CYBERLAW

BY CIJIC

DIREITO: A PENSAR TECNOLOGICAMENTE

EDIÇÃO N.º XIII

Junho 2025

CIJIC
Centro de Investigação Jurídica do Ciberespaço
da Faculdade de Direito de Lisboa

FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA

Iuris
Instituto de
Investigação
Interdisciplinar

CYBERLAW

BY CIJIC

EDIÇÃO N.º XIII – JUNHO DE 2025

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CYBERLAW

BY CIJIC

DIRETOR DA REVISTA: NUNO TEIXEIRA CASTRO

EDITORIAL: AFONSO DE FREITAS DANTAS – MARGARIDA FERREIRA - EUGÉNIO ALVES DA SILVA

COMISSÃO CIENTÍFICA DA REVISTA:

- ALFONSO GALAN MUÑOZ

- ANGELO VIGLIANISI FERRARO

- ANTÓNIO R. MOREIRA

- DANIEL FREIRE E ALMEIDA

- ELLEN WESSELINGH

- FRANCISCO MUÑOZ CONDE

- MANUEL DAVID MASSENO

- MARCO ANTÓNIO MARQUES DA SILVA

- MARCOS WACHOWICZ

- ÓSCAR R. PUCCINELLI

- RAQUEL A. BRÍZIDA CASTRO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

CYBERLAW

BY CIJIC

EDIÇÃO N.º XIII – JUNHO DE 2025

ÍNDICE

NOTAS SOBRE A XIII EDIÇÃO

PARTE I

DOUTRINA:

REGULATING LARGE LANGUAGE MODELS (LLMS) UNDER THE EU AI ACT AND THE GDPR

– CHRISTOS PHIDAS/DIMITRIOS KOSMOPOULOS/ GEORGIOS THOMOPOULOS/ IOANNIS IGLEZAKIS/ PANAGIOTA KIORTSI/

THE ROLE OF ANONYMISATION AND PSEUDONYMISATION ON GDPR COMPLIANCE

- SANDRO SANDRI

A DIPLOMACIA E OS SEMICONDUTORES NO CAMINHO DA GEOPOLÍTICA DO CIBERESPAÇO

- HÉLDER FIALHO JESUS

DA SEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS PELO PODER JUDICIAL EM PORTUGAL E NO BRASIL

- MANUEL DAVID MASSENO

OS DIREITOS FUNDAMENTAIS NA INTERNET: UMA NOVA ERA DE CONSTITUCIONALISMO DIGITAL

- DIANA CAMÕES

PARTE II

M.S.I.D.C.

RESPONSABILIDADE CIVIL NA INTELIGÊNCIA ARTIFICIAL - UMA ANÁLISE DA LEGISLAÇÃO EXISTENTE

- CRISTINA REIS HENRIQUES

SOFTWARE LIVRE E DIREITOS FUNDAMENTAIS

- ADRIANO ROBERTO PINTO

METADADOS: DESAFIOS DE PRIVACIDADE E SEGURANÇA NO CONTEXTO JURÍDICO E TECNOLÓGICO

- JOÃO MANUEL MARQUES LUCAS

SEGURANÇA DE INFORMAÇÃO NAS ORGANIZAÇÕES: A IMPORTÂNCIA DA FORMAÇÃO DOS COLABORADORES

- ANA CATARINA TAVARES FARINHAS

GESTÃO DE VULNERABILIDADES EM SISTEMAS DE INFORMAÇÃO

NAS ORGANIZAÇÕES PORTUGUESAS

- MARTA MONTEIRO FERREIRA

PARTE III

2030: *THE UNFOLDING CONVERSATION - BEYOND THE SCRIPT* - A BUSCA POR UMA CONEXÃO HUMANA AUTÊNTICA NO FUTURO.

JUST THE HUMAN IN THE LOOP: WORK, WORTH AND THE ALGORITHMIC ECONOMY OF 2030

- MARCIA NARINE WELDON

THE AI ERA: CHARTING A DIGITAL CONSTITUTIONAL PACT FOR EVOLUTION BY 2030

- RAQUEL BRÍZIDA CASTRO

MORE THAN MONEY: HUMAN STORIES BEHIND CURRENCY EXCHANGE

- RACHEL CANALES

CYBERLAW

BY CIJIC

NOTAS SOBRE A XIII EDIÇÃO:

Recuperando a matriz da sociedade em rede de Castells, a Inteligência Artificial (IA), e particularmente os grandes modelos de linguagem (LLMs)[1], têm vindo a revolucionar a forma como interagimos com a informação. E uns com os outros[2]. Há todo um movimento, um novo ecossistema, que se vai propagando pelas sociedades ocidentais. Com a sua capacidade computacional crescente, gerando respostas intrincadas (embora nem sempre precisas)[3] e *arrebatadoras*[4], todavia, não se estende a todos nem de forma

1 Sem olvidar que a emergência de sistemas cada vez mais autónomos, os *Agentics*, representa uma nova fronteira na evolução da IA.

2 Por exemplo, ganha tracção o conceito de *Singularidade*, popularizado por Ray Kurzweil em 2005 em «*The Singularity Is Near*» e revisitado em 2024 em «*The Singularity Is Nearer: When We Merge with AI*». Esta *Singularidade* reaparece-nos como um dos horizontes mais discutidos e quiçá transformadores para o futuro da nossa existência humana. Kurzweil insiste que o crescimento exponencial da inteligência artificial, da biotecnologia e da nanotecnologia acabará por nos conduzir a esse ponto de inflexão *singular* onde o ritmo da mudança tecnológica será tão acelerado e o seu impacto tão profundo que a vida humana, como hoje a conhecemos, será irreversivelmente redefinida pela fusão íntima entre a nossa biologia e artificialidade da máquina.

3 Ao aprofundarmos um pouco o funcionamento interno da essência dos modelos de linguagem, percebemos que, entre a autorregressão e o *Chain-of-Thought* (CoT) *prompting*, a sua *cadeia de pensamento* é, fundamentalmente, matemática sofisticada a operar em função de cada utilizador individual. Sem entrar na discussão mais abrangente sobre a inclusividade, no acesso a estas ferramentas, impõe-se, contudo, destacar o potencial de disparidade que o *prompt engineering* é capaz de provocar. Apesar de toda a *sofisticação técnica*, existem desafios práticos e éticos que reclamam (mais) atenção de todos nós.

4 Num momento decisivo para as gerações mais novas, onde parece sobressair algum laxismo e "facilitismo" *prompted* pela IA, o segredo esta(rá) na capacidade de adaptação. Dos estudantes, dos Professores, das Escolas, das Universidades. Mais do que proibir, seria (muito mais) profícuo *ensinar-a-perceber-para-e-como-usar*. Até porque: «*While technologies will continue to evolve, essential skills such as reading, writing, and critical thinking will remain foundational. Therefore, students must be literate to*

equitativa. Pelo contrário. A disparidade de acesso e a ausência/impossibilidade de condições de fruição plenas, configuram a infoexclusão, representando um desafio social acrescido. Apesar destes *recorrentes* obstáculos, os LLMs e a IA prometem ter chegado para ficar, redefinindo o nosso quotidiano e as nossas sociedades.

O nosso percurso doutrinal na presente edição da *Cyberlaw by Cijic* foca-se, precisamente, na intrincada intersecção entre a inovação dos LLMs e o rigor da regulamentação europeia. Vasta. Por exemplo, entre as implicações legais do Regulamento (UE) 2024/1689 - o EU AI Act - e o Regulamento Geral de Protecção de Dados (RGPD). Questões jurídico-constitucionais, questões de transparência, questões éticas, persistem e assombram-nos, particularmente em matérias de objectividade no tratamento de dados pessoais. Como regular? Como proteger? O que regular? O que proteger?

Historicamente, a anonimização foi-nos sugerida como uma solução robusta para a privacidade. Porém, a sua aplicabilidade prática e a persistente ameaça de re-identificação, revelaram-nos algumas das suas limitações. O legislador europeu, tentando acompanhar a velocidade do ecossistema, passou a optar por uma abordagem baseada no risco. As lições de Beck, sempre fundamentais, ensina(ra)m-nos a melhor compreender o mundo. Assim, uma protecção de dados eficaz, o uso de ferramentas e de *software*, na era da IA, intima-nos a estratégias flexíveis e orientadas ao risco, sublinhando a importância da anonimização *de facto* e da implementação robusta da pseudonimização. Este é um caminho (desejado) para salvaguardar a privacidade, o segredo, os direitos fundamentais e a conformidade. Uma sociedade de cidadãos vítreos não é democrática.

Embora intuamos o capitalismo de vigilância e o Estado de vigilância, na verdade não compreendemos plenamente nem um nem outro, tal como a IA, os LLMs, os potenciais do seu uso ou os seus riscos. Para colmatar o hiato entre os quadros legais vigentes e as complexas realidades (também) do tratamento de dados, salvaguardando simultaneamente os direitos fundamentais, cremos que o legislador europeu deve (continuar a) ser o farol e impulsionador da inovação responsável. Sim, inovação

---

effectively process information and use AI intelligently.» - Andrew Woon, 11 June 2025, «Rethinking Exams in the Age of AI: Should We Abandon Them Completely?» - @ https://www.hepi.ac.uk/2025/06/11/rethinking-exams-in-the-age-of-ai-should-we-abandon-them-completely/

responsável. As pessoas são o centro de tudo. E aqui impõe-se a questão fundamental: Palavras temos[5]. Soberania procura-se. Assim como acções decisivas.

Ainda que num plano paralelo, no complexo panorama da *slowbalization* e *fragmentegration*, a indústria dos semicondutores emerge como ponto nevrálgico, exemplificando a intrincada interacção entre a geopolítica, a economia e a tecnologia. Uma efervescente competição entre potências como os EUA e a China impulsiona uma *nova ordem mundial* baseada no *techno-nationalism*, onde governos recorrem à diplomacia agressiva, barreiras comerciais e políticas industriais proteccionistas para moldar cadeias de abastecimento globalizadas. Esta rivalidade manifesta-se e projecta-se (também) no ciberespaço como um novo *campo de batalha*, que exacerba a *fragmentação da Rede* - qual Torre de Babel - ameaçando soberanias e os direitos fundamentais individuais. Neste volátil cenário, quase esquizofrénico dum "*nós contra eles*", a União Europeia enfrenta um desafio musculado de agência. Um desafio para alcançar a sua própria autonomia e soberanias digitais, de competitividade, de crescimento. Mas sem abalar as nossas fundações de promoção da vida e da condição humana. Um desafio de onde deve emergir as tão necessárias acções decisivas, suportado numa estratégia holística, concertada, colaborante, que, além da salvaguarda das suas pessoas e da nossa economia, promova uma sustentabilidade e inovação responsáveis face a ameaças e oportunidades futuras.

A complexidade da regulação da IA e as dinâmicas geopolíticas também mergulham na forma como os dados pessoais são geridos. Seja em sectores específicos e sensíveis ou não. Na verdade, a discussão sobre a IA e a geopolítica dos semicondutores, e que sublinha a necessidade duma estratégia europeia coesa e cooperante, holística, para a autonomia digital, ressoa directamente com as particularidades da aplicação da protecção de dados no terreno. Sob premissas desta particular granularidade, nesta nova edição, somos levados a analisar os regimes de tratamento de dados pessoais pelo poder judicial, tanto sob o *Regulamento Geral sobre a Protecção de Dados* (RGPD) da União Europeia quanto à luz da *Lei Geral sobre Proteção de Dados Pessoais* (LGPD) brasileira. *Prima facie*, os regimes previstos para o tratamento de dados pessoais pelo poder judicial no RGPD e na LGPD, apesar das suas semelhanças superficiais, reportam divergências

5 «*The future of European competitiveness*: Report by Mario Draghi» - @: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en - A Europa pode e deve posicionar-se para liderar no cenário global da inovação, incluindo no digital e na IA, sem comprometer os nossos valores fundamentais. Temos recursos, temos pessoas, temos ferramentas. Falta-nos saber arregaçar as mangas para compreendermos as acções necessárias para transformar "palavras" em "acções" concretas.

legislativas profundas relativas à autonomia normativa e administrativa desse poder judicial, com particular ênfase no que tange à responsabilidade pela segurança no tratamento dos dados. Daí a necessidade e oportunidade desta análise detalhada e comparativa de ambos os regimes, complementando as nossas discussões que perfumam a presente edição, sobre os desafios regulatórios da era digital, bem como a macro-dinâmica da *fragmentegration* e do *techno-nationalism* e os reflexos concretos e diferenciados na harmonização e implementação dos direitos fundamentais da pessoa humana.

Muito a propósito, os desafios presentes (porque o futuro é já hoje) são tremendos. Na complexa teia e em constante mutação da sociedade em rede, a maior dificuldade reside na criação de condições propícias à adequada protecção dos direitos fundamentais das pessoas por este ecossistema pungente.

É consabido que as plataformas digitais, actuando enquanto actores privados com poderes quase ilimitáveis - pouco aptos à regulação tradicional - moldam conteúdos disponíveis *online*, percepções, comportamentos e, no fundo, acabam por contribuir - *mesmo que de forma não intencional?* – e em determinadas situações, para a violação dos direitos fundamentais.

A evolução jurídico-constitucional tem-nos revelado gerações distintas de direitos fundamentais. No entanto, certos permanecem imutáveis e basilares e com enorme impacto no contexto digital. É o caso da liberdade de expressão. Mas não só. Com a perda do *domínio*, do exclusivo, dos meios de comunicação tradicionais e à proliferação de *informações* pelos próprios utilizadores nas novas Ágoras, esses fóruns públicos digitais, a forma como a liberdade de expressão é perspectivada e respeitada reclama uma actuação ponderada.

Mas, e a censura?

Sem receios. No Direito, não há absolutismo, mas sim ponderação, critério e proporcionalidade, princípios essenciais para discriminar eventuais restrições[6].

---

6 É adequada? É necessária? É proporcional?
Ou seja, «*O princípio da proporcionalidade desdobra-se em três subprincípios: i) Princípio da adequação (as medidas restritivas de direitos, liberdades e garantias devem revelar-se como um meio para a prossecução dos fins visados, com salvaguarda de outros direitos ou bens constitucionalmente protegidos); ii) Princípio da exigibilidade (essas medidas restritivas têm de ser exigidas para alcançar os fins em vista, por o legislador não dispor de outros meios menos restritivos para alcançar o mesmo desiderato); iii) Princípio da justa medida ou proporcionalidade em sentido estrito (não poderão adoptar-se medidas excessivas, desproporcionadas para alcançar os fins pretendidos).*» - por exemplo, Acórdão do Tribunal Constitucional n° 632/2008 de 23-12-2008.

A garantia da tutela efectiva dos direitos fundamentais exige uma constante adaptação à realidade multifacetada quer da sociedade quer do ciberespaço. Uma que equilibre a inovação com a defesa intransigente dos pilares democráticos e da dignidade humana. Também no digital. Sim. As plataformas iteram. Replicam de forma instantânea. Acrítica. Amoral. Maquinal. Alguns aproveitam este meio. Dele fazendo uso para fins próprios. Egoístas, como qualquer natural e insatisfeito humano. Fins não totalmente compreendidos. Mas isto não tem de ser necessariamente assim[7].

Uma cidadania atenta e participativa pode contrariar este seguidismo de agência, impulsionado por *clercs* (intelectuais, influenciadores e *brainroters*), que vai prosperando neste *abusus non tollit usum* ambiente. As novas formas de comunicação e a actuação de tais agentes contribui decisivamente para a intensificação da polarização, da desinformação e da fragilidade das democracias modernas. Como Anne Applebaum (2020) de forma previdente nos alertara sobre tal frenético ambiente e de corrosão social tolerado por *political systems with radically simple beliefs* (that) *are inherently appealing, especially when they benefit the loyal to the exclusion of everyone else*[8].

Mas, e quem protege e promove os direitos, liberdades e garantias fundamentais de *everyone else*?

Audi alteram partem[9]. As trevas do seguidismo acrítico podem (e devem) ser contrariadas.

É aqui que tem de resistir o farol. Que nos ilumine. É por aqui que a União Europeia tem e deve continuar a apostar, e bem, na regulação.

As críticas são constantes. Quase sempre não de forma construtiva. Um entrave, apregoam. A regulação desnecessária e obliterante. Embora na sua execução a regulação, sim, acabe por *dificultar* a inovação *disruptiva*, só mentes pouco conscientes poderão afirmar que a posição da U.E. é um tal (tamanho) entrave a um *admirável novo mundo*. De todo. E a *fórmula do objecto*, postulado Kantiano, enquanto lição primacial, explica de forma lógica mas muito simples tudo aquilo que não pode ser feito: a objectificação

---

7 Até porque, por exemplo, Anne Applebaum ensina-nos uma forma de contrariar esse *design* algorítmico das plataformas digitais, que amplifica a polarização e a desinformação. Isto passa pela reconfiguração fundamental das redes sociais, pelo fortalecimento das instituições democráticas para combater a corrosão social daí decorrente e, fundamentalmente, pelo empoderamento duma cidadania atenta e consciente. Mais em: https://www.anneapplebaum.com/2021/03/08/the-internet-doesnt-have-to-be-awful/ (último acesso Junho 2025)

8 Mais em Applebaum, Anne - *Twilight of Democracy: The Seductive Lure of Authoritarianism*, Doubleday, 2020.

9 *Idem*.

da pessoa humana. As pessoas são o fim de tudo. Não um meio para se atingir um dado fim. Não um objecto duma qualquer finalidade.

Assente nestas premissas, o caminho da abordagem regulatória, e assim a U.E. resista à *pulsão de agência de uma qualquer nova ordem mundial*, está já pressuposta em alguns instrumentos fundamentais tais como o RGPD, o Regulamento dos Serviços Digitais (DSA) e o Regulamento de Inteligência Artificial (EU AI Act), complementados pelo Regulamento dos Mercados Digitais (DMA). Poderemos até já vislumbrar uma nova vaga de direitos fundamentais, adaptada aos hercúleos desafios do presente. O direito de acesso à Internet, o direito à explicabilidade e/ou o direito à protecção das decisões algorítmicas, são apenas alguns exemplos que começam a furar a malha. Assim consigamos garantir, de forma colaborante e cooperante, uma harmonia europeia entre os diversos interesses em confronto, assegurando a protecção dos direitos fundamentais e o bom funcionamento do ecossistema, sem nunca abdicar da dignidade da pessoa humana como seu pilar fundacional. Os outros, seguir-nos-ão[10].

Para complementar a nossa investida doutrinal da presente edição, no campo das investigações levadas a cabo no Mestrado Bolonha em Segurança de Informação e Direito no Ciberespaço[11] , e apesar dos avanços regulatórios da União Europeia que aqui já fomos dando conta, a *leges artis* actual (ainda) revela insuficiências. Desde logo na camada de protecção dos lesados por danos causados pela Inteligência Artificial, seja em transacções de bens e produtos, questões financeiras ou protecção de dados. Esta lacuna na atribuição de responsabilidades e a consequente insegurança jurídica, onera-nos a uma acção. E que deve ser colmatada. A aplicação da responsabilidade civil à IA enfrenta desafios notáveis, sabemos. A opacidade dos algoritmos, as decisões autónomas e as complexas interacções entre diferentes ordens jurídicas, e em particular o nexo de causalidade, tornam a protecção efetiva das pessoas, potenciais vítimas, uma agreste tarefa. Reclamamos, portanto, uma maior harmonização legislativa que equilibre os riscos da IA com a segurança jurídica e a inovação, visando construir uma sociedade mais equitativa e justa na era tecnológica, mas onde a dignidade da pessoa humana permaneça um pilar inabalável.

