (26.10.2012). [Em linha]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN

Jurisprudência:

ACÓRDÃO do Tribunal de Justiça nos processos apensos C-793/19 | SpaceNet e C-794/19 | Telekom, Deutschland. COMUNICADO DE IMPRENSA 156/22. Luxemburgo. [Em linha]. (20.9.2022). Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220156pt.pdf (consult.1 fev.2023).

ACÓRDÃO do Tribunal de Justiça (Grande Secção) de 9 de março de 2010, Processo C-518/07: — Comissão Europeia/República Federal da Alemanha (Incumprimento de Estado — Diretiva 95/46/CE — Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados — Artigo 28º, nº 1 — Autoridades nacionais de controlo — Independência — Tutela administrativa exercida sobre essas autoridades). [Em linha]. Disponível em: https://eur-lex.europa.eu/legal-

content/PT/TXT/PDF/?uri=CELEX:62007CA0518&qid=1680022484676&from=PT (consult.1 fev.2023).
Nota prática n.º 2/2013, 3 de abril de 2013, "A obtenção do endereço IP – súmula da jurisprudência recente", Procuradoria-Geral da República – Gabinete Cibercrime.

Internet:
ARAÚJO, Sara**, Observatório sobre Crises e Alternativas,** Centro de Estudos Sociais da Universidade de Coimbra. [Em linha]. Disponível em:

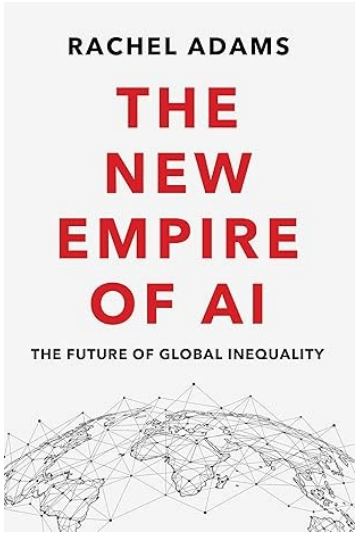
https://www.ces.uc.pt/observatorios/crisalt/index.php?id=6522&id_lingua=1&pag=7868

Comissão Europeia. Proteção de Dados - **Regras melhores para as pequenas empresas**. [Em linha]. Disponível em: https://ec.europa.eu/justice/smedataprotect/index_pt.htm (última consult.12 mar.2023).
Guía adaptación de la LOPD a LOPDGDD en 2021, [Em linha]. Disponível em: https://ayudaleyprotecciondatos.es/lopdgdd/ (última consult.10 mar.2023).

Invisibly- "How Much is Your Data Worth? The Complete Breakdown for 2021" [Em linha]. (13.7.2023). Disponível em: https://www.invisibly.com/learn-blog/how-much-is-data-worth/
PROTEÇÃO dos Dados Pessoais, do Parlamento Europeu. [Em linha]. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf

Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) [C (80)58/FINAL, as amended on 11 July 2013 by C (2013)79]. [Em linha]. Disponível em: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

IV Recensões



Rachel Adams, "The New Empire of AI", Polity Press, UK, 2025

Alexandre Sousa Pinheiro [386]

O recente trabalho de Rachel Adams, que trazemos para uma breve recensão, desenvolve o papel da inteligência artificial num contexto global em que se discute o papel da igualdade entre Estados e blocos políticos, concluindo a autora no sentido do aprofundamento das diferenças entre o norte e África, bem coo o sul profundo.

A autora funda a necessidade do livro, nomeadamente, nas denúncias e Edward Snowden e nas atividades da Cambridge Analytica, nas eleições estadunidenses de 2018.

Assim, os desenvolvimentos conseguidos através das novas ferramentas tecnológicas não abrangem a humanidade, mas apenas a sua dimensão mais rica e desenvolvida. Faz-se referência a Estados desenvolvidos e a Estados e territórios essencialmente carentes de tecnologia e de bens materiais, para proceder à distinção entre produtores de matérias primas como o cobalto e o lítio e produtores e tecnologia com base nesses elementos.

Para além desta componente global, a autora adverte para os riscos de construção e, África, essencialmente, de algoritmos viciados – *biased* – compatíveis com uma cultura em que os fatores coloniais e de cariz imperial podem afetar pessoas negras ou racializadas com base em elementos que afetam o princípio da

386 Pós-Doutorada na área da Propriedade Intelectual, Universidade Nova de Lisboa. Doutorada em Direito na Especialidade em Ciências Jurídicas e Políticas pela Universidade Autónoma de Lisboa (UAL) e Programa Doutoral em Ciência Política na especialidade de políticas públicas, Universidade Católica Portuguesa. Bolseira da Fundação Gulbenkian na Universidade de Oxford, St Antony's College. Curriculum vitae: Ciência ID: 711B-87B9-6826. ORCID ID: https://orcid.org/0000-0001-6925-1877.

igualdade – na sua dimensão jurídica, contribuindo para a desigualdade – *inequality* – social.

Aceitando os LLM como exemplo e verificando o modo como os dados são treinados num processo de *machine learning*, conclui-se que a digitalização de *nondominant languages* contribui para um universo em que a inteligência artificial vai contribuir para maiores afastamentos do que para a difusão dos méritos tecnológicos de um modo global.

A autora refere que o mesmo ocorrerá em pequenos estados, como idiomas pouco representativos, por exemplo no caso europeu.

Assentando nos riscos citados, a autora desenvolve as possibilidades de resolução dos citados problemas com base numa construção da inteligência artificial baseada na ética e na regulação necessária para obvias à desigualdade quer geográfica, quer conceitual.

No quadro dos riscos básicos causados por uma utilização indevida da inteligência artificial a autora integra a privacidade, em especial comunicações privadas, dada a necessidade de informação que deve ser recolhida para a construção de modelos de aprendizagem.

Universidade Europeia