---

10 Por exemplo, na Dinamarca há uma proposta arrojada, no combate a *deepfakes*, na vanguarda da protecção da identidade digital. É um tema que merece o devido destaque e acompanhamento. Mais em: https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence - (último acesso 27Jun2025)

11 https://fenix.tecnico.ulisboa.pt/cursos/msidc

Por todo este complexo ecossistema, as tecnologias de informação, embora indispensáveis para promover e salvaguardar direitos fundamentais, são frequentemente afrontadas como uma panaceia. Tendem a ser tratadas sob aspetos meramente comerciais e de segurança, por vezes encapsuladas em conformidades à protecção de dados, mas em detrimento de questões socioambientais e de outros direitos fundamentais. É sob esta premissa que emergem duas importantes ferramentas para a promoção destes direitos: o *Software* Livre e as Licenças *Copyleft*.

O crescimento do *Software* Livre é lento devido às pressões de *lobbies* e monopólios de grandes empresas dominantes no sector tecnológico. Sabemos. Fabricantes de *hardware* e *software* tendem a manter as especificações dos seus produtos e os códigos fechados, dificultando a implementação de *drivers*, bibliotecas e dependências livres, e limitando a compatibilidade entre dispositivos e sistemas de fabricantes distintos. Este regime legado perpetua e estimula o monopólio ou o oligopólio.

Em contraste, o *Software* Livre e as Licenças *Copyleft* oferecem uma alternativa. Além de contrariarem esta lógica *dominadora*, possuem potencial enorme para, entre outras, combater as alterações climáticas, ajudando a impedir a obsolescência programada. Quem diria. A obsolescência programada enquanto prática, leva ao descarte prematuro de dispositivos em boas condições, estimula a produção de lixo, poluição e o uso desenfreado de recursos naturais. E tudo isto é reconhecidamente insustentável.

Também neste cenário, a União Europeia deve actuar de forma decisiva, resistindo às *pressões dominantes* de mercado, promovendo activamente modelos abertos como o *Software* Livre, essenciais para garantir um futuro digital centrado na dignidade humana, mais equitativo e inclusivo, mais sustentável e amigo do ambiente. E de todos nós.

Além disto, e como temos vindo a tentar elucidar por todo este desafiante ecossistema, onde a inovação tecnológica se cruza com dinâmicas geopolíticas e com a redefinição dos nossos direitos, a questão da privacidade dos cidadãos e da segurança interna adquire uma centralidade crescente, particularmente no contexto dos metadados. Os desafios impostos pela Diretiva 2006/24/CE e pela jurisprudência subsequente, destacando-se aqui o Acórdão do Tribunal Constitucional n.º 268/2022, ilustram a complexidade de tais tensões.

Neste conspecto, princípios como o sigilo das comunicações e a sua excepção restrita ao processo criminal com autorização judicial para suspeitos determinados, o "*problema do cruzamento de dados*", e a primazia do Direito como fonte fundamental - alinhada à defesa da dignidade humana como um *fim em si mesmo* - proclamam-se baluartes.

O equilíbrio é delicado. Assim também na gestão da informação que geramos e partilhamos, reside, portanto, um dos maiores desafios do presente. A forma como os metadados são conservados, acedidos, tratados e explorados transforma-se e revela-se num barómetro da saúde das nossas democracias e num teste contínuo à capacidade do Direito para salvaguardar a dignidade da pessoa humana perante, também, o próprio Estado.

Ademais, a defesa do estado de direito democrático, das suas pessoas, dos seus valores não é uma responsabilidade *tout court* apenas do Estado ou de entidades isoladas. Esta é uma incumbência difusa, individual mas também colectiva, uma *defesa em profundidade* em que a soma das acções duma cidadania activa, consciente e responsável, zela e promove a ordem e ajuda a construir um futuro (também digital, mas não só) que respeita e promove os direitos e liberdades de todos e de cada um de nós.

Ser social acarreta responsabilidades. Esta é apenas uma das suas manifestações.

Cum granus salis, e citada a *defesa em profundidade*, importa ainda trazer à colação três aspectos fundamentais: a segurança de informação e a formação dos trabalhadores, e a gestão de vulnerabilidades.

No que concerne à segurança da informação e à formação dos trabalhadores, a transformação digital, impulsionada pela aceleração da conectividade pós-pandemia, redefiniu-nos o panorama global, o ecossistema, e, concomitantemente, expôs desafios críticos à cibersegurança. A engenharia social exponenciou-se, e ataques como *phishing* e *smishing*, subsistem como vectores primários para ameaças de maior complexidade, a exemplo do *ransomware*, impactando a segurança de todos, nos sectores público e privado. Esta persistência sublinha uma lacuna fundamental nas estratégias de defesa convencionais, realçando a necessidade duma abordagem multifacetada e de múltiplas camadas para alavancar uma protecção mais eficiente.

O factor humano continua a emergir enquanto vulnerabilidade crítica nas organizações. Contrariamente a alguns adágios populares ainda bem arreigados em algumas cadeias de topo de organizações, a tecnologia por si só é insuficiente. A gestão eficaz da segurança da informação transcende a dimensão puramente tecnológica. Os trabalhadores são, outrossim, a primeira e mais decisiva linha de defesa. A sua capacitação contínua é, não um mero complemento mas, um pilar fundamental para mitigar riscos. A implementação de estratégias de formação diversificadas, incluindo vídeos, *gaming*, exercícios *tabletop*, sessões presenciais, entre outros, tem vindo a demonstrar eficácia comprovada na redução

da susceptibilidade a ataques e na construção duma cultura organizacional proactiva de segurança.

Paralelamente, a gestão de vulnerabilidades assume outro dos papéis fundamentais. Este processo não se limita à mitigação de riscos. Ele transcende a mera ferramenta de protecção. É (mais um) factor estratégico e vital para a resiliência das organizações. Precisamente, numa visão de defesa em profundidade.

A gestão de vulnerabilidades envolve a identificação, priorização e mitigação de falhas de segurança, apoiada por diversas metodologias e *frameworks* que visam estruturar e padronizar as abordagens. Metodologias como o ciclo de vida de gestão de vulnerabilidades (alinhado ao PDCA), a abordagem baseada no risco e a metodologia de testes (*penetration testing* e *vulnerability scanning*) são amplamente adoptadas para garantir uma mitigação eficiente e consistente. *Frameworks* reconhecidas como NIST Cybersecurity Framework (CSF), ISO/IEC 27001/27002, CIS Controls e MITRE ATT&CK fornecem guias, orientações e processos práticos para a implementação de sistemas robustos de gestão da segurança da informação. Entre outros, veja-se, por exemplo, o ataque de *ransomware* sofrido pela EDP e que ilustra vividamente as severas consequências da exploração de vulnerabilidades não corrigidas.

Na preparação e na antecipação está o ganho. Como nos elos duma corrente, exige-se uma abordagem holística e integrada, que combine infraestruturas resilientes, formação contínua, pertença e responsabilidade, eficiente gestão de riscos e uma cultura engajada de segurança: uma (verdadeira) *defesa em profundidade*. Somente através desta sinergia positiva as organizações poderão, de forma sustentada, salvaguardar os seus activos mais valiosos: a informação e, intrinsecamente, as suas pessoas e que a gerem, face aos desafios do ciberespaço.

Por fim, e *en passant* sobre esta nossa nova edição, fomos desvelando um ecossistema digital de complexidades multifacetadas, desde o impacto da IA e a geopolítica dos semicondutores, passando pela intrincada teia da protecção de dados e a responsabilidade civil da IA, até à urgência da cibersegurança e ao potencial libertador do *Software* Livre. Percorremos os desafios impostos por modelos centralizados e a necessidade imperativa duma acção regulatória por parte da U.E., sempre com a dignidade da pessoa humana e os direitos fundamentais como nosso pilar fundacional e intransigente. Sublinhamos que a defesa da democracia e dos seus valores não é uma incumbência exclusiva doutros, mas uma responsabilidade difusa e colectiva, uma *defesa em profundidade* que exige uma cidadania activa, consciente e responsável.

Antes de terminar, expressamos um sentido agradecimento a todos aqueles que têm participado activamente na consolidação deste projecto. São (já) nove anos de história, treze edições publicadas, e a certeza de que muito mais há por fazer(mos). A todos, sem excepção, o nosso mais sentido "Muito Obrigado!". A todos.

Este percurso conjunto tem sido um verdadeiro testemunho de todo o potencial humano para um crescimento contínuo: um exemplo vivo de colaboração, cooperação, partilha e participação dedicada. É na soma de todas estas contribuições que reside a força e a capacidade de superação que nos permite continuar focados no futuro.

Assim e depois de todo este percurso na presente edição, finalizamos procurando ir além do roteiro esperado, desafiando narrativas pré-estabelecidas e elucidando os diálogos não escritos dum futuro que se nos revela e acelera a cada dia. Considerando a natureza intrínseca e vital da necessidade humana pelo outro e o nosso ideal humano de interdependência, construção conjunta, colaboração, cooperação, partilha, pertença e coexistência, é para um futuro dinâmico e evolutivo - que nos desafia a pensar sobre quem somos hoje, a nossa natureza humana amanhã e como nos reencontraremos - que decidimos projectar a nossa nova utilidade. A nossa edição deste ano termina com a abertura dum marcador novo: «2030: *THE UNFOLDING CONVERSATION - BEYOND THE SCRIPT*».

Sejam todos bem-vindos à busca por uma conexão humana autêntica no futuro.

Faculdade de Direito da Universidade de Lisboa
Instituto de Investigação Interdisciplinar do Direito – IURIS
Centro Investigação Jurídica do Ciberespaço – CIJIC
Junho de 2025
Nuno Teixeira Castro

CYBERLAW

BY CIJIC

DOUTRINA

CYBERLAW

BY CIJIC

REGULATING LARGE LANGUAGE MODELS (LLMS) UNDER THE EU AI ACT AND THE GDPR

CHRISTOS PHIDAS/DIMITRIOS KOSMOPOULOS/GEORGIOS THOMOPOULOS/ IOANNIS IGLEZAKIS/ PANAGIOTA KIORTSI/

ABSTRACT:

This paper examines the legal issues arising from the regulation of Large Language Models (LLMs) under Regulation (EU) 2024/1689, the EU AI ACT and the General Data Protection Regulation (GDPR). It highlights that, with advances in technology, LLMs are continuously improving, enabling them to generate more accurate and complex responses. However, ethical and transparency concerns persist regarding their use and potential societal impact, particularly in relation to privacy protection and ensuring objectivity in the processing of personal data.

KEYWORDS: *LARGE LANGUAGE MODELS (LLMS); EU AI ACT; GENERAL DATA PROTECTION REGULATION (GDPR); REGULATION; ETHICS; TRANSPARENCY*

I. INTRODUCTION

Interactive AI models are advanced applications that continuously learn and refine their responses through iterative training processes incorporating human feedback, enabling them to improve accuracy, adaptability, and contextual understanding over time. The purpose of training is to enable AI models to understand natural language in a way that allows them to generate text, images, and code to answer questions, mimicking human communication. The use of AI models is rapidly expanding into an increasing number of applications with a global reach, even as this is being written[1].

These applications cover a wide range of areas such as customer service, education, healthcare, and legal support. They are also used in content creation, process automation, and big data analysis. With advances in technology, the capabilities of interactive models are constantly improving, allowing them to produce more accurate and complex answers. However, ethical and transparency issues remain regarding the way they are used and the impact they may have on society, especially regarding the protection of privacy and ensuring objectivity in the processing of personal data.

Interactive or large language models, such as ChatGPT, GEMINI, LLama, and ORCA, among others, are generative models trained through supervised learning using datasets of questions and answers. Then, as a standard practice, a reward model is trained to evaluate the responses of the generative model, optimizing its performance through reinforcement learning.[1] This evaluation system enables the refinement of the generative model via reinforcement learning, where responses are gradually improved through interaction with human feedback

II. TECHNICAL CHARACTERISTICS OF LLMS

Large language models can also be trained on a vast collection of texts to recognize and predict word sequences. This enables them to perform natural language

---

1 See *W. X. Zhao*, A Survey of Large Language Models, https://doi.org/10.48550/arXiv.2303.18223, ChatGPT for good? On opportunities and challenges of large language models for education, *E. Kasnec et al.i,* Learning and Individual Differences, Volume 103, 2023, 102274, ISSN 1041-6080, https://doi.org/10.1016/j.lindif.2023.102274, *T. Teubner, C.M. Flath, C. Weinhardt, et al.,* Welcome to the Era of ChatGPT, *Bus Inf Syst Eng* 65, 95–101 (2023). https://doi.org/10.1007/s12599-023-00795-x.

1 See I. Iglezakis, Interactive AI systems and their applications in law - The case of ChatGPT, Synigoros 155/2023, pp. 60-63 (in Greek).

processing.[2] Large language models are trained from a huge amount of data. Precisely because of the huge amount of data used to train such a system, concerns arise about potential violations of fundamental human rights, such as the protection of privacy and personal data, but also the violation of other legislation protecting copyright or industrial and commercial secrecy. Furthermore, the risk of incorrect, inappropriate or biased responses to the content of the response produced by the model is increasingly threatening.[3]

The phenomenon of wrong answers that the large language model may give has already become known as the "hallucinations" of large language models. This occurs in cases in which the system generates responses that either promote stereotypes, or are false, or outside of meaning and logic. The "hallucinations" may be caused by, among other things, "noise" in the training data, i.e. training the AI system in a way that creates a distorted statistical/training model.[4]

In the same context, depending on the data entered for language model training or algorithmic choices, the system may generate results that contain biases or discriminate against certain groups based on gender, social class, ethnicity, age, political beliefs, etc.[5]

The more the use of interactive AI models expands, the more the concern grows: who is responsible if, for example, the model gives the wrong answer to a question about access to work or basic benefits such as healthcare? Is the provider responsible for knowingly not taking care to train the model with scientifically based material? What if, worse, he chose to train it with data that is flawed or reinforces biases?

The research questions arising from the above concerns are whether the current legal framework can effectively protect users. If legal liabilities arise when these models are trained—intentionally or unintentionally—on incorrect or false data, who will be held responsible?

---

2 See *ibid*.

3 See Iglezakis, The law of digital economy, 2nd ed., Sakkoulas Publication, p. 210 et seq. (in Greek).

4 *L. Huang et all,* A Survey on Hallucination in Large Language Models: Principles, Taxonomy, Challenges, and Open Questions, Published in arXiv.org, 9 November 2023, DOI:10.48550/arXiv.2311.05232

5 *S. Wachter, B Mittelstadt, C Russell*, Do large language models have a legal duty to tell the truth? Royal Society Open Access, 07 August 2024, https://doi.org/10.1098/rsos.240197.

III. Legal regulation of large language models under Regulation 2024/1689

The EU Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonised rules on artificial intelligence[6] is a very important EU legislative initiative that aims to establish a common, human-centered legal framework to regulate artificial intelligence systems. [7]

Articles 51 and 52 of Regulation 2024/1689 distinguish between general-purpose AI models and general-purpose AI models with systemic risks. A general-purpose AI model is classified as having systemic risk if it meets the conditions set out in Article 52, particularly if it falls within the cases specified in the Commission Decision or if the cumulative volume of computation used for its training, measured in floating-point operations, exceeds 10^{25}.

Providers of general-purpose AI models with systemic risks are subject to the obligations set out in the Regulation, such as the preparation of model assessments and mitigation strategies for systemic risks, transparency duties, duties to report serious incidents, to take corrective measures, the obligation to protect cybersecurity and to respect human rights and intellectual property law (Article 55). Similarly, for general purpose model providers not used in a high-risk environment, the provider has an obligation to inform the user that he is communicating with a chatbot.[8]

Although the guarantees provided by the Regulation are undeniable, valid concerns have been raised about its effectiveness.[9] In particular, informing users that they are talking to an AI system that may give incorrect, biased or inappropriate answers does not actually

---

6 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj

7 Edwards, Lilian. "The EU AI Act: a summary of its significance and scope." *Artificial Intelligence (the EU AI Act)* 1 (2021): 25; Veale, Michael, and Frederik Zuiderveen Borgesius. "Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach." *Computer Law Review International* 22.4 (2021): 97-112; Laux, Johann, Sandra Wachter, and Brent Mittelstadt. "Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk." *Regulation & Governance* 18.1 (2024): 3-32; Butt, J. "Analytical study of the world's first EU Artificial Intelligence (AI) Act." *International Journal of Research Publication and Reviews* 5.3 (2024): 7343-7364.

8 *R. Diab,* Too Dangerous to Deploy? The Challenge Language Models Pose to Regulating AI in Canada and the EU, University of British Columbia Law Review, Forthcoming, January 1, 2024. Available at: SSRN: https://ssrn.com/abstract=4680927

9 *G. De Minico*, Too Many Rules or Zero Rules for the Chatgpt? BioLaw Journal – Rivista di BioDiritto, n. 2/2023, https://teseo.unitn.it/biolaw/article/view/2723/2625, διαθέσιμο σε διαδικτυακή μορφή: https://ssrn.com/abstract=4517127

offer them any help, nor does it remove the feeling of trust in the omnipotence of the chatbot.

As it has been mentioned, it is as if the water supplier has an obligation to inform the inhabitants of a town that the water contains dangerous chemicals, without being obliged to take measures to purify the water. The concern is expressed because the Regulation allows general purpose AI model providers to take certain initiatives to avoid the obligations imposed on them by the Regulation. Providers of general-purpose AI models that fall within the conditions referred to in Article 51 are free to present substantiated arguments to demonstrate that these models should not be classified as general-purpose AI models with systemic risks, even though they fulfil these conditions.[10] In this case, if the arguments are accepted, they are exempted from the transparency obligations.

In addition, providers of general purpose AI models with systemic risks, being public bodies or working with and on behalf of public bodies, have quite extensive transparency obligations, such as, for example, the obligation to register their high-risk system in the database and to enter information about it, i.e. a description of its intended purpose, a summary description of the information used by the system and its operating logic, a summary of the findings of the impact assessment, a description of the information used by the system and its operating logic, a summary of the results of the impact assessment, and a description of the system's risk assessment.[11] However, developers of high-risk AI systems in the private sector are not subject to these obligations. Consequently, there is also an unjustified lack of transparency in this case, even though the risk is real.[12]

10 Wachter, *ibid*, 699.

11 The Ethical Guidelines for Trustworthy AI focus on the issue of respecting the fundamental rights enshrined in the EU Treaties. At the same time, it recognises that an important prerequisite for the capability of systems is accuracy, i.e. the ability to make correct judgements, to correctly classify information into appropriate categories or the ability to make correct predictions, recommendations or decisions based on data or models. As the Guidelines state 'Where it is not possible to avoid occasional inaccurate predictions, it is important that the system is able to indicate how likely it is that such errors will occur. A high level of accuracy is particularly important in situations where the AI system directly affects human lives." Ethical Guidelines for Trustworthy AI, Independent High Level Expert Group on AI, Established by the European Commission, June 2018, available online ethics_guidelines_for_trustworthy_ai-el_87FCEA3A-BC42-126F-1D66D4437C34812B_60424.pdf

12 EDRi and AI coalition partners “EU’s AI Act fails to set gold standard for human rights A round-up of how the EU Artificial Intelligence (AI) Act fares against the collective demands of a broad civil society coalition that advocated for prioritizing the protection of fundamental human rights in the law”, April 3, 2024, διαθέσιμο στην ηλεκτρονική διεύθυνση https://edri.org/our-work/eu-ai-act-fails-to-set-gold-standard-for-human-rights/

IV. The provisions of the General Data Protection Regulation

In contrast to EU Regulation 2024/1689 on artificial intelligence, the General Data Protection Regulation (GDPR)[13] takes a different approach, whereby it is not left to the discretion of providers/controllers to document whether they will comply with their obligations. By way of example, according to Article 35 GDPR, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. This obligation applies to controllers, regardless of whether they are public or private bodies. In addition, Article 35 applies to general purpose AI systems, but also to general purpose AI models with systemic risks.

The General Data Protection Regulation does not leave room for providers of such applications to argue that they do not fall under Article 35, especially if the competent regulatory authorities have included the types of processing they deal with in the specific list of processing for which an impact assessment is mandatory. In addition, the impact assessment shall include an assessment as to whether the data processing is likely to result in discrimination against groups with particular social characteristics.[14]

In the same vein, Article 22 GDPR provides that the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Accordingly, the controller has an obligation to inform the data subject of the way in which data are obtained and the parameters with which they are used to obtain results from the artificial intelligence system.[15]

---

13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

14 *P. Hacker, A. Engel, M. Mauer*, Regulating ChatGPT and other Large Generative AI Models, FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, 12 Ιουλίου 2023, pp. 1112 - 1123, https://doi.org/10.1145/3593013.3594067

15 *J. Luckett*, Regulating generative AI: A pathway to ethical and responsible implementation, Journal of Computing Sciences in Colleges, International Journal on Cybernetics and Informatics (IJCI) Vol 12, No 5 October 2023, pp 80-92

V. Loopholes in the EU AI Act

Finally, concerns have been raised about the fact that the safety and security safeguards in the AI Act apply to AI systems from EU-based providers and used by users located in the EU. However, the safeguards do not cover cases where users are located outside the EU, leaving them unprotected against the risks of these systems, even if they are classified as high-risk.

Regarding the latter concern the EU, the UK and the US, recognizing the need for international partnership on AI, signed the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, which was adopted on May 17, 2024. The Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law is a pioneering international treaty aimed at ensuring that artificial intelligence (AI) systems are developed and utilized in ways that uphold fundamental human rights, democratic principles, and the rule of law.

Article 1 para. 2 provides that "Each Party shall adopt or maintain measures to ensure that activities within the life cycle of artificial intelligence systems are consistent with the obligations to protect human rights as enshrined in applicable international and domestic law".[16]

This approach, however, is problematic in terms of the content of human rights. According to the American constitutional theory of human rights, the latter are protected from encroachments by the State. They cannot be opposed to private individuals when they act in a way that violates fundamental rights, contrary to the European legal order, in which the protection of fundamental human rights is provided against infringements by either the State or private individuals.[17] Thus, a gap exists between human rights pronounced in the Framework Convention and its implementation in the States.

16 https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

17 F. Krumbein. Human Rights in the EU and the US: Social Worker v. Good Cop? Open Journal of Political Science, 7, 2017, σελ. 101-115. doi: 10.4236/ojps.2017.71008.

VI. A Research Project on the Use of an LLM in a specific area

The authors of this paper are participating in the research project titled "*Artificial Intelligence-Driven Framework and Legal Advice Tools for Phishing Prevention and Mitigation in Information Systems*" (AILA – PROJECT ID: 15440).[18]

The aim of the project is to design an interactive artificial intelligence-driven system (LLM) to provide legal advice in cases of phishing attacks to users who have fallen victim to such attacks, as well as to legal or banking institutions. The methodology of the system follows the supervised and reinforcement learning of the AI system, with feedback of legal texts.

Specifically, the AILA research project aims to implement an interdisciplinary research project that will address the following challenges: a) to formalize a new and interdisciplinary user model against phishing that will integrate human, technological and legal factors of phishing, b) to use the user model to design and develop intelligent algorithms that will allow organizations to justify their level of preparedness to address phishing attacks and make informed decisions about the susceptibility of employees and stakeholders to such attacks, thus providing groundbreaking scientific advances in phishing prevention and personalization of anti-phishing measures, c) to design and develop innovative recommendation functions that will provide personalized legal advice to organizations (based on sector factors) and end users (based on profiles), d) to demonstrate an open-source interdisciplinary anti-phishing framework that will implement prevention and mitigation algorithms, reaching Technology Readiness Level 4 (TRL4 - Technology Validated in Lab) and e) to provide validated heuristics for adapting anti-phishing methods with the aim of facilitating the transfer of scientific knowledge which will result from valid real-world case studies that will be applied to participating organizations.

18 See <https://aila.upatras.gr/>.

CYBERLAW

BY CIJIC

THE ROLE OF ANONYMISATION AND PSEUDONYMISATION ON GDPR COMPLIANCE

SANDRO SANDRI [1]

1 Sandro Sandri is a Legal & Compliance Manager and DPO at Coverflex, an EU fintech. With over a decade of experience across the UK, Portugal, and other European jurisdictions, he specializes in privacy law, financial regulation, and digital innovation. Sandro holds postgraduate qualifications from Queen Mary University of London, LSE, and Universidade Católica Portuguesa.

ABSTRACT:

Our analysis delves into the evolving roles of anonymisation and pseudonymisation in EU data protection, particularly under the GDPR. We highlight that early optimism for anonymisation as a primary privacy method was soon tempered by its practical limitations and the persistent threat of re-identification. This shift compelled regulators to formally recognize pseudonymisation as a (the) crucial safeguard. The GDPR, acknowledging the complexity of achieving absolute anonymity, therefore encourages a risk-based approach and explicitly brings pseudonymised data within its scope, offering significant privacy benefits and easing compliance burdens. This paper argues that effective data protection demands flexible, risk-based strategies, underscoring the importance of *de facto* anonymisation and robust pseudonymisation implementation. It concludes by advocating for the development of practical tools, such as certification mechanisms and codes of conduct, to bridge the gap between legal frameworks and the complex realities of data processing, thereby fostering responsible innovation while protecting fundamental rights.

KEYWORDS: *ANONYMISATION; PSEUDONYMISATION; GDPR; DATA PROTECTION; RISK-BASED APPROACH.*

I. INTRODUCTION

1.1. LEGAL FRAMEWORK

Prior to the implementation of the General Data Protection Regulation (GDPR), telecommunications privacy in the United Kingdom was primarily governed by the Data Protection Act 1998 (DPA), the Privacy and Electronic Communications Regulations (PECR), and the Data Protection Directive 95/46/EC (DPD). In addition, several other laws had a direct or indirect impact on privacy, including the Regulation of Investigatory Powers Act 2000, the Counter-Terrorism Act 2008, the Wireless Telegraphy Act 2006, the Communications Act 2003, the Anti-Terrorism, Crime and Security Act 2001, and the Human Rights Act 1998[1]. This paper focuses on the European legal framework for data privacy, particularly the now-repealed Data Protection Directive (DPD) and its successor, the General Data Protection Regulation (GDPR), in force since 25 May 2018. As a directly applicable regulation, the GDPR harmonised data protection laws across all EU Member States. A brief reference to the UK's Data Protection Bill—now the Data Protection Act 2018—will also be made in Section 3.1.

1.2. PERSONAL DATA AND IDENTIFICATION

To provide a general overview of anonymisation, I realised that I should firstly identify which is its counterpoint in the identifiability spectrum, this being the concept of identification. While anonymisation could be characterised as the absence of personal data in a particular dataset, identification stands as its opposite, meaning that in this context it became paramount to also provide a comprehensive definition of personal data and identification.

The DPD defined personal data as: «… *any information relating to an identified or identifiable natural person; an identifiable person is an individual who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*[2].»

1 Ian Walden, *Telecommunications Law and Regulation* (Oxford University Press 2012)

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281

On the other hand, the GDPR enlarges the scope of the DPD definition by establishing that a person can be identified by reference to an identifier such as a name, an identification number, location data, or an online identifier[3]. Also, regarding the combination of factors by which a person may be identified, the GDPR includes factors specific to genetic identity.[4]

The definitions above clearly indicate that personal data will be paramount in order to correctly identify individuals. This being the case, it is now important to understand the concept of identification or identifiability on both the DPD and the GDPR and to outline their differences.

Recital 26 of the DPD establishes that 'to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person'[5]. On the other hand, the wording chosen for Recital 26 of the GDPR exemplifies *singling out* as a reasonable mean likely to be used and gives the same importance to direct and indirect identification.[6]

Some examples of identification (direct and indirect) can be found through the processing of certain data fields such as names (as found in the findings of the Court of Appeals in Edem – 'A name is personal data unless it is so common that without further information, such as its use in a work context, a person would remain unidentifiable despite its disclosure[7]); location data (this kind of data is not included in the Regulation, however, its value and risk resides in the fact that through this sets of data, much can be inferred, such as sleep location, commuting patterns or even religious beliefs or health related data – what we can also call sensitive data); and online identifiers (these 'may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them'[8] – examples include cookies and IP addresses[9]).

The AOL case (explained in more detail in section 2.4) stands as a good example on how identification (in this case re-identification) can have an impact on individuals' lives. In

---

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119

4 Ibid

5 Recital 26 DPD (n2)

6 Recital 26 GDPR (n3)

7 Efifiom Edem v Information Commissioner and The Financial Services Authority [2014] EWCA Civ 92

8 Recital 30 GDPR (n3)

9 Slaughter and May, 'Personal data, anonymisation and pseudonymisation under the GDPR' (Publication July 2016) https://www.slaughterandmay.com/media/2535637/personal-data-anonymisation-and-pseudonymisation-under-the-gdpr.pdf

this case, an individual was positively identified – against her will – simply by analysing her search history and identifying number - 4417749. This happened in the United States, but, if it were to have happened in the United Kingdom, we could have faced two different approaches. Under the DPA, it is likely that that set of data would not have been deemed as personal data when it was ingested, as an online service provider/web browser like AOL, let's say Google[10], would (in theory) not have additional records necessary to identify the data subject. On the other hand, under the DPD's criteria, 'the material would probably have been classed as personal data as [the service provider] would have been required to consider the possibility that third parties could perform the task of identification.'[11] It is possible that if those processing activities had been carried out in the UK or in any other Member State, the responsible individual for (re-identifying those data subjects would have been deemed as a data controller.[12]

Still regarding the concept of identification in the European Union, it is relevant to highlight that such concept will have different social and cultural connotations throughout Member States as "*every nation states taking very different views of what kind of information should be treated as private*"[13]. In Sweden for example, tax returns are made available for the general public, while in France, telephone bills are itemised to avoid displaying the last few digits of the number called. Hence the importance of the GDPR in terms of harmonising, not only privacy law and its inherent legal procedures, but also basic legal definitions of concepts such as personal data, data controllers, processing of personal data, data processors, consent, and many other definitions as the ones encapsulated in article 4.

Identification can be achieved not only by processing classic categories of personal data, or what Americans and Canadians would call Personally Identifiable Information (PII), but also by processing some new categories of personal data introduced in the GDPR.

One of these categories are IP addresses[14] (in the opinion of the Information Commissioner's Office (ICO), 'only if the organisation handling the IP address can access other information linked to that address that identifies an individual'[15], and, in the same,

---

10 --, 'Google defies use over search data' *BBC* (20 January 2006) <http://news.bbc.co.uk/2/hi/technology/4630694.stm>

11 Ian J. Lloyd, *Information Technology Law* (Oxford University Press 2017) 64-65

12 Ibid

13 Chris Reed, *Internet Law* (Cambridge University Press 2004)

14 Article 29 Working Party Opinion WP136 (2007)

15 ICO decision notice FER0529617

line MAC addresses[16]). The Court of Justice of the European Union (CJEU) confirmed in Scarlett Extended[17] (2011) that IP addresses are in fact personal data. Not only that, but the Court also confirmed – in the Breyer Case[18] – that dynamic IP addresses can already be considered as personal data. Even though Mr. Breyer's IP address did not directly identify him (all parties agreed on that), the truth is that if that dataset was to be combined with his account data held in his ISP, then that would be enough for a positive identification of Mr. Breyer by the other party. This means that the Court took a relative approach rather than an objective approach, as through the former 'the IP address is personal data in the ISP's hands, but would not be personal data in the hands of another party that had no lawful means of accessing the information held by the ISP'[19], while through the latter 'the IP address is personal data in everybody's hands because the ISP can link the IP address to Mr Breyer's real world identity, even if nobody else can do so'[20].

Another new category of personal data introduced by the GDPR is cookies. In Google v Vida-Hall, the Court of Appeal held that there was a "*serious issue to be tried*"[21] as to whether browser-generated information (BGI) stands as personal data. In fact, the GDPR states in Recital 30 that: *... natural persons may be associated with online identifiers [...] such as internet protocol addresses, cookie identifiers or other identifiers [...]. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them*[22].

This means that, when cookies can identify an individual via their device, it is considered personal data. It is then clear that identification can be achieved by processing personal data fields as name, date of birth, email address, address, IP address, cookies, phone number, or gender.

However, there are additional categories of personal data that, due to their uniqueness, can more easily identify individuals and due to their sensitivity require higher levels of legal protection. Under article 9, the GDPR has branded these categories as special

16 ICO, *Guidance on Wi-Fi location analytics* (February 2016)
17 Case C-70/10 – *Scarlett Extended*
18 Case C-582/14 *Breyer v Brundersrepublik Deutschland*
19 Martin Munz, Tim Hickman and Matthias Goetz, 'Court confirms that IP addresses are personal data in some cases'(Publication White & Case 31 October 2016) <https://www.whitecase.com/publications/alert/court-confirms-ip-addresses-are-personal-data-some-cases>
20 Ibid
21 Google Inc v Vidal-Hall, [2014] EWHC 13 (QB)
22 Recital 30 GDPR (n3)

categories of personal data, these being "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership*", and also "*genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*"[23]. The importance of consent for the purpose of processing personal data is even more preeminent when it comes to sensitive data. In Bodil Lindqvist[24] we were made aware that, as insignificant as it might look, identifying an individual through the processing of his/her personal data will constitute a great risk of breaching data protection legislation. However, it is still important to note that in certain circumstances context shall be more important than content, or, as Ian Lloyd exemplifies: "*a reference to the fact that an athlete was unable to compete in a race because of a broken leg (…) does not seem to be possessed of a sufficient degree of sensitivity to justify the imposition of additional control*"[25].

In the context of defining personal data, if one analyses recital 26 of the GDPR "*personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person*"[26], we can extract a main distinction between anonymisation and pseudonymisation, which must be made for the purpose of this paper when defining personal data: while pseudonymous data still qualifies as personal data (as it includes indirectly identifying information) – and is consequently subject to the GDPR – anonymous data does not. Thus, the benefits of pseudonymisation pale in comparison to the benefits of full anonymisation[27]. I will address this issue below, on sections 2.1, 3.1 and 3.2.

1.3. PROCESSING OF PERSONAL DATA

In R v. Department of Health, *ex parte* Source Informatics Ltd, the Court of Appeal held that the disclosure of anonymous prescription data by pharmacists to Source was not a breach of confidence.

---

23 Article 9 (1) GDPR (n3)
24 Case C-101/01 *Lindqvist* [2004]
25 *Lloyd* (n11)
26 Recital 26 GDPR (n3)
27 Mike Hintzeand Khaled El Emam, '*Comparing the Benefits of Pseudonymisation and Anonymisation Under the GDPR'* (Privacy Analytics White Paper 17 November 2017) <https://iapp.org/media/pdf/resource_center/PA_WP2-Anonymous-pseudonymous-comparison.pdf >

Counsel raised the issue of applicability of the DPD, by which it was held that the process of anonymisation – converting identifiable data into non-identifiable data – fell within the definition of *processing* as established in the DPD and therefore, the DPD was applicable to the processing of that anonymised data set. The Court favoured the interpretation of the counsel for the General medical Council, which stated that "*the Directive can have no more application to the operation of anonymising data than to the use or disclosure of anonymous data*"[28].

However, the Information Commissioner's Office opposed such a view in its definition of personal data (2000): "*In anonymising personal data the data controller will be processing such data, in respect of such processing, will still need to comply with the provisions of the Act*".

This case illustrates the need to consider an anonymisation process as a type of processing personal data. As this case was held under English Law, we can then state that the data protection principles enshrined in the DPA are applicable to that process of anonymisation, particularly the fair and lawful processing principle, by which the controller is required to notify the data subject that such a process would be carried out. This kind of processing needs to fall within the criteria defined in Schedule II or Schedule III for sensitive data for it to be lawful.[29] The criteria can be based on consent given by the data subject or on the *necessity* of processing (legitimate interest).

Esayas understands that the "processing" of personal data is the main criteria for the applicability of data privacy rules.[30] This means that for the (now-repealed) DPD to apply, two preconditions should be fulfilled (Article 1 (1)): *data being processed* and this *data being personal*.[31] This remains the same under the GDPR.

Article 2 (b): "*processing of personal data*" (processing) shall mean any operation or set of operations which is performed upon personal data, whether by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[32]

---

28 Ian Walden citing the Information Commissioner's Office, 'Personal Data – Definition' (2000)
29 Articles 6 (1) (a), 7 and 8 DPD (n2)
30 S.Y. Esayas, 'The role of anonyimisation and pseudonomysation under the EU data privacy rules: beyond the 'all or nothing' approach' (2015) European Journal of Law and Technology, Vol 6, No 2
31 Ibid
32 Article 2 (b) DPD (n2)

Also, for the (now-repealed) DPD to apply, personal data needs to be any kind of information relating to an identified or identifiable natural person. As described above, this *identifiability* requirement means that even though an individual has not yet been identified, it is however possible, by combining information which is already being processed with other information, to correctly identify that individual.

For Esayas, for personal data to fall under the scope of identifiability, the mere possibility of associating certain information with a particular individual is sufficient.[33]

Again, in my opinion, there is no reason why this reasoning should not be equally applicable in the scope of the GDPR.

II. ANONYMISATION

2.1. DEFINING ANONYMISATION

Until recent years, citizens have been able to live a relative anonymous day-to-day life. Taxi and public transportation trips were not tracked; retailers had no idea what kind of products a specific customer liked the most; banks were not able to profile their clients based on their credit-worthiness rating; and media providers had no clue of which show every single viewer was keener on. Technology evolution has enabled the provision of more tailored and efficient services to citizens, especially thanks to the development of social media, cloud computing, the Internet of the Things, distributed ledger, biometrics, big data and other disruptive technologies.

However, the more these technologies tend to develop, the more citizens' privacy rights are likely to be at risk as the balance between privacy and monetization of data looks more elastic than ever. If we take London's Transport's Oyster Card as an example, we can properly understand how anonymisation might become increasingly harder to achieve in the future of services provision. Every commuter's Oyster holds a record containing all trips made for 8 weeks. Data is supposed to be held in an anonymised format for an indefinite period, however, as Ian Lloyd stated 'one of the issues that is arising with improvements in processing power is whether supposedly anonymised data might be re-linked to an identifiable individual'[34]. The question is of upmost pertinence, and I shall analyse this current debate that is dividing computer science on section 4.1. In the meanwhile, I will address the definition of the concept of anonymisation. Still on the issue

33 *Esayas* (n 30)
34 *Lloyd* (n 11) 4

of Oyster's re-identification possibilities, we should bear in mind that only in 2011, more than seventeen requests per day (more than 6,200 in total) were made by the London Metropolitan Police (to identify Oyster's users) as the card itself has proven being a valuable investigative resource for criminal investigations. Law enforcement in the UK is empowered by the Regulation of Investigatory Act 2000 to seek access to communications data[35].

Paul Ohm[36], Professor of Law at Georgetown University Law Centre and faculty director for the Centre on Privacy and Technology at Georgetown, has been creating terminology regarding the issue of anonymisation in recent years. One of the terms he created is the *robust anonymisation assumption*, by which he establishes that in the past decades the IT industry (which includes controllers and regulators) has developed the idea (and users have bought it) that privacy for users is achievable through the implementation of minor changes (as anonymisation techniques) to their data.[37] This means that through all this period, legal systems have adopted a *robust anonymisation* approach to privacy laws and regulations and developed their own existence based on the robust anonymisation assumption. However, Ohm states that in the last 15 years computer scientists have established what he calls the *easy re-identification result*, by which he also identifies that the above assumption is flawed, as it turns out to be possible to reverse-engineer those simplified anonymisation procedures and therefore, somehow 're-identify' living individuals through their personal data. "*By undermining the robust anonymisation assumption, easy re-identification will topple the edifices of promise and expectation we have built upon anonymisation*"[38].

In a generic way, Ohm defined anonymisation as "*a process by which information in a database is manipulated to make it difficult to identify data subjects"*[39]. Esayas stated that the problem with such definition is that it makes no mention to personal information, as it mainly encompasses "*techniques used to produce aggregated information"*[40]. On the other hand, the Information Commissioner's Office affirmed that the aim of such

35 Ibid 5
36 B.S., B.A., Yale; J.D., University of California, Los Angeles
37 Paul Ohm, 'Broken Promises of Privacy: Responding to the surprising failure of anonymisation' (2009) 57 UCLA Law Review 1707
38 Ibid
39 Ibid
40 *Esayas* (n 30)

techniques should be to process data linked to a particular individual without the individual being identified[41].

It was then relevant to understand if the process of anonymisation fell under the DPD's definition of processing, as such term 'encompasses a wide range of activities on data under the DPD'.[42]

The DPD established a possibility for processing for purposes (which cannot be incompatible) other than "*specified, explicit and legitimate*". In this context, Walden believes that the processing of personal data for the purpose of anonymisation clearly falls within the scope of the DPD by stating that it will always be a second purpose "*distinct from the purposes for which data was initially collected"*[43].

This means that, even though anonymised data does not stand as personal data, because it lacks the identifiability characteristic, the fact that a specific technique would need to be used for anonymising (or pseudonymising) data[44], turns such action an example of data processing as encompassed in the DPD and, therefore, relevant in the context of data protection legislation.

On the other hand, the GDPR clearly states that anonymous data is not personal data and therefore is not subject to the Regulation. Nothing is said about considering the implementation of anonymisation techniques as a way of processing personal data, but, as what happens under the DPD, there is no reason for not considering these activities as an example of data processing. The GDPR has not changed the concept of anonymisation, which makes Walden's interpretation of data processing for the purpose of anonymisation compatible with the GDPR.

In the UK, anonymisation has been defined by the ICO as "*the process of turning data into a form which does not identify individuals and where identification is not likely to take place"*[45].

We could say that the word "*likely*", which implies a possibility, is crucial for this definition. Through the ICO's view, the risk of re-identification needs only to be remote[46], as, although desirable, anonymisation does not stand as a requirement by the DPA. The

---

41 Esayas citing the ICO (2012) 51
42 *Esayas* (n 30)
43 Ian Walden, 'Anonymising Personal Data, International Journal of Law and Information Technology' (2002) Vol. 10 No. 2, Oxford University Press
44 Ibid
45 Information Commissioner's Office, 'Anonymisation: managing data protection risk code of practice' (Guidance January 2014)
46 *Slaughter and May* (n 9)

GDPR does not include the word "*likely*", which means that the Regulation is willing to set up a stricter threshold. As a matter of fact, the Working Party 29 (WP29) believes that anonymisation should, not only be desirable, but also irreversible[47], removing the "*likelihood factor*" out of the equation.

2.2.CONSENT AND PURPOSE

A relevant topic around consent is the compatibility between the purposes for collection and for processing. WP29 stated that anonymisation "*must satisfy the requirement of compatibility by having regard to the legal grounds and circumstances of the further processing"*.[48] This means that, in order to avoid data protection legislation for the repurposing of data, the purpose for the processing of data through anonymisation techniques can not differ from the purpose for which that specific set of data was collected for.

However, such approach stands as a limitation of the benefits of implementing anonymisation techniques as it narrows the possibilities for which anonymisation can be used for. Esayas noted that Emam and Alvarez suggested interesting approaches such as using anonymisation as a mean to comply with Article 6(1)(e) of the DPD, as deletion of personal data could be achievable through anonymisation[49]. On the same page, Hon, Millard and Walden believe that "*the stance adopted by the Working Party would discourage the use of anonymisation and pseudonymisation as privacy-enhancing techniques"*[50].

Using the definition of legitimate interest can suffice for overriding the existing limitations for anonymisation in the context of (purpose) compatibility, provided that the controller's interests do not pose a threat to the interests or fundamental rights of the data subjects. This is the position of both the ICO ("*in the absence of any unwarranted damage or distress resulting from anonymisation, there is no need to justify the process of anonymisation itself"*[51]) and the GDPR ("*processing of data to the extent strictly*

47 Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (10 April 2014)
48 *WP29* (n 47) 3
49 *Esayas* (n 30)
50 W. Kuan Hon, Christopher Millard and Ian Walden, Ian, 'The Problem of 'Personal Data' in Cloud Computing – What Information is Regulated? The Cloud of Unknowing, part 1' (2011) Queen Mary University of London, School of Law Legal Studies Research Paper No. 75 15
51 Information Commissioner's Office, 2012, p.28

necessary for the purposes of ensuring network and information security (…) constitutes a legitimate interest of the concerned data controller"[52]).

2.3.FAILED ANONYMISATION CASES

2.3.1.AOL

On 2006, web portal and online service provider America Online (AOL) proposed the "*AOL Research"*[53] initiative with the intention of publicly releasing records related to 20 million queries over 3 months from more than 650.000 AOL's search engine users.

This set of information was very well received by most of the scientific internet-related community, especially by internet behaviour experts, as it is very rare to come across data with such amount of density and description. Normally, data originating from search engines is treated as a "*closely guarded secret*"[54].

To publicly publish the data, AOL tried to anonymise it by suppressing data fields as AOL username and IP address. However, as a way of potentiating the utility of that data, it replaced those attributes with identification numbers (representing data subjects), which enabled to correlate searches and queries to each one of them.

After the data release[55], many of these user identification numbers become particularly infamous among bloggers competing to identify users and were quickly singled out by their very particular search history: «User No. 3505202 ask[ed] about "*depression and medical leave*". No. 7268042 type[d] "*fear that spouse contemplating cheating*." User 17556639 searched for "*how to kill your wife*" followed by a string of searches like "*pictures of dead people*" and "*car crash photo*"[56].»

Although some bloggers argued that even though the information related to the identification numbers could sometimes be titillating, the release of the data did not violate AOL data subjects' privacy rights. This assertion was proven wrong as Tom Zeller and Michael Barbaro[57], reporters from the *New York Times*, were easily able to identify user No. 4417749 as Thelma Arnold, a 62-year-old widow who by then lived in Lilburn, Georgia, USA. The search history for Mrs. Arnold's identification number included

---

52 *Esayas* (n 30)
53 *Ohm* (n 37) 1717
54 Ibid
55 Some authors, like Paul Ohm, prefer using the term data breach.
56 *Ohm* (n 37) 1718
57 Tom Zeller and Michael Barbaro Jr. 'A Face Is Exposed for AOL Searcher No. 4417749' (9 August 2006) The New York Times <http://www.nytimes.com/2006/08/09/technology/09aol.html>

queries for "*landscapers in Lilburn, Ga,*" several people with the last name Arnold and "*homes sold in shadow lake subdivision Gwinnet county Georgia.*" Indeed, Mrs. Arnold "*frequently researches her friends' medical ailments and loves her three dogs"*[58].

The fact that a data subject was easily identified, even though the released information was previously anonymised (i.e. identifiers were removed and replaced by identification numbers), demonstrates how some anonymisation techniques are not safe enough for ensuring individuals' privacy rights. In this case, the data was not completely anonymised, instead, it was pseudonymised, meaning that a pseudonymous was attributed to each one of them (Thelma Arnold was 4417749). In practice this meant that each individual user could then be segregated, and information relating to him or her could therefore be correlated. This correlation of data inevitably created an individual profile of a living individual.

The aftermath of the AOL data release resulted in the firing of both the researcher who put the queries online and the manager who oversaw the project, and in the Chief Technology Officer announcing her resignation.

2.3.2. GIC - Group Insurance Commission

On 2000, Latanya Sweeney was able to demonstrate the efficiency of re-identification techniques[59] by analysing the Massachusetts' Group Insurance Commission (GIC) purchase of health insurance for state employees and subsequent data release. For research purposes, in the mid-1990's the GIC decided to freely release that data to whoever would request it. To do so, they firstly removed some data fields containing personal data as name, address or social security number, believing that this process would efficiently anonymise data and therefore, preserving those data subjects' privacy rights.

Unfortunately, the anonymisation technique used (suppression) was not adequate as "*nearly one hundred attributes per patient and hospital visit were still included*"[60]. Among these attributes, a specific trio stood as a common denominator for Sweeney when re-identifying individuals: ZIP code, birth date and sex.

Sweeney was able to discover that: «*... 87.1 percent of people in the United States were uniquely identified by their combined five-digit ZIP code, birth date (including year), and*

58 Ibid
59 L. Sweeney, 'Simple Demographics Often Identify People Uniquely. Carnegie Mellon University' Data Privacy Working Paper 3 (2000) Pittsburgh
60 *Ohm* (n 37) 1719

sex. According to her study, even less-specific information can often reveal identity, as 53 percent of American citizens are uniquely identified by their city, birth date and sex, and 18 percent by their country, birth date, and sex.»[61]

This means that it is very probable to identify an individual whose data has been anonymised by only matching its gender, age and location on an anonymised database (country, city or zip code).

That is what Sweeney did when (then) Governor of Massachusetts William Weld publicly stated that GIC had efficiently preserved patient privacy by suppressing identifiers[62]. By knowing that the Governor lived in Cambridge, Massachusetts, a town of seven ZIP codes, she merely had to match that information against the complete voter rolls from the same town (which included attributes such as ZIP code, birth date and gender). After that, she was left with six people living in Cambridge with the same birth date, three of those were men and only one lived in that ZIP code: the Governor.

2.3.3.NETFLIX

In 2006, Arvind Narayanan and Vitaly Shmatikov stated that "*an attacker who knows only a little bit about an individual subscriber can easily identify this subscriber's record if it is present in the [Netflix Prize] dataset, or, at the very least, identify a small set of records which include the subscriber's record*"[63].

This assertion came in the context of the 2006 Netflix data release, by which the movie rental company released one hundred million records, each record containing information regarding how more than half-million of the company users rated movies between December 1999 and December 2005 (movie rated, rating assigned and date of rating[64]). Again, this release delighted internet behavioural experts.

The reason for the data release was to launch what they called the "*Netflix Prize*", by which the team that was able to best use the data to improve Netflix's recommendation algorithm would win a prize of one million dollars[65].

As in the cases above, Netflix anonymised the data before releasing it by removing identifiers, e.g. usernames. However, they also assigned a "*unique user identifier to*

61 Ibid
62 Ohm citing Henry T. Greely, 'The Uneasy Ethical and Legal Underpinnings of Large-Scale Genomic Biobanks' (2007) 8 Ann. Rev. Genomics & Hum. Genetics 343, 352
63 Arvind Narayanan and Vitaly Shmatikov 'How to Break the Anonymity of the Netflix Prize Dataset' (2006) ARVIX <http://arxiv.org/abs/cs/0610105v1>
64 The Netflix Prize Rules, http://www.netflixprize.com/faq
65 Ibid

preserve rating-to-rating continuity. Thus, researchers could tell that user 1337 had rated Gattaca a 4 on March 3, 2003, and Minority Report a 5 on November 10, 2003".[66]

Briefly after the release, Narayanan and Shmatikov demonstrated that it was notably effortless to re-identify individuals within the Netflix database only by knowing some high-level movie preferences. They stated that they would efficiently identify an individual 84 percent of the time simply by knowing how that data subject has rated six movies outside of the top five hundred movies rated in the database (Ohm, describes these as "*obscure movies*"[67]). The re-identification mechanism is even more powerful when the factor "time" is taken into consideration, as an individual will efficiently be identified 99 percent of the time if they are able to roughly know when (within two weeks) the individual rated the movie (regardless of being an obscure movie or not). In the words of Ohm: 'In fact, knowing when ratings were assigned turns out to be so powerful that knowing only two movies a rating user has viewed (with the precise ratings and the rating dates give or take three days), an adversary[68] can re-identify 68 percent of the users[69]'.

To exemplify the above results, Narayanan and Shmatikov compared that data to similar data in the Internet Movie Database (IMDB), an online database of information related to films and television programs which allows users to publicly rate contents on the website. Through the matching of both databases, the researchers were able to find 2 identifiable users in the Netflix database, out of a sample of 50 users in the IMDB database[70].

III. THE EMERGENCE OF PSEUDONYMISATION

3.1. HOW DID WE GET HERE?

While on one hand, the development of pseudonymisation is one of the biggest innovations introduced by the GDPR, on the other hand, one can confirm that the concept of anonymisation and its framework remained practically untouched when comparing the evolution form the wording in the DPD to the one in the GDPR. We could even say that a paramount piece was removed while drafting the Regulation, which is the use of codes of conduct as a "*useful instrument for providing guidance as to the ways in which data*

66 *Ohm* (n37) 1720
67 *Ohm* (n37)
68 Term used by computer scientists
69 *Ohm* (n 37) 1721
70 Ibid

may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible".

At first glance, it is hard to understand such a decision, especially given the importance given to the matter of anonymisation during the early works of the Regulation by institutions as the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE); the European Union Commission; the European Union Council; the European Data Protection Supervisor (EDPS); or the WP29.

The EDPS' 1st Opinion

It was only on the 14th of January of 2011 – 16 years after the Directive was enforced (13 December 1995) – that the EDPS firstly addressed the need for further development on the definitions of both anonymisation and pseudonymisation (among others). In its opinion, the EDPS included a proposal to include more items to the list in article 2 (Definitions) of the Directive 'in order to provide for more legal certainty'[71]. This opinion was later adopted by LIBE.

The EU Commission's proposal

On the 25th of January of 2012, the European Commission issued a proposal for a reform of Directive 95/46/EC, which ultimately resulted in the GDPR, adopted in 2016 and in force since 2018. This is the first time where we realise that the use of codes of conduct is firstly stripped from the wording regarding the framework of anonymisation, as the only mention to this concept resides in recital 23: 'The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable'[72]. On the other hand, there is no mention whatsoever to pseudonymisation at this point.

The EDPS' 2nd Opinion

Shortly after the proposal's publication, the EDPS issued an opinion on the 7th of March of 2012. In this opinion, the EDPS merely focused on the processing of personal data for research purposes, stating, in reference to article 83 of the proposal that 'the point

71 Point 54 Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — 'A comprehensive approach on personal data protection in the European Union' (2011/C 181/01)

72 Recital 23 of the European Commission Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - 5853/12. 27 January 2012

of departure for data processing for historical, statistical and scientific research purposes should be that such processing is done by using anonymised data.'[73]

WP29 Opinion

On the same month (23 March 2012), WP29 published their first opinion on the data protection reform proposals. This is the first time that pseudonymisation is suggested as an appropriate mechanism to achieve better data protection and WP29 recommends the introduction of such concept on the wording of the (future) Regulation, stating that 'such a principle could be introduced in Article 5 and in the context of data protection by design and default in Article 23'[74]. On this context, the only reference that WP29 makes to anonymisation remains on a suggestion to 'introducing a general obligation to anonymise or pseudonymise personal data where feasible and proportionate according to the purpose of processing'[75]. Later, on the 5th of October of 2012, the WP29 published a new opinion providing further input on the data protection reforms discussion (08/2012)[76], however, no attention was given to neither anonymisation nor pseudonymisation.

LIBE's Working Documents

This was not the case when, only three days later (8 October 2012), LIBE published the second of a set of three working documents regarding the proposed data protection reform where both anonymisation and pseudonymisation were addressed as good mechanisms to "*reach the best level of data protection and enable new business models"*[77]. One of the most interesting points on this working document was LIBE's opinion to clearly define anonymisation in the GDPR, as a way of 'helping data controllers understand when they are outside of scope of the Regulation'[78]. Although we now know that such definition was not include in the final text of the Regulation, I tend to agree with LIBE's opinion as a way of bringing higher legal certainty to both data controllers and data processors. Encompassing a clear definition of the concept of anonymisation would help mitigating certain risks provoked by the current ambiguous

73 Point 302 of the Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012
74 Opinion 01/2012 on the data protection reform proposals, Article 29 Data Protection Working Party, Adopted on 23 March 2012, p. 11
75 Ibid
76 Opinion 08/2012 providing further input on the data protection reform discussions, Article 29 Data Protection Working Party, Adopted on 05 October 2012
77 Working Document 2 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht, 8.10.2012
78 Ibid

approach, especially in the difference between anonymisation and pseudonymisation and due to the lack of both adequate codes of conduct and certifications (article 40).

Still on the LIBE's working document, it is important to note that it was the Committee's opinion that the pseudonymous use of services could comprehend an alleviation mechanism 'with regard to obligations for the data controller'[79], meaning that, when anonymisation is not possible, the use of pseudonymisation (singling out individual persons by a pseudonym) may lighten the compliance burden.

LIBE's Draft Report

An important document was also produced by LIBE on the 16th of January of 2013. This was the LIBE's Draft Report on the EU Commission's proposal for a regulation of 25 January 2012. On this report, LIBE addressed recital 23 of the proposal – 'The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable'[80] – providing a definition of what could qualify as anonymous data: «*... any data that cannot be related, directly or indirectly, alone or in combination with associated data, to a natural person or where establishing such a relation would require a disproportionate amount of time, expense, and effort, taking into account the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed*.[81]»

LIBE also proposed the addition of a new paragraph to article 81 of the Commission's proposal (processing of personal data concerning health), advising, on the context of processing health related data (with regard to research that serves a high public interest) for such data to be anonymised 'or if that is not possible for the research purposes, pseudonymised under the highest technical standards, and all necessary measures shall be taken to prevent re-identification of the data subjects'[82]. This advice was also extended to article 83 of the proposal, stating, on amendment 335, that 'data about children and sensitive data (…) may only be used without the consent of the data subject if it serves an exceptionally high public interest, and in this case must be anonymised or at least

79 Ibid
80 EU Commission (n 72) Recital 23
81 Amendment 14, European Parliament Committee on Civil Liberties, Justice and Home Affairs, ***I Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 16.1.2013
82 Ibid, Amendment 328

pseudonymised using the highest technical standards[83]'. (However, these amendments were not included in the Regulation's final wording.

LIBE's Draft Report includes the first proposal including a definition of the concept of pseudonym: "*unique identifier which is specific to one given context, and which does not permit the direct identification of a natural person but allows the singling out of a data subject*"[84].

Amendment 117 clearly shows LIBE's opinion on how pseudonymisation should lighter data controller's compliance burdens by suggesting, in reference to article 10 of the Commission's proposal, that if: «… *the data processed by a controller do[es] not permit the controller to identify or single out a natural person, or consist[s] only of data relating to pseudonyms, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation*[85].»

LIBE's report clearly states, in amendment's 33 justification that the use of pseudonyms is encouraged by this Regulation[86], which demonstrated the importance given to the subject of pseudonymisation on the draft report, paving the way to the further emergence of this concept on the GDPR.

IMCO's, ITRE's and JURI's Opinions

On the same month (28 January 2013), the Committee on the Internal Market and Consumer Protection (IMCO) published their opinion for LIBE on the Commission's proposal. On this opinion, the Committee referred to recital 23 (principles of data protection should not apply to anonymous data) stating that pseudonymous data might be useful if the key to link the pseudonymous with the identity is safe *according to the state of the art*[87].

It is indeed strange to confirm the lack of attention given to anonymisation on the final wording of the Regulation, given that several opinions were issued by different European institutions. IMCO, the Committee on Industry, Research and Energy (ITRE) and the Committee on Legal Affairs (JURI) issued some more amendments on their opinion

83 Ibid, Amendment 334
84 Ibid, Amendment 85
85 Ibid, Amendment 117
86 Ibid, Amendment 33
87 Amendment 4, European Parliament Committee on the Internal Market and Consumer Protection, opinion on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 28 January 2013

papers, such as: advising on anonymising or pseudonymising personal data before sending it to health professionals for processing[88]; providing a definition of anonymous data[89,90,91]; advising on including anonymised data as an exception to the right to object to automated decisions making[92] or; advising data processors to anonymise or pseudonymised personal data where feasible and proportionate according to the purpose of processing[93]. The lack of attention given to anonymisation on the final version of the Regulation contrasts the importance given to pseudonymisation (these Committees provided a definition for pseudonymous data). This could reflect the compromise achieved by European legislators as a way to lighten the compliance burden to data controllers and data processors through the implementation of pseudonymisation mechanisms. Although anonymisation is the preferable option, the fact that we can confirm how it was slowly taken off the debate and replaced by pseudonymisation might help to demonstrate how, due to its technical challenges, regulators felt conscientious of the difficulties on regulating on an issue which was running too fast. This resulted on acknowledging that pseudonymisation succeeded on achieving a balancing exercise by which controllers are still responsible for their data processing activities, but with less compliance burden than the one expected for "standard" personal data processing activities.

LIBE's Amendments

Taking into consideration their views and all the recent opinions issued by IMCO, ITRE and JURI, LIBE submitted an exhaustive set of 3133 amendments (divided in 10 documents[94]) to the Commission's proposal. In those amendments, LIBE addressed many of the suggestions and advices made by all the Committees on the topics of anonymisation and pseudonymisation (some of them referred above) making it clear that even though

88 Amendment 43, Ibid
89 Amendment 59, Ibid
90 Amendment 79, European Parliament Committee on Industry, Research and Energy, opinion on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 26 February 2013
91 Amendment 35, European Parliament Committee on Legal Affairs, on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 25 March 2013
92 Amendment 192, Ibid
93 LIBE (n 87) Amendment 139
94 European Parliament Committee on Civil Liberties, Justice and Home Affairs amendments on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

both topics were of paramount importance, pseudonymisation was rising as a crucial instrument for implementing best data protection practices: «*... This Regulation recognises that pseudonymisation is in the benefit of all data subjects as, by definition, personal data is altered so that it of itself cannot be attributed to a data subject without the use of additional data. By this, controllers should be encouraged to the practice of pseudonymising data*[95].»

LIBE voted to adopt the EU Commission's proposal with the amendments above on the 21st of October of 2013. As part of the European Union's legislative procedure –to pass the Regulation – the Commission's proposal needed to be reviewed and voted by both the Council of the European Union and the Parliament of the European Union. This means that following steps at that stage were the review, amendments and approval by the Parliament and the Council.

EU Parliament and EU Council Resolutions

These Institutions voted to adopt their own versions and published their resolutions one year apart. The Parliament published its resolution on the 12th of March of 2014, while the Council published its resolution on the 11th of June of 2015.

Both documents included lesser references to anonymisation than in previous opinions issued by the EDPS, WP29, LIBE, IMCO, ITRE and JURI. Some of the few references to anonymisation included a definition of anonymisation (this being the Council's only reference to the topic)[96,97] and opinions on how personal data processed by health professionals should be anonymised[98] and on how anonymised data should be considered as an exception to the requirement of consent for research that serves a high public interest[99].

Pseudonymisation, on the other hand, was recurrently referred on both resolutions, clearly demonstrating the intent of legislators to shift to pseudonymisation as an appropriate mechanism to achieve better data protection. Some of the issues on pseudonymisation addressed by the Parliament and the Council were: presuming data processing limited to

---

95 Ibid, Amendment 395

96 Recital 23 of the European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

97 Recital 23 of the Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 9565/15, 11 June 2015

98 Parliament (n 96), Recital 122a

99 Ibid, Article 81 (2a)

pseudonymous data to meet the reasonable expectations of the data subject in the context of a controller's legitimate interest[100]; presuming profiling activities based on pseudonymous data to not significantly affect the interests, rights or freedoms of data subjects[101]; providing a definition of pseudonymisation[102,103]; clarifying how pseudonyms stand as information concerning an identifiable natural person[104]; identifying pseudonymisation as an appropriate measure to ensure data protection[105] by design and by default[106] and an adequate level of security of processing[107]; stating that pseudonymisation reduces risks to data subjects while helping data controllers and data subjects meeting their data protection obligations[108]; or identifying data breaches[109] and the unauthorised reversal of pseudonymisation as a risk for the rights and freedoms of individuals[110] while at the same time, classifying the pseudonymisation of personal data as soon as possible as an appropriate measure to protect the rights and freedoms of individuals to ensure that the requirements of the GDPR are met[111].

Finally, article 38 (1a) (bb) of the Council's resolution addresses a very interesting issue. It is the Council's view that Member States, Supervisory Authorities, the EDPB and the EU Commission should encourage the drawing of codes of conduct on the topic of pseudonymisation[112]. No codes of conduct have been published on this topic however.

After the Parliament and the Council voted to adopt their own versions, the Regulation passed into the final legislative stage, known as the Trilogue negotiations, which lasted until the 15th of December of 2015.

EDPS' 3rd Opinion

On the meantime, the EDPS published a new Opinion paper (27 July 2015) which included no reference whatsoever to anonymisation and merely addressed

100 Ibid, Recital 38
101 Ibid, Recital 58a
102 Ibid, Article 4 (2a)
103 Council (n 97), Article 3 (b)
104 Ibid, Recital 23
105 Parliament (n 96), Article 33 (3e)
106 Ibid, Article 23 (1)
107 Ibid, Article 30 (1)
108 Ibid, Recital 23 (a)
109 Ibid, Recital 67
110 Ibid, Recital 60a
111 Ibid, Recital 61
112 Council (n97) Article 38 (1a) (bb)

pseudonymisation to indicate that pseudonymised data should definitively be considered as personal data[113] and, therefore, within the scope of the Regulation.

The Trilogue Outcome

On the 15th of December of 2015, the Parliament and Council came to an agreement because of the Trilogue negotiations (which LIBE adopted). The outcome of the Trilogue was published two days later. The only reference to anonymisation was to indicate how the principles of data protection should not apply to anonymised data making it therefore outside the scope of the Regulation[114].

Differently, we can observe the culmination of the emergence of pseudonymisation as it received much more attention than it did on the 2012 Commission's proposal. Most of the references included in the Trilogue outcome are in line with the opinions of the Parliament and the Council, more specifically: Recitals 23, 23a, 23c, 60a, 61, 67 and articles 4(3b), 6(3a)(e), 23(1), 30(1) and 38 (1a)(bb). The Trilogue outcome also included the classification, in recital 125, of pseudonymisation as an appropriate safeguard to deny identification of data subjects.

After the political agreement on the Trilogue outcome, the text was adopted by the Council and the Parliament on the 8th and the 16th of April of 2016, respectively. The GDPR was published on 4 May 2016 and has been in force since 25 May 2018.

The Data Protection Bill

After the GDPR was published, many European Members as the Netherlands, Spain or Austria published their own data protection implementation bills as a mechanism to supplement the GDPR. The UK was no exception and after being announced in the Queen's speech on the 21st of June of 2017, the Data Protection Bill, which later became the Data Protection Act 2018, was published on 14 September 2017.

The Bill is also meant to implement the EU Law Enforcement Directive and extend data protection laws to areas which are not covered by the GDPR[115]. One of these areas lays on the field of criminal offences, and, for the purpose of this paper, I shall briefly refer to the criminal offences introduced by article 169 of the Data Protection Bill – Re-

113 European Data Protection Supervisor, Opinion 3/2015 (with addendum) Europe's big opportunity, EDPS recommendations on the EU's options for data protection reform, 27 July 2015 (updated with addendum, 9 October 2015), 5

114 Recital 23 of the Trilogue outcome proposal - Regulation (Eu) No Xxx/2016 of the European Parliament and of the Council, 17 December 2015 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

115 Information Commissioner's Office, 'An introduction to the Data Protection Bill'

identification of De-identified[116] personal data. From article 169 we can conclude that it is a criminal offence to both re-identify information which has been previously anonymised[117] and to process information previously anonymised[118]. It is of no importance whether the perpetrator acts recklessly or knowingly in terms of being criminally accountable. There have been reports stating that "some House of Lords members considered that this could allow organisations to relax the methods they use to anonymise data on the basis that people will not attempt to re-identify individuals because it is a criminal offence"[119].

An amendment to the Bill was added in order to protect security researchers carrying out effectiveness testing. Researchers will have to notify the ICO within 72 hours of successfully re-identifying personal data and demonstrate that they had acted in the public interest and without intention to cause harm or damage to data subjects (article 169(5)).

3.2.PSEUDONYMISATION UNDER THE GDPR

It is largely consensual that to reduce privacy exposure, anonymity will be the desired threshold in what we could call "*the identification-spectrum"*. Even though individuals have, in recent years, resorted to privacy-enhancing systems like Tor (which, however, has already been proven to leak users' IP addresses[120]) or "*semi anonymous*" cryptocurrencies like Bitcoin (which are far from flawless[121]), the truth is that anonymous communications and transactions are becoming harder to achieve day by day, as *interlinkable* data systems and tracking devices seem to develop at a faster pace than anonymity-enhancing technologies.

These difficulties once again highlight the actual binomial between data privacy and efficiency, and that is why, in some situations –'MAC numbers to track equipment, cookies and browser fingerprints to track software and its users, or cross-linking of location data with other data captures, be it phones, faces, loyalty cards, or self-surveillance'[122] – enabling the use of pseudonyms (robust privacy-enhancing identities)

116 On this context, de-identification shall mean anonymisation and de-identified data shall mean anonymised data

117 Article 162 (1) Data Protection Bill

118 Article 162 (5) Data Protection Bill

119 Alison Deighton, 'Data Protection Bill under review by Parliament' (2017) Lexology <https://www.lexology.com/library/detail.aspx?g=1c4ec2ab-921b-4eee-9f88-e4d3d4549d2a>

120 HelpNetSecurity, 'Tor Browser flaw leaks users' real IP address' (2017) <https://www.helpnetsecurity.com/2017/11/06/tor-browser-ip-leak/>

121 Michael A. Froomkin 'Pseudonyms by Another Name, Privacy in the Modern Age' (2015) The New Press, 64

122 Ibid

will actually be a preferred solution to anonymity. This is why, on those situations, it will be preferable to adopt identity management solutions – which will most probably incorporate substantial traceability in them.

For the sake of understanding what pseudonymisation is in practice, I believe that I should contextualize it under the scope of the GDPR to be able to provide a reasonable legal framework. The reason being is that this concept, although very common in Information Security terminology, is firstly introduced in data protection legislation under the GDPR and is now enshrined in several of its recitals and articles.

In fact, pseudonymisation is one of the biggest changes to privacy and data protection that the GDPR brings when compared to the DPD. This being said, the Regulation describes it as: «… *the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*[123].»

We can describe it as a privacy-empowering technique that ensures non-attribution by enabling the secure separation of directly identifying data (fields) from processed data. The IAPP defines it as: «*The separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately. Pseudonymisation, therefore, may significantly reduce the risks associated with data processing, while also maintaining data's utility*.[124]»

Hintze and El Emam went a step further and understood that two definitions of pseudonymisation arise from the GDPR: Basic Pseudonymisation ("*direct identifiers are transformed and appropriate controls are put in place to ensure that cryptographic keys are stored and handled appropriately*"[125]) and Strong Pseudonymisation ("*where some indirect identifiers in the data are also perturbed, any cryptographic keys are destroyed (…) and stronger security and privacy controls on the management of the data itself are put in place*"[126]).

Esayas stated that pseudonymisation can be considered as one technique of anonymisation, as it is a particular technique which can be used for reducing the

123 Article 4 (5) GDPR (n 3)
124 Gabe Maldoff, 'Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization', IAPP <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/>
125 *Hintze and El Elam* (n 27)
126 Ibid

identifiability of individuals.[127] However, as shortly explained above in section 1.2, pseudonymisation does differ from anonymisation as the former qualifies as a mechanism by which personal data is processed, while the latter is not. This means that while pseudonymous data is personal data and therefore falls under the scope of the GDPR, anonymous data not, and consequently escapes from that scope.

It could be argued that pseudonymisation is a process that renders data neither anonymous nor directly identifying, which makes it a unique process by its own, a "tertium genus". But although truthful, such approach is however not recommended, as, even though data is not directly identifiable, a natural person can still be indirectly identified, which will be enough to contextualise a data set under the GDPR definition of personal data.

To substantiate this statement, I reviewed the GDPR's definition of personal data. Article 4 clearly defines personal data as, "*any information relating to an identified or identifiable natural person* ('data subject')"[128]. At the same time, Recital 26 states that "*personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person"*. Therefore, the junction of article 4 and recital 26 indicates that pseudonymised data is personal data, as it can be attributed to an identifiable natural person using additional data and, consequently, it is subject to the Regulation.

In general terms, the similarity that these two techniques (anonymisation and pseudonymisation) have in common is that both are used to de-identify data, which makes them de-identification techniques[129]. On the other hand, the main difference that sets them apart, is that while re-identification can be operated on pseudonymous data, the same will not be possible with anonymous data, as (in theory) it will be impossible to link/trace this sets of data to any living individual. Ideally, anonymisation techniques cannot be reverse engineered.

After analysing Recital 26, it becomes clear that, under the GDPR, if a data controller wishes to implement measures of pseudonymisation and to run related general analysis, that controller needs to: a) take technical and organisational measures to ensure that the GDPR is implemented; b) ensure that additional information for attributing the personal

127 *Esayas* (n 30)
128 Article 4 (1) GDPR (n 3)
129 Hintze and El Emam (n 27) use de-identification as a general term that includes the full spectrum of methods, from simple pseudonymisation to full anonymization.

data to a specific subject is kept separately; and c) indicate the authorised persons of processing the personal data.[130]

In essence, pseudonymisation can be considered as a 'security measure [that] organisations can apply to personal data, much like encryption'[131]. Recital 5 of the GDPR, defines pseudonymisation as: «… *the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person*.[132]»

It is important that controllers follow the adequate procedures set in the GDPR for processing pseudonymous data as any 'unauthorised reversal of pseudonymisation may result in a risk to the rights and freedoms of natural persons'[133]. If such thing happened, and regardless of the fact that the data controller was trying to protect individuals' personal data by allowing for measures of pseudonymisation, the truth is that this controller would be in breach of the GDPR, specifically because one of the main objectives of the whole Regulation, set out in article 1 (2), is to 'protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'[134]. This would then mean that that specific processing activity (pseudonymising personal data), when used for example for the purposes of the controllers' legitimate interest, would fail the lawfulness test set out in article 6 (1)(f), which states that: «*Processing shall be lawful only if and to the extent that (…) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject*.[135]»

Still about the lawfulness of processing through pseudonymisation techniques, article 6 (4)(e) also states that if processing data without consent for a different purpose other than that which the personal data has been collected, the controller shall take into account the existence of appropriate safeguards, which may include pseudonymisation[136]. Hence the importance and influence that adopting good pseudonymisation techniques can have

130 Recital 29 GDPR (n3)
131 Slaughter and May (n 9)
132 Recital 5 GDPR (n 3)
133 Ibid, Recital 75
134 Ibid, Article 1
135 Ibid, Article 6
136 Ibid, Article 6 (4)(e)

when demonstrating compliance with the GDPR[137], as, at least in cases like this, can 'help enable data processing for secondary purposes without the need to obtain explicit consent from data subjects'[138].

If done correctly, pseudonymising data can be one of several measures that meet the principles of data protection by design and data protection by default[139], which *per se*, would enable demonstrating compliance with the Regulation as the rights and freedoms of natural persons would be adequately protected. Also, article 25 makes it clear that pseudonymising personal data will enable and respect the principle of data minimisation, as it is a measure that allows for limiting personal data collection, storage, and usage to data that is relevant, adequate, and absolutely necessary for carrying out the purpose for which the data is processed.[140]

When combining Recital 156 and article 25, one can understand that pseudonymising data is both an appropriate safeguard that controllers can implement to process data which does not permit or no long permits the identification of data subjects, and a technical measure that ensures the principle of data minimisation. This is relevant for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes as it would act as a safeguard of the rights and freedoms of data subjects in the context of the GDPR[141]. Still about technical measures, it is important to highlight that article 32 clearly identifies pseudonymisation as an appropriate technical measure that both controllers and processors shall implement to ensure a level of security appropriate to the risk of processing.[142]

Failure in implementing pseudonymisation techniques in a secure manner is not the only way by which personal data can, unexpectedly, be traced back to a living individual. An example of an exemption could be a data breach, as it may, if not addressed in an appropriate and timely manner, result in unauthorised reversal of pseudonymisation and therefore cause damage to data subjects.[143]If such thing happens, the controller has to follow the established procedures for data breach management set out in recitals 85, 86, 87 and 88 and in articles 33 and 34.

---

137 Ibid
138 *Hintze and El Elam* (n 27)
139 Article 25 GDPR (n 3)
140 Dataguise, 'Data Minimization in the GDPR: A Primer' (2017) <https://www.dataguise.com/gdpr-compliance-data-minimization-use-purpose/>
141 Recital 156 GDPR (n 3)
142 Ibid, Article 32
143 Ibid, Recital 85

IV. TECHNICAL MEASURES

4.1.IDENTIFICATION, DE-IDENTIFICATION AND RE-IDENTIFICATION - IS ANONYMISATION AN EFFECTIVE TOOL FOR PROTECTING PRIVACY?

Although many companies promise to preserve their clients' personal data in an anonymous way, the truth is that these promises are many times easily broken, be the data controllers or by some of their competitors. Such bad practices help bringing into the spotlight what Ohm identifies as a "*foundational belief about data privacy: Data can be either useful or perfectly anonymous, but never both*"[144].

Identifying a data subject can both be accomplished through direct or indirect identification. Through direct identification, an individual can be identified by analysing a single data source, e.g. full name. Through indirect identification, we can identify data subjects by combining two or more data sources, or what we could call contextual data. This means that we could identify someone by analysing their data from a particular context, e.g. in a university or a school, a student's identification number would be enough for positively identifying the student/data subject.

In some situations, a given controller or processor might not be processing personal data from a particular individual (no identification). However, it can occur that the controller/processor does not know whether other sets of data are available, which means that re-identification by a third party is a possibility. The ICO Guidance on Anonymisation indicates 2 clear examples, "*where publicly available data – such as the Electoral Roll or data easily retrievable from a web-search – can be combined with the 'anonymised' data, allowing individuals to be identified (...), to be able to establish a reliable connection between particular data and a known individual*"[145].

It will be difficult in some situations to identify an actual risk of re-identification. One of these situations might involve processing pseudonymised data sets as "*the possibility of linking several anonymised datasets to the same individual can be a precursor to identification*"[146]. This can be somehow contradictory, as even though pseudonymous data does not identify a data subject, the truth is that the processing of a that data subject's

144 *Ohm* (n 30)
145 Information Commissioner's Office, 'Anonymisation: managing data protection risk code of practice' (Guidance 2014) 21
146 Ibid

personal data can be an obstacle for complete anonymisation. This does not mean however that anonymisation through pseudonymisation is not possible.

Personal data can either be quantitative or qualitative and controllers and processors might want to anonymise just one of these types, or even both. I have compiled below several anonymisation methods/techniques which can be reviewed in section 4.2 and 4.3. However, the techniques used to anonymise quantitative data are not as efficient when it comes to qualitative data and are normally more time-consuming and dependent upon human judgement. The ICO has listed some of the main techniques used for anonymising qualitative data, these are: 'redacting individuals' names from documents, blurring video footage to disguise faces, electronically disguising or re-recording audio material, and changing the details in a report (precise place names, precise dates, etc.)'[147]

It has become clear that to tackle the privacy challenges embedded in the de-identification and re-identification of datasets, a joint approach between data protection law and computer science is advisable. The reason for this rests on the fact that it is computer science's natural obligation to conclude whether de-identification is an effective privacy-ensuring tool (including all its different anonymisation techniques), while it will be data protection law's responsibility to create a legal framework to accommodate such tool. This is why a look must be given to recent computer science literature which has been spurring very interesting debates on the effectiveness of de-identification.

One of these debates gravitated around a paper published by Cavoukian and Castro in 2014[148]. In the opinion of these authors, de-identification is the main mechanism to ensure that those privacy rights are assured. However, some computer science researchers as Arvind Narayanan have lately been indicating that there are several techniques nowadays to re-identify de-identified datasets. Cavoukian and Castro believe that such understanding is a myth which leads to a subsequent lack of trust in de-identification, making data custodians 'less inclined to provide researchers with access to much needed information'[149]. In fact, they believe that the risk of re-identification from anonymised datasets is considerably lower than indicated on primary literature. In the author's opinion, personal information may be anonymised in a way that mitigates re-identification risks while still assuring an elevated level of data quality, proving, in their

147 Ibid, p. 22

148 Ann Cavoukian and Daniel Castro, 'Big Data and Innovation, Setting the Record Straight: De-identification Does Work (2014)

149 Ibid

judgement, that de-identification is not impossible (in contrast with Narayanan and Felten) and that de-identified data should not be classified as Personally Identifiable Information[150].

Cavoukian and Castro commented Sweeney's[151] 2000 study by which - based on 1990's US census data - she concluded that 87 per cent of the population in the United States could be identified by combining gender, date of birth and ZIP code. Their interpretation is that "*commentators should not simply rely on this early research as definitive evidence that datasets containing personal information cannot be effectively de-identified*"[152] and based their opinion on a similar study conducted by the Palo Alto Research Centre which replicated Sweeney's study with data from 2000 with an identifiability percentage of 63 per cent. When referring to this study, the authors seem to reach an obvious conclusion, that is that the 'risk of unique identification drops off sharply when given slightly more abstract data[153]', i.e. if we can replace date of birth with month or ZIP code with country, the odds of positively identifying individuals will be much lower. But such conclusion and other similar interpretations done by the authors does not prove that de-identification does in fact work (hence the title of their article), it merely demonstrates the difference between processing detailed personal datasets or more ambiguous or abstract datasets, which, in terms of the latter, earlier authors have already defended that makes anonymisation much effective.

Cavoukian and Castro also commented Sweeney's re-identification of Governor Weld's health records, defending that to cite this case 'as evidence against current de-identification standards is highly misleading'[154]. Narayanan and Felten strongly oppose that view as they defend that all that Sweeney needed in order to re-identify the governor was his gender, date of birth, and ZIP code, which were accurate in the voter database.[155] And while Cavoukian and Castro concluded that 'there was zero risk for individuals not appearing in the voter database', Narayanan and Felten still found such statement to be incorrect as those individuals 'would be at risk of identification by anyone who could learn their gender, date of birth, and ZIP code'[156], which meant that if the governor's data

150 Narrow definition of personal data used in North America
151 *Sweeney* (n 59)
152 *Cavoukian and Castro* (148)
153 Ibid
154 Ibid
155 Arvind Narayanan and Edward Felten, 'No silver bullet: De-identification still doesn't work' (2014)
156 Ibid

would lack from the voter database, anyone could still re-identify him by using public information.

Narayanan and Felten were even more critical of Cavoukian and Castro's position on the Netflix case. Narayanan was one of the two researchers who in 2008 published a report[157] in which they positively identified Netflix users by comparing dates and ratings given to movies in an anonymous dataset with similar personal data on IMDB. Cavoukain and Castro defended the study was not relevant as the authors were merely able to re-identify two out of 480,189 Netflix users, but forgot to state an evidence, which is that those "results should (…) be viewed as a proof of concept"[158], which misses the point made by Narayanan and Felten, who by using an analogy replied: 'If someone made a video showing that a particular car security system could be hacked, it would be an error to claim that there is nothing to worry about because only one out of 1,000,000 such cars had been compromised'[159]. Narayanan & Felden concluded by stating that the most important part of the Netflix report was to demonstrate that if an individual is able to know 'a little bit about the movie preferences of a user in the Netflix dataset, there's an upwards 80% chance of identifying that user's record in the dataset' and, with this in mind, it is self-evident that Cavoukian and Castro failed on suggesting any de-identification methods for the Netflix dataset.

An interesting statement made by Cavoukian and Castro was that 'in the case of high-dimensional data, additional arrangements may need to be pursued, such as making the data available to researchers only under tightly restricted legal agreements'[160]. This says nothing in terms of how de-identification would be operated in high-dimensional datasets, which are nowadays the norm, not the exception[161]. Being a high-dimensional dataset one with a large number of attributes or features, it is easy to understand that social media networks represent high-dimensional datasets as we may be presented with hundreds of dimensions per connection. If we connect this to the recent Facebook-Cambridge Analytica developments[162], we can easily see how, through behavioural micro-targeting,

---

157 Arvind Narayanan and Vitaly Shmatikov, 'Robust De-anonymisation of Large Sparse Datasets", (Proceedings of the 2008 IEEE Symposium on Security and Privacy 2008) <https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf>

158 Ibid

159 *Narayanan and Felten* (n 155)

160 *Cavoukian and Castro* (148)

161 *Narayanan and Felten* (n 155)

162 Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' (2018) The Guardian <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

every user has hundreds of pages and connections associated with them, thus allowing for strong unique identification.

In summary, it seems evident that Cavoukian and Castro, although correctly defending that de-identification is one of the most effective ways of protecting individuals' privacy, they seem to fail on providing evidence that de-identification undeniably works. The authors seem to reject re-identification theories (and proven cases) while avoiding to provide practical solutions and preferring to provide generalisations as 'organisations should perform an initial risk-assessment, taking into account the current state of the art in both de-identification techniques and re-identification attacks'[163], or 'a governance structure should be in place that enables organizations to continually assess the overall quality of their de-identified datasets[164]. Statements like these, although correct, do not provide any clarification on the controverted topic, being the effectiveness of de-identification techniques. On another example, the authors state that "*in many cases (...) it is possible to strongly de-identify the data (...) while at the same time preserve the required level of data quality necessary for data analysis*"[165], however, the only case that the authors can provide is the above-mentioned US Heritage Health Prize.

In their conclusion, the authors state that 'when researchers discover a new technique for re-identifying data, this should be seen as an opportunity to improve de-identification techniques, not as an indictment of the utility of creating anonymised datasets[166]. I am not saying that re-identification discoveries should be seen as any kind of indictment but is not that the purpose of the discovery? i.e. the scientific challenge seems to be to re-identify datasets to prove that those datasets are not as anonymous as they seemed. Although one can still see it as an opportunity to improve de-identification, if someone proves that a dataset is not completely anonymous and therefore the data contained in it may then be re-identified, it has been proved the lack of effectiveness of that specific de-identification technique on that specific dataset, which per se is of scientific value.

4.2.ANONYMISATION TECHNIQUES

There are several techniques that can be used to ensure anonymisation. Applying the techniques below will ideally ensure that the link between the individual and his

163 *Cavoukian and Castro* (148)
164 Ibid
165 Ibid
166 Ibid

personal information is adequately broken. If applied correctly, the process would make it impossible to reverse engineer the anonymisation procedure, which would significantly reduce privacy exposure and protect and preserve individuals' personal information.

Suppression

Suppression is probably the easiest and simplest anonymisation technique there is. Consider the deletion of a specific set of data fields containing personal information from a database before sharing it with a third party. In this case, even though the database was shared with e.g. a supplier, from its analysis there cannot be a positive identification of a living individual as all the identifiers, along with any identifiable attribute, have been suppressed or deleted.

Data Masking - Removal of personal identifiers

To share certain databases with third parties, a controller can sometimes remove personal identifiers (names, social security numbers, etc.) and contextual personal identifiers - i.e. information that, in the given context can also act as personal identifiers – student ID (university), bank account (bank), customer ID (retailer).

Personal identifiers are a subset of personal data by which someone can be identified by assumption. For a unique individual to be identified, depending on the identifiers, they can be used: by themselves; they can be combined with an individual's name; they can be combined with other personal identifiers data fields; and they can be combined with other personal data fields.

Aggregation

By aggregating data, no sets relating to or identifying any individual are displayed, as data is displayed as totals. Aggregation techniques (as inference control, perturbation, rounding, sampling, synthetic data or tabular reporting) are known for their low risk as it will be difficult to find anything about a particular individual by using aggregated data'[167].

Regarding aggregation and k-anonymity, WP29 highlights the importance of these techniques as they group data subjects with other data subjects to prevent them from being singled out, meaning that data subjects share the same attribute values, as they are generalized. WP29 explains by exemplifying that more individuals shall be included if we 'lower the granularity of a location from a city to a country'[168].

---

167 Information Commissioner's Office, 'Anonymisation: managing data protection risk code of practice' (Guidance 2014) 53
168 WP29 (n 47) 16

Micro-aggregation

When operating on an observed value, this technique, can allow for anonymisation of a specific group of sets of data by replacing those values 'with the average computed on a small group of units'[169].

Derived data

This is another low-risk re-identification exposure technique as it turns data-matching difficult or impossible. Derived data (which hides original values but reflects the character of the source data) is normally used through banding techniques 'to produce coarser-grained descriptions of values than in the source dataset e.g. replacing dates of birth by ages or years, addresses by areas of residence or wards, using partial postcodes or rounding exact figures so they appear in a normalised form'[170].

Removing variables

This is one of the simplest anonymisation methods. It entails the removal of specific variables that can provide direct or indirect identifiers from a data file. Certain variables 'can be removed if deemed too sensitive for public use or irrelevant for analytical purpose'.[171]

Local suppression

The finality of this method is to minimise the information content of rare combinations to produce an increase in 'the frequency count of records containing the modified combination'[172]. This will consist of deleting an observed value and inserting a "missing" value as a replacement. The ICO believes that it should nevertheless be only applied to 'records that contain combinations at risk'[173].

L-Diversity/T-Closeness

Through l-diversity, deterministic attacks are no longer possible. To create greater uncertainty to a prospective attacker with background knowledge on a specific individual, it will be possible to 'limit the occurrence of equivalence classes with poor attribute variability'[174]. It can be said that t-closeness is an upgrade to l-diversity as its main objective is to 'create equivalent classes that resemble the initial distribution of

169 Ibid, 90
170 ICO (n 73)
171 Ibid 82
172 Ibid 88
173 Ibid 89
174 Ibid 18

attributes in the table'[175]. T-closeness will be more advantageous in situations where it will be paramount to maintain the data as similar as possible to the initial one.

4.3.PSEUDONYMISATION TECHNIQUES

Although WP29 clearly states that pseudonymisation is not a method of anonymisation, in its opinion on Anonymisation Techniques it includes some examples of pseudonymisation techniques. I will then summarise five of the most used pseudonymisation techniques as described on WP29 opinion 05/2014[176].

Encryption with secret key

Through this technique, a key-holder may be able to re-identify individuals by decrypting the dataset as the identifiable information is still contained on that dataset. Decryption however will only be possible with knowledge of the key.

Hash function

Through a hash function, a fixed sized output will be returned 'from an input of any size'[177], which impedes reversion, meaning it no longer exists the reversal risk as seen with encryption. However, as this technique is designed to be fast to compute, implementing it may result on systems susceptible to brute force attacks.

Keyed-Hash function with stored key

This technique is similar to the previous one with the exception of using a secret key as 'an additional input'[178], meaning that the data controller will be able to 'replay the function on the attribute using the secret key, but it is much more difficult for an attacker to replay the function without knowing the key as the number of possibilities to be tested is sufficiently large as to be impractical'[179].

Deterministic encryption of key-hashed function with deletion of the key

This technique will reduce the risk of linking personal information in a certain dataset to personal information from the same data subject in a different dataset where another pseudonym is being used. The technique could be explained as selecting a 'random number as a pseudonym for each attribute in the database and the deleting the correspondence table'[180]. It is very difficult for an external agent to decrypt the function

175 Ibid
176 Ibid 20
177 Ibid, p.20
178 Ibid
179 Ibid
180 Ibid, p.21

as that would mean that he would have to test every possible key, as the key is not available.

Tokenisation

Tokenisation is normally used by financial service providers to 'replace card ID numbers by values that have reduced usefulness for an attacker'[181]. It involved the assignment of a sequence number or a "randomly generated number that is not mathematically derived from the original data'[182].

V. CONCLUSION – THE FUTURE OF ANONYMISATION AND PSEUDONYMISATION.

In 2010, Paul Ohm warned of the failure of contemporary anonymisation techniques and the unfulfilled promises they offered in terms of privacy protection, urging regulators to assess the new risks introduced by re-identification while carefully balancing them against relevant countervailing values. In his view, re-identification had lifted a veil that had for too long "*obscured privacy debates"*[183].

Against this backdrop, early drafts of the GDPR raised expectations that anonymisation would feature prominently as a means of protecting personal data. However, much like the DPD, the GDPR does not include anonymisation within the core scope of data protection principles. Given the rapid evolution of data analytics and processing capabilities, absolute anonymisation is becoming increasingly difficult to achieve. Faced with this reality, regulators began to shift focus towards formally recognising pseudonymisation within the text of the Regulation. This evolution is reflected in the numerous documents—opinions, proposals, and amendments—issued by the EU Commission, the EDPS, WP29, LIBE, IMCO, ITRE, JURI, the EU Parliament, and the EU Council, as well as the outcome of the Trilogue negotiations.

One of the most relevant contributions was the WP29's opinion on anonymisation techniques, which recommended a case-by-case approach to evaluating their effectiveness. This approach remains highly relevant, as the accelerating pace of technological change will continue to challenge the viability of existing anonymisation

181 Ibid
182 Ibid
183 *Ohm* (n 30)

methods. If identifiability is assessed through a "reasonability test"[184], as set out in Recital 26, then absolute anonymity may be practically unattainable. To navigate these limitations, a shift toward *de facto* anonymisation has been suggested. Given its adaptability, *de facto* anonymity may offer a more effective and sustainable approach for assessing anonymisation, both today and in the future.

Another important insight from the GDPR concerns the definition of data processing. Article 4(2) defines processing as 'any operation or set of operations which is performed on personal data or on sets of personal data'[185]. Anonymising personal data falls within this scope, as it requires operations to be carried out on identifiable data before it becomes anonymous. As Walden argued under the DPD, if anonymisation constitutes processing, it must be carried out in compliance with data protection principles up to the point where data is rendered truly anonymous. This reasoning remains relevant under the GDPR and helps clarify its material scope in cases involving anonymisation processes.

Recital 26 of the GDPR explicitly refers to "all the means reasonably likely to be used"[186] when assessing whether data can be considered anonymous. This implies that data controllers must consider factors such as cost, time, and technological capability[187], which in turn requires ongoing reassessment of the effectiveness of their anonymisation strategies.

Although many expectations were raised around anonymisation during the development of the GDPR, it was ultimately left outside the Regulation's scope. This has led to interpretive uncertainty—particularly regarding which techniques are sufficient to achieve definitive anonymisation. While clearer legislative definitions might have addressed these gaps, codifying technical requirements could risk becoming outdated as technology advances. Rather than relying on legislative fixes, a more pragmatic solution would be the development of appropriate codes of conduct or certification mechanisms for both anonymisation and pseudonymisation (which still do not exist), as a way to calibrate "the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons."[188]

---

184 Recital 26 GDPR (n 3)
185 Article 4 (2) GDPR (n 3)
186 *Breyer* (n 18)
187 'Personal Data, Anonymisation & Pseudonymisation under European Data Protection Law, A Comparison of the DPD and the GDPR on the Example of Cloud Computing' (Thesis 2016) Faculty Of Law University of Oslo
188 Recital 98 GDPR (n 3)

The shift that led to the formal recognition of pseudonymisation left anonymisation as the ideal privacy-preserving method, while positioning pseudonymisation as a more workable compromise - offering risk reduction with a lighter compliance burden but retaining accountability. This explains why pseudonymisation is expressly covered under the Regulation, whereas anonymisation is not.

Pseudonymisation is, in fact, one of the most significant innovations introduced by the GDPR. Its growing importance is evident throughout the Regulation's legislative development. While pseudonymised data is closer to identifiable than to anonymised data—and remains within the scope of the GDPR - it offers considerable value as a privacy-enhancing tool. It is clear that the GDPR encourages data controllers to adopt pseudonymisation where feasible. When implemented effectively, it can reduce risks to data subjects, help controllers and processors meet their obligations, support the principles of data minimisation and privacy by design and by default, prevent easy identification of individuals, and contribute to an appropriate level of security for the processing of personal data.

As data ecosystems become increasingly complex and re-identification risks persist across sectors, the debate surrounding anonymisation and pseudonymisation will remain central to the future of data protection. While anonymisation may offer the highest theoretical level of privacy, its practical limitations require regulators, organisations, and researchers to adopt flexible, risk-based approaches. Pseudonymisation, by contrast, has proven to be a viable and scalable safeguard within the GDPR's legal framework. Moving forward, the development of practical tools—such as certification mechanisms, sector-specific codes of conduct, and robust technical standards—will be essential to bridge the gap between legal theory and operational reality. In this context, the value of both anonymisation and pseudonymisation lies not in abstract compliance, but in their capacity to enable responsible innovation while preserving fundamental rights in a data-driven world.

BIBLIOGRAPHY

Books

- Lloyd, Ian, *Information Technology Law* (Oxford University Press 2017)
- Reed, Chris, *Internet Law* (Cambridge University Press 2004)
- Walden, Ian, *Telecommunications Law and Regulation* (Oxford University Press 2012)

Articles

- Cavoukian, Ann and Castro, Daniel, 'Big Data and Innovation, Setting the Record Straight: De-identification Does Work (2014)
- Esayas, S.Y., 'The role of anonyimisation and pseudonomysation under the EU data privacy rules: beyond the 'all or nothing' approach' (2015) European Journal of Law and Technology, Vol 6, No 2
- Froomkin, Michael A. 'Pseudonyms by Another Name, Privacy in the Modern Age' (2015) The New Press
- Hon, W. Kuan, Millard, Christopher and Walden, Ian, 'The Problem of 'Personal Data' in Cloud Computing – What Information is Regulated? The Cloud of Unknowing, part 1' (2011) Queen Mary University of London, School of Law Legal Studies Research Paper No. 75
- Narayanan, Arvind and Felten, Edward, 'No silver bullet: De-identification still doesn't work' (2014)
- Narayanan, Arvind and Shmatikov, Vitaly, 'Robust De-anonymisation of Large Sparse Datasets", (Proceedings of the 2008 IEEE Symposium on Security and Privacy 2008) <https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf>
- Ohm, Paul, 'Broken Promises of Privacy: Responding to the surprising failure of anonymisation' (2009) 57 UCLA Law Review 1707
- Schaar, Peter, 'Data Protection and statistics – a dynamic and tension-filled relationship, Working Paper 82, German Council for Social and Economic Data', March 2009
- Sweeney, L., 'Simple Demographics Often Identify People Uniquely. Carnegie Mellon University' Data Privacy Working Paper 3 (2000) Pittsburgh
- Walden, Ian, 'Anonymising Personal Data, International Journal of Law and Information Technology' (2002) Vol. 10 No. 2, Oxford University Press

- ‘Personal Data, Anonymisation & Pseudonymisation under European Data Protection Law, A Comparison of the DPD and the GDPR on the Example of Cloud Computing’ (Thesis 2016) Faculty Of Law University of Oslo

Reports, Legislation and Opinions

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281
- Article 29 Working Party Opinion WP136 (2007)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119
- Information Commissioner’s Office, ‘Anonymisation: managing data protection risk code of practice’ (Guidance January 2014)
- Article 29 Data Protection Working Party, ‘Opinion 05/2014 on Anonymisation Techniques’ (10 April 2014)
- ICO, *Guidance on Wi-Fi location analytics* (February 2016)
- Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — ‘A comprehensive approach on personal data protection in the European Union’ (2011/C 181/01)
- European Commission Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - 5853/12. 27 January 2012
- Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012
- Opinion 01/2012 on the data protection reform proposals, Article 29 Data Protection Working Party, Adopted on 23 March 2012
- Opinion 08/2012 providing further input on the data protection reform discussions, Article 29 Data Protection Working Party, Adopted on 05 October 2012
- Working Document 2 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data

Protection Regulation), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht, 8.10.2012

- European Parliament Committee on Civil Liberties, Justice and Home Affairs, ***I Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 16.1.2013
- European Parliament Committee on the Internal Market and Consumer Protection, opinion on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 28 January 2013
- European Parliament Committee on Industry, Research and Energy, opinion on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 26 February 2013
- European Parliament Committee on Legal Affairs, on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 25 March 2013
- European Parliament Committee on Civil Liberties, Justice and Home Affairs amendments on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
- European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))
- Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the

processing of personal data and on the free movement of such data (General Data Protection Regulation), 9565/15, 11 June 2015

- European Data Protection Supervisor, Opinion 3/2015 (with addendum) Europe's big opportunity, EDPS recommendations on the EU's options for data protection reform, 27 July 2015 (updated with addendum, 9 October 2015)
- Trilogue outcome proposal - Regulation (Eu) No Xxx/2016 of the European Parliament and of the Council, 17 December 2015 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
- Information Commissioner's Office, 'An introduction to the Data Protection Bill'
- Information Commissioner's Office, 'Anonymisation: managing data protection risk code of practice' (Guidance 2014)

Digital Sources

- Arvind Narayanan and Vitaly Shmatikov 'How to Break the Anonymity of the Netflix Prize Dataset' (2006) ARVIX <http://arxiv.org/abs/cs/0610105v1>
- Slaughter and May, 'Personal data, anonymisation and pseudonymisation under the GDPR' (Publication July 2016) https://www.slaughterandmay.com/media/2535637/personal-data-anonymisation-and-pseudonymisation-under-the-gdpr.pdf
- Martin Munz, Tim Hickman and Matthias Goetz, 'Court confirms that IP addresses are personal data in some cases'(Publication White & Case 31 October 2016) <https://www.whitecase.com/publications/alert/court-confirms-ip-addresses-are-personal-data-some-cases>
- Mike Hintzeand Khaled El Emam, '*Comparing the Benefits of Pseudonymisation and Anonymisation Under the GDPR'* (Privacy Analytics White Paper 17 November 2017) https://iapp.org/media/pdf/resource_center/PA_WP2-Anonymous-pseudonymous-comparison.pdf
- The Netflix Prize Rules, http://www.netflixprize.com/faq
- Tom Zeller and Michael Barbaro Jr. 'A Face Is Exposed for AOL Searcher No. 4417749' (9 August 2006) The New York Times <http://www.nytimes.com/2006/08/09/technology/09aol.html>
- --, 'Google defies use over search data' *BBC* (20 January 2006) <http://news.bbc.co.uk/2/hi/technology/ 4630694.stm>

- Alison Deighton, 'Data Protection Bill under review by Parliament' (2017) Lexology <https://www.lexology.com/library/detail.aspx?g=1c4ec2ab-921b-4eee-9f88-e4d3d4549d2a>
- HelpNetSecurity, 'Tor Browser flaw leaks users' real IP address' (2017) <https://www.helpnetsecurity.com/2017/11/06/tor-browser-ip-leak/>
- Gabe Maldoff, 'Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization', IAPP <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/>
- Dataguise, 'Data Minimization in the GDPR: A Primer' (2017) <https://www.dataguise.com/gdpr-compliance-data-minimization-use-purpose/>
- Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' (2018) The Guardian <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

Cases

- Case C-582/14 *Breyer v Brundersrepublik Deutschland*
- Efifiom Edem v Information Commissioner and The Financial Services Authority [2014] EWCA Civ 92
- Google Inc v Vidal-Hall, [2014] EWHC 13 (QB)
- Case C-101/01 *Lindqvist*

Case C-70/10 – *Scarlett Extended*

CYBERLAW

BY CIJIC

A DIPLOMACIA E OS SEMICONDUTORES NO CAMINHO DA GEOPOLÍTICA DO CIBERESPAÇO

HÉLDER FIALHO JESUS

RESUMO

A geopolítica do ciberespaço[1] reflete as disputas estratégicas entre grandes potências, com destaque para a rivalidade entra os Estados Unidos da América (EUA) e a China. O ciberespaço deixou de ser apenas um domínio tecnológico, tornando-se uma arena de competição por inovação, segurança e influência. Nos últimos anos, a China tem desafiado a liderança tecnológica dos EUA por meio de avanços em áreas como a inteligência artificial, o 5G e os semicondutores (chips). Por sua vez, estes países acusam-se mutuamente de ciberespionagem e disputam o estabelecimento de normas globais, com o enfoque na ciberdiplomacia, com os EUA a defender uma internet aberta e a China a promover a soberania digital. Este confronto ocorre no contexto da desglobalização, marcada por uma fragmentação económica e digital. A guerra tecnológica e a busca pela soberania digital impulsionam a criação de ecossistemas tecnológicos nacionais, com destaque para os semicondutores, aprofundando a divisão do ciberespaço em blocos, onde as cadeias de abastecimento são um fator fundamental. Neste contexto, a União Europeia vive um dilema, na medida em que a relação política com o outro lado do Atlântico não é acompanhada na área económica, sendo os semicondutores um elemento claro desta realidade. Como resultado, a integração global cede lugar a uma competição estratégica que está a redefinir uma nova ordem mundial.

Palavras-chave: Globalização, Fragmentação, Competição Estratégica, Ciberdiplomacia, Diplomacia Digital, Semicondutores, Chips Act.

ABSTRACT

The geopolitics of cyberspace reflects strategic disputes between great powers, with emphasis on the rivalry between the United States of America and China. Cyberspace is no longer just a technological domain but has become an arena for competition for innovation, security, and influence. In recent years, China has challenged US technological leadership through advances in areas such as artificial intelligence, 5G, and semiconductors (chips). In turn, these countries accuse each other of cyberespionage and compete to establish global standards, focusing on cyber diplomacy, with the US defending an open internet and China promoting digital sovereignty. This confrontation occurs in the context of deglobalization, marked by economic and digital fragmentation. National technological ecosystems are being built because of technological war and the search for digital sovereignty. These ecosystems focus on semiconductors and further divide cyberspace into blocks, with supply chains playing a key role. In this context, the European Union is confronted with a dilemma, as the political relationship with the other side of the Atlantic is not followed in the economic area, with semiconductors being a clear element of this reality. As a result, global integration gives way to strategic competition that is redefining a new world order.

Keywords: Globalization, Fragmentation, Strategic Competition, Cyberdiplomacy, Digital Diplomacy, Semiconductors, Chips Act.

1 Ciberespaço - consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação. Ref: *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. https://www.cncs.gov.pt/pt/estrategia-nacional/ .

I. INTRODUÇÃO

Nos últimos anos, a geopolítica do ciberespaço emergiu com relevância crescente nas relações internacionais, refletindo as dinâmicas de poder entre as principais potências mundiais. O ciberespaço deixou de ser apenas um domínio tecnológico para se tornar um palco de disputas estratégicas, onde interesses políticos, económicos e de segurança convergem. Nesse contexto, a competição entre os EUA e a China ocupa o centro das atenções, simbolizando uma nova fase da ordem mundial marcada por uma inflexão na globalização vivida desde os finais do século passado.

A globalização, que de forma simples pode ser considerada como um sistema mundial instantâneo de comunicação, comércio e finanças, tem tido muitos comentadores a anunciar a sua sentença de morte desde 2008. Tal situação deve-se às alterações sentidas na Organização Mundial do Comércio[2] desde essa data, a que se associou a crise financeira de 2008/2009, sendo esta realidade caraterizada pelo termo "*Slowbalization*"[3]. Neste sentido pode ainda falar-se numa "*Fragmentegration*"[4], que se carateriza por uma fragmentação da economia global e integração regional simultânea. Considera-se ainda que a fragmentação da internet, que decorre da sua divisão em redes menores e isoladas, é impulsionada por fatores como ações governamentais, diferenças tecnológicas e comerciais, e alterações no modelo de governança multissetorial[5]. Esta fragmentação tem impactos diretos na sociedade, na economia e ameaça os direitos humanos fundamentais, limitando a liberdade de expressão e o acesso à informação.

Por sua vez, o rápido crescimento das tecnologias de informação e comunicação (TIC) está a alterar significativamente as relações internacionais e a política no século XXI. As redes digitais, onde cada vez mais assentam as relações entre as pessoas e entre estas e os governos, revelam-se com novas formas de poder descentralizado refletindo mudanças

---

2 Thomson, Stéphanie (2024). Is globalization dying? An economic historian weighs up the evidence. *WEF*. https://www.weforum.org/stories/2024/08/globalization-dying-economic-historian-evidence-adam-tooze/

3 The Economist (2019). The steam has gone out of globalization. https://www.economist.com/leaders/2019/01/24/the-steam-has-gone-out-of-globalisation .

4 Roloff, Ralf (2024). Goodbye Globalization? Hello 'Fragmentegration'! - The World Economy and Strategic Competition. Connections QJ 23, no. 2 (2024): 191-202. https://doi.org/10.11610/Connections.23.2.02 https://procon.bg/system/files/23.2.02_fragmentegration.pdf?download=1 .

5 Global Partners Digital (2024). Regional Perspectives on Internet Fragmentation. https://www.gp-digital.org/publication/regional-perspectives-on-internet-fragmentation-a-summary-of-reports-from-the-europe-latin-america-sub-saharan-africa-and-asia-pacific-regions/ .

fundamentais na estrutura dos sistemas de informação nas sociedades modernas. O comércio, as comunicações pessoais e a comunicação de massas, que constituem as três principais redes de informação das relações internacionais[6], evoluíram ao longo dos séculos. Hoje, pela primeira vez na história, tem-se esta tripla mudança de paradigma que converge para uma infraestrutura comum – o ciberespaço.

O mundo hoje vive a quarta revolução industrial, que transforma os nossos contextos económicos, sociais, ecológicos e culturais, numa rápida mudança onde as tecnologias emergentes desempenham um papel fundamental, conforme refere Klaus Schwab[7], presidente do *World Economic Forum* (WEF). Esta realidade assenta numa situação inversamente proporcional entre a dimensão dos sensores e a sua capacidade envolvendo cada vez mais a Inteligência Artificial (IA) para a ligação dos mundos físico e virtual. Mas, para tal, três elementos são fundamentais, nomeadamente os dados, a informação e a comunicação.

A realidade digital atual carateriza-se pelo enorme volume de dados gerado, na medida em que qualquer ação, por mais simples que seja, gera dados, como seja uma busca na internet, uma publicação nas redes sociais ou uma compra online. Esta situação origina grandes desafios, pois verifica-se que esta enorme quantidade de dados é gerada de forma continua, e contribui para a obtenção de informação valiosa na geração de conhecimento, apoio à decisão, melhoria de indicadores de desempenho (KPI[8]) e diagnósticos, entre outros muitos casos. Estes dados, conhecidos como *Big Data* não podem ser geridos, processados ou analisados eficazmente utilizando os métodos tradicionais, tornando-se elementos presentes no nosso dia a dia. Por sua vez, a forma como recolhemos, gerimos e analisamos a informação também se vai modificando, naturalmente.

O estudo de enormes quantidades de dados tendo em vista retirar padrões de comportamento, descobrir correlações desconhecidas e conhecer as tendências designa-se por *Big Data Analytics*. Verifica-se então, que a IA e o *Big Data* têm associações colaborativas como refere Muhammad Tariq[9], na medida em que o *Big Data Analytics* tem de controlar a IA para uma melhor analise dos dados e a IA necessita de uma maior

6 US State Gov (2017). 21st Century Statecraft. https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy_USA.html .
7 Schwab, Klaus (2016). The Fourth Industrial Revolution, World Economic Forum, Geneva, Switzerland.
8 KPI – *Key Performance Indicator.*
9 Tariq, Muhammad (2024). AI-Driven Learning and Engagement in Higher Education, IGI Global Scientific Publishing, DOI: 10.4018/979-8-3693-4074-5 .

quantidade de dados para aprender e melhorar o seu processo de decisão. Pode assim dizer-se que o termo *Big Data* pressupõe um conjunto vasto de dados e situações associadas, naquilo que se designa por 5V[10], cujas características são: (1) Valor - que decorre da descoberta de *insights* e do reconhecimento de padrões potenciando a otimização dos processos/operações, sendo o "V" mais importante na perspetiva do negócio; (2) Variedade - a diversidade e a obtenção de diferentes tipos de dados, nomeadamente dados estruturados (como bases de dados) e dados não estruturados (como publicações nas redes sociais ou dados de sensores); (3) Velocidade - a celeridade como são recebidos, armazenados e geridos os dados, geralmente medido em terabytes ou petabytes; (4) Veracidade - a qualidade e fiabilidade dos dados, uma vez que o *Big Data* pode incluir muitas vezes ruído e inconsistências; e (5) Volume - a dimensão e as quantidades de *Big Data* que é gerido e analisado.

Daqui podemos verificar que as tipologias e os padrões culturais vão influenciar os resultados obtidos. Recente, em setembro de 2024, a União Internacional das Telecomunicações, a agência da ONU especializada em tecnologias de informação e comunicação publicou o relatório "*ICT Development Index*" (IDI)[11] tendo em vista apresentar os progressos dos países em direção a uma conectividade universal. No caso de países desenvolvidos e de grande dimensão, como os EUA, em que a sociedade assenta na utilização do digital, são carregados enormes volumes de dados. Sendo o inglês a língua mais universal, então o "seu" *Big Data* irá servir de base às respostas apresentadas pela IA, fazendo com que estes padrões sejam então mais disseminados pelo resto do mundo, numa resposta global que vai assentando cada vez ainda mais nestes padrões. Esta situação leva a uma assimilação, o que pode ser naturalmente preocupante, levando a uma forma única de estar, limitando a diversidade e o espírito crítico.

Como as transformações globais levam o seu tempo, alude-se aqui ao Relatório do projeto *Europe's Digital Power*[12], realizado pelo Conselho Europeu dos Negócios Estrangeiros, entre dezembro de 2015 e fevereiro de 2017. Este assenta em dois pressupostos: (1) que, à escala internacional, o poder económico e político está a ser redistribuído de acordo

10 Institute of Data (2023). Why Big Data is Important: Exploring Its Benefits and Uses. https://www.institutedata.com/blog/why-big-data-is-important/ .
11 International Telecommunication Union (2024). ICT Development Index. https://www.itu.int/itu-d/reports/statistics/idi2024/ .
12 Soesanto Stefan (2017). Europe's Digital Power: from Geo-economics to Cybersecurity. *European Council on Foreign Relations* https://ecfr.eu/wp-content/uploads/DIGITAL_POWER_PROJECT_REPORT_13_April_pages.pdf .

com as novas realidades de um mundo digital interligado; e (2) a União Europeia é um gigante económico, mas não uma união política nem um mercado digital totalmente integrado, encontrando-se mal preparada para competir nas esferas geoeconómicas e geopolíticas da altura e do futuro. Podemos dizer que esta situação se tem vindo a acentuar, como o relatório "*The future of European competitiveness, a competitiveness strategy for Europe*"[13], também conhecido como relatório Draghi, assim o mostra.

Do outro lado do Atlântico, em agosto de 2024, o *Congressional Research Service* (2024)[14] publicou o "*Great Power Competition: Implications for Defense - Issues for Congress*", onde refere que na última década se verificou o surgimento de uma crescente competição dos EUA com a República Popular da China (RPC ou China) e com Federação Russa (Rússia) - frequentemente chamada de competição entre grandes potências (GPC) ou competição estratégica. Em questão está a forma como o planeamento e o orçamento de defesa dos EUA devem responder a esta rivalidade e se devem aprovar, rejeitar ou modificar a atual estratégia de defesa, os níveis de financiamento, os planos e os programas propostos no contexto desta competição estratégica. As decisões do Congresso sobre estas questões podem ter implicações significativas para as capacidades de defesa dos EUA, bem como para a sua base industrial de defesa. No contexto do presente documento, dos 14 pontos ali referidos, relevam-se três: (1) *Innovation and speed of U.S. weapon system development and deployment*; (2) *Supply chain security, meaning awareness and minimization of reliance in U.S. military systems on components, subcomponents, materials, and software from non-allied countries, particularly China and Russia*; e (3) *Capabilities for countering so-called hybrid warfare and gray-zone tactics*.

Assim, verifica-se que as tecnologias não só estão a avançar rapidamente para o campo de batalha, como também são objeto de tensões internacionais[15]. Os governos de todo o mundo procuram uma maior vantagem tecnológica e autonomia, utilizando barreiras comerciais, controlos de exportação/investimento e políticas industriais para remodelar os fluxos de dados e as cadeias de abastecimento globais. Para tal, irão contar com o seu poder diplomático na cena internacional para fazer prevalecer os seus interesses,

13 European Commission (2024). The future of European competitiveness, a competitiveness strategy for Europe. https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en .
14 Congressional Research Service (2024). Great Power Competition: Implications for Defense—Issues for Congress. https://sgp.fas.org/crs/natsec/R43838.pdf .
15 Feakin, Tobias (2024). Navigating the New Geopolitics of Tech. *Harvard Business Review*. https://hbr.org/2024/11/navigating-the-new-geopolitics-of-tech .

assentando muitos destes na componente económica, onde a componente tenológica é cada vez mais um fator relevante. Complementarmente, importa referir que a competição entre as grandes potências tem vindo a crescer, e as atividades na chamada "zona cinzenta", num contexto cada vez mais híbrido, são viabilizadas pela tecnologia e estão a tornar-se mais comuns na política, num ambiente mais dinâmico e contestado[16].

Assim, a geopolítica do ciberespaço contempla a disputa por diversas áreas ao nível do controlo, influência e segurança. Nelas podem englobar-se as infraestruturas digitais, as redes de comunicação e os fluxos de dados, os quais sustentam a economia global. Mas esta competição é igualmente visível nas suas políticas de regulação e proteção de dados, através da diplomacia no contexto da sua governação, bem como por ações especificas no ou através do ciberespaço, no exercício do poder dos Estados, essencialmente através da componente militar, recorrendo a atividades maliciosas abaixo do limiar do conflito armado, como ciberataques ou espionagem.

Desta forma, pretende-se com este artigo apresentar uma reflexão sobre a geopolítica do ciberespaço, assente em alguns elementos de diplomacia, concretamente ao nível da ONU, da UE e dos EUA, com relevo para as áreas da governação e da economia. Ainda sobre esta última, apresentar alguns elementos orientados para o setor dos semicondutores, pela importância que têm na sociedade atual.

II. ELEMENTOS DE DIPLOMACIA PARA A GEOPOLÍTICA DO CIBERESPAÇO

O trabalho da diplomacia, que envolve as interações entre representantes de Estados soberanos, tem sentido nos últimos tempos uma mudança devido às novas TIC. Assim, verifica-se nas características distintivas da arte de governar do século XXI, o apontar para um caminho com mudanças profundas que irão gradualmente atravessar toda a política externa, pela expansão do seu âmbito, na utilização de novas ferramentas e levando mesmo à mudança dos seus valores[17].

16 Australia Gov (2021). Australia's International Cyber and Critical Tech Engagement Strategy. https://www.dfat.gov.au/sites/default/files/international-cyber-critical-technology-engagement-strategy-2021.pdf .
17 US State Gov (2017). 21st Century Statecraft.

Uma vez que os riscos do ciberespaço são quase sempre transnacionais, tal como a própria tecnologia, é necessário um nível sem precedentes de coordenação, envolvimento e cooperação internacional para combater as ameaças. Concomitantemente, importa abraçar e impulsionar o potencial económico e social que o ciberespaço oferece. O esforço diplomático deve também ser transversal porque os desafios de segurança, económicos e de direitos humanos no ciberespaço estão frequentemente interligados.

A utilização de termos específicos para caraterizar fases de momentos na sociedade tem sido uma caraterística recorrente, naquilo que se pode designar de "moda". No que ao desenvolvimento tecnológico diz respeito, tem-se como exemplo a utilização dos termos:

- Ciber: Derivado de "ciberespaço", referindo-se ao mundo virtual da informática e das redes de computadores. Envolve aspetos como cibersegurança[18], ciberespaço e atividades realizadas online - final do século XX;

- E-: Prefixo que significa "eletrónico", para denominar serviços ou atividades realizadas por meio eletrónico, como e-commerce (comércio eletrónico), e-learning (aprendizagem eletrónica) e *e-government* (governo eletrónico) - início do século XXI;

- Digital: Termo amplo que se refere à representação de dados em formato binário (dígitos). Abrange tecnologias, dispositivos e processos que utilizam dados digitais, como transformação digital, economia digital e comunicação digital - a partir de 2010;

- Big Tech: Relativo às grandes empresas de tecnologia que dominam o mercado global, as designadas *Big Tech*, como as Google, Apple, Meta, Amazon e Microsoft (GAMAM)[19]. Estas empresas influenciam significativamente a economia digital, a privacidade de dados e as políticas de Cibersegurança, sendo atualmente verdadeiros atores geopolíticos, com influência na guerra e na paz[20] - com maior ênfase a partir de 2015.

---

18 Cibersegurança - consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem. Ref: *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. https://www.cncs.gov.pt/pt/estrategia-nacional/ .

19 GAMAM, anteriormente conhecidas pelo acrónimo de GAFAM (Google, Apple, Facebook, Amazon, Microsoft).

20 Cronin, Audrey (2023). How Private Tech Companies Are Reshaping Great Power Competition. *Henry A. Kissinger Center for Global Affairs at the Johns Hopkins University School of Advanced International*

Por sua vez, estas situações foram replicadas na área diplomática, com o atraso inerente pelas diferenças de abordagem à realidade dos temas e pela situação burocrática associada. Por outro lado, também trazem complexidade e dificuldade conceptual, pois existe falta de consenso sobre a terminologia a ser utilizada para descrever a interseção entre diplomacia e tecnologia. Esta ambiguidade foi identificada e exposta pelo *Government Accountability Office* (GAO)[21] dos EUA, em janeiro de 2024, pela dificuldade que acarreta na ação diplomática, onde a linguagem é crucial para uma ação eficaz.

No fundo, pode dizer-se que existe uma confusão terminológica e conceptual em torno da "diplomacia digital", "ciberdiplomacia" e "diplomacia tecnológica". Verifica-se que o termo "ciberdiplomacia" será mais apropriado para negociações ligadas à cibersegurança, à governação da internet, aos direitos digitais ou no combate ao cibercrime, onde a componente legal tem uma grande preponderância. Uma outra forma deste termo ser utilizado é através das *confidence-building measures* (CBM), que visam o apoio aos países em desenvolvimento para a melhoria das suas infraestruturas de cibersegurança, tendo em vista a ciber-resiliência. Ao fornecer assistência técnica, formação e recursos, estas iniciativas podem elevar a postura geral da cibersegurança global, dificultando a exploração de ciberameaças no sistema internacional[22]. Por seu lado, o termo "diplomacia tecnológica" focar-se-á mais na componente tecnológica, envolvendo o relacionamento entre os governos e os gigantes tecnológicos, ou a conflitualidade estratégica pelo domínio das tecnologias. Assim, a escolha do termo depende do contexto.

A este respeito, Jovan Kurbalija, na Diplo[23], recomenda a utilização do termo "digital" como sendo o mais preciso, pois abrange três aspetos: (1) o impacto da digitalização no ambiente geopolítico; (2) a emergência de temas digitais na agenda diplomática e (3) o uso de ferramentas digitais em atividades diplomáticas (ex.: negociações). Complementa

---

Studies. https://sais.jhu.edu/kissinger/programs-and-projects/kissinger-center-papers/how-private-tech-companies-are-reshaping-great-power-competition# .

21 GAO (2024). Cyber Diplomacy: State's efforts aim to support U.S. interests and elevate priorities. *United States Government Accountability Office*. https://www.gao.gov/assets/d24105563.pdf .

22 Lanceiro, R. (2024). The Importance of Cyber Diplomacy in International Relations Today. *IDN Brief*. https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2024/IDN%20brief%20junho%202024%20Cyberdiplomacy.pdf .

23 Kurbalija, Jovan (2024). Untangling digital, cyber, and tech diplomacy: A search for clarity of thinking and action. Diplo. https://www.diplomacy.edu/blog/untangling-digital-cyber-and-tech-diplomacy-a-search-for-clarity-of-thinking-and-action/ .

ainda reforçando a necessidade de os diplomatas compreenderem os fundamentos da tecnologia tendo em vista uma ação diplomática eficaz.

O ciberespaço tem um impacto cada vez mais notório nas sociedades e nas Relações Internacionais, levando a adaptações organizacionais, que no caso do mundo diplomático se materializa com o surgimento de novos cargos de embaixador[24]. Como alguns exemplos desta diversidade de situações temos o caso dos EUA que criaram o "*Office of the Coordinator for Cyber* Issues", em 2011, sendo o primeiro do género no mundo[25]. Alterações entretanto surgidas no panorama interno e externo deste país, levaram a que em 2022 fosse criado o "*Bureau of Cyberspace and Digital Policy*"[26]. Em Portugal, tem-se o Embaixador para a Ciberdiplomacia, desde 2016, acumulando em 2020 o cargo de Embaixador para a Diplomacia Digital[27]. Em 2017 a Dinamarca tornou-se o primeiro país a nomear um Embaixador para a Tecnologia[28] para representar o governo dinamarquês junto da grande indústria tecnológica. Releva-se a particularidade de chefiar uma organização com sede em Copenhaga e dois escritórios, um em Sillicon Valley e outro em Beijing, junto aos principais polos de inovação e para acompanhamento dos desenvolvimentos tecnológicos. Espanha, em 2018, teve a sua primeira Embaixadora para a Misión Especial para las Amenazas Híbridas y la Ciberseguridad[29].

A importância dos assuntos da diplomacia no Ciberespaço vai para além dos próprios Estados em si, havendo igualmente propostas de criação de cargos nas diversas organizações internacionais, sendo o G20[30] um exemplo.

Assim, a preocupação dos Estados com a necessidade de utilizar meios diplomáticos tradicionais nas discussões sobre políticas para o ciberespaço decorre da evolução sentida na dimensão digital, tendo André Barrinha referido que o ciberespaço, como domínio de

---

24 Jesus. H (2024). How important is the cyberdiplomacy to the deterrence in cyberspace? *IDN Brief*. https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2024/IDN%20brief%20junho%202024%20Cyberdiplomacy.pdf .

25 Painter, Chris (2018). The rise of the internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century. https://afsa.org/diplomacy-cyberspace .

26 US Department of State. https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/ .

27 https://expresso.pt/podcasts/o-futuro-do-futuro/2023-08-08-Os-valores-do-mundo-digital-chines-nao-sao-os-mesmos-que-os-nossos.-Sao-ate-rivais-recorda-embaixador-para-a-Diplomacia-Digital-52abf573 .

28 Office of Denmark's Tech Ambassador. https://techamb.um.dk/blog/denmark-seeks-to-strengthen-european-tech-diplomacy-and-global-engagement .

29 Agencia Estatal Boletín Oficial del Estado. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-3364 .

30 Torres, Mario & Riordan, Shaun (2020). The cyber diplomacy of constructing norms in cyberspace. Task Force 5 - The future of multilateralism and global governance. https://www.global-solutions-initiative.org/wp-content/uploads/2022/11/T20_TF5_PB4.pdf .

política internacional, foi diplomatizado[31], no que considera ser um novo campo diplomático. Neste campo, à semelhança de outros, importa o capital diplomático, tendo a sua centralidade na segurança do ciberespaço, para a elaboração de políticas para a prevenção de conflitos no ciberespaço. Por seu lado, refere igualmente a ambiguidade conceptual pela falta de consenso entre os diplomatas sobre uma definição exata para ciberdiplomacia e como ela difere de outros tipos de diplomacia.

i) Nações Unidas

O tema da segurança do ciberespaço está na agenda da ONU desde 1998, evoluindo ao longo dos anos através de *Groups of Governmental Experts* (GGE) e, mais recentemente, dos *Open Ended Working Group* (OEWG).

As primeiras considerações à escala internacional sobre a aplicação do direito internacional ao ciberespaço ocorreram então em 1998, com uma iniciativa russa que encorajou os Estados a expressarem as suas perspetivas sobre a segurança da informação e a "necessidade de formular princípios internacionais para reforçar a segurança dos sistemas globais de telecomunicações de informação e ajudar a combater o terrorismo e a criminalidade na componente informacional"[32].

Esta situação decorreu da preocupação com o uso indevido das TIC, cujas primeiras iniciativas se concentraram no seu uso estatal. Em 2003-2004 iniciou-se o processo dos GGE, mas não conseguiu chegar a acordo sobre um relatório devido a divergências sobre o impacto das TIC na segurança nacional e nos assuntos militares[33]. Desde então, surgiram seis grupos de trabalho de GGE; três destes grupos alcançaram resultados substantivos, que juntos formam o atual quadro da ONU, e que contribuíram para a construção de um entendimento comum entre os Estados. Esses relatórios[34] abordaram temas como a aplicação do direito internacional ao ciberespaço, a necessidade de normas de comportamento responsável dos Estados, medidas de fomento da confiança e a

31 Barrinha, André (2024). Cyber-diplomacy: The Emergence of a Transient Field. The Hague Journal of Diplomacy. https://brill.com/view/journals/hjd/19/3/article-p439_1.xml?ebody=full%20html-copy1 .
32 Schmitt, Michael & Johnson, Durward (2024). Cyber operations come of age. *Cadernos do IUM, nº59*, 5-22.
https://www.ium.pt/files/publicacoes/Cadernos/59/Cadernos_IUM_59_Military_Operations_Cyberspace.pdf .
33 Digital Watch - Geneva Internet Platform. https://dig.watch/actor/un-group-governmental-experts-developments-field-information-and-telecommunications-context .
34 Tiirmaa-Klaar, Heli (2021). The Evolution of the UN Group of Governmental Experts on Cyber Issues. *The Hague Centre for Strategic Studies and the Global Commission on the Stability of Cyberspace*. https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf .

importância da construção de capacidades. O quadro referido consiste em três pilares: (1) reconhecimento da aplicabilidade do direito internacional, (2) normas não vinculativas de comportamento dos Estados em tempo de paz, e (3) medidas de reforço da confiança no ciberespaço[35]. O GGE tem uma abordagem um pouco exclusiva e centrada no Estado para as normas para o ciberespaço. O GGE original era composto por peritos governamentais que representavam quinze Estados, número que foi crescendo até vinte e cinco em 2017. As reuniões do GGE são fechadas e não está presente qualquer outro observador mesmo governamental de outro Estado não participante, ou outras entidades não governamentais, o que pode ser considerado limitativo.

Em 2018, a Assembleia Geral da ONU foi confrontada com duas resoluções concorrentes. A Rússia propôs a criação de um OEWG, enquanto os EUA defenderam a continuação do formato tradicional do GGE. Ambas as resoluções foram adotadas, deixando a comunidade internacional com dois processos distintos com objetivos similares e a necessidade de encontrar uma forma de garantir que ambos produzissem resultados úteis.

A duplicação de processos representa um desafio para a diplomacia multilateral e pode ser vista como uma oportunidade se houver uma divisão lógica de trabalho entre o GGE e o OEWG[36]. Daniel Stauffacher, fundador e presidente do ICT4Peace, sugere que o GGE se devia concentrar na questão da aplicabilidade do direito internacional às operações dos Estados no ciberespaço, enquanto o OEWG, com sua maior participação e transparência, poderia desenvolver normas, medidas e acordos multilaterais para governar o comportamento estatal no ciberespaço. Esta opção decorre de o OEWG ter o potencial de incorporar contribuições do setor privado e da sociedade civil, conforme explicitamente estabelecido no seu mandato. A garantia de financiamento para as consultas com essas partes interessadas será crucial para o sucesso do processo.

O relatório final do último GGE (2019-2021)[37] foi aprovado por consenso, num período especialmente difícil, uma vez que as tensões entre os Estados estavam a aumentar devido a ciberataques em grande escala sem precedentes contra infraestruturas críticas, empresas

35 Ruhl, Christian; Ducan, Hollis; Hoffman, Wyatt & Maurer, Tim (2020). Cyberspace and Geopolitics-Assessing Global Cybersecurity Norm Processes at a Crossroads Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/Cyberspace_and_Geopolitics.pdf .

36 Stauffacher. D. (2019). UN GGE and UN OEWG: How to live with two concurrent UN Cybersecurity processes. ICT4Peace to Jeju Forum. https://ict4peace.org/wp-content/uploads/2019/11/ICT4Peace-2019-OEWG-UN-GGE-How-to-live-with-two-UN-processes.pdf .

37 Let's Talk Cyber. https://letstalkcyber.org/news/2019-2021-gge-adopts-final-consensus-report .

privadas e processos eleitorais. A adoção deste relatório foi crucial, uma vez que o anterior GGE (2016-2017) não conseguiu produzir um relatório final, sendo este passo agora visto como um aspeto positivo para a aplicação do direito internacional no ciberespaço e a promoção de um comportamento *on-line* responsável.

Por sua vez, o OEWG 2019-2021[38] também teve o seu relatório aprovado, o qual aborda temas como as ameaças existentes e potenciais; as regras, normas e princípios de um comportamento responsável pelo Estado; o direito internacional; medidas de reforço da confiança e de capacidades; e o diálogo institucional regular. Após a conclusão bem-sucedida da primeira ronda de negociações, que terminou com um Relatório Substantivo Final, o OEWG foi renovado em dezembro de 2020 para o período de 2021-2025 pela resolução A/RES/75/240[39]. Sobre o atual OEWG 2021-2025[40], pode referir-se que tem enfrentado alguns desafios, com a participação de atores não-estatais, que gerou alguma controvérsia, bem como a guerra na Ucrânia, que aumentou as tensões. No entanto, houve avanços em medidas de fomento da confiança e desenvolvimento de capacidades, havendo ainda pontos de discórdia que persistem quanto à aplicabilidade do direito internacional às TIC e à necessidade de novas normas. O OEWG publica relatórios anuais que servem como roteiros para negociações futuras. O terceiro relatório, publicado em julho de 2024, destaca a divergência sobre a aplicabilidade do direito internacional e normas de comportamento responsável, mas regista dois sucessos: o lançamento do Diretório de Pontos de Contato (POC) e a concordância sobre os elementos básicos do mecanismo que sucederá o OEWG.

De acordo com o Embaixador português para a Ciberdiplomacia e Diplomacia Digital, que acompanha de perto estes assuntos, os Estados democráticos têm feito um esforço significativo para que as convenções internacionais sejam aplicadas no ciberespaço, mas este conceito não tem tido o apoio de alguns países com regimes políticos diferentes, os quais defendem uma convenção própria que garanta a paz no ciberespaço[41].

Existe ainda o *United Nations Internet Governance Forum* (UN IGF) [42] que é uma organização que reúne partes interessadas para discutir políticas públicas digitais. Inclui

38 Reaching Critical Will. https://reachingcriticalwill.org/disarmament-fora/ict/oewg/documents .
39 Global Cyber Security Capacity Centre - University of Oxford. https://gcscc.ox.ac.uk/article/cmm-at-the-un-oewg .
40 Digital Watch - Geneva Internet Platform. https://dig.watch/processes/un-gge .
41 https://expresso.pt/podcasts/o-futuro-do-futuro/2023-08-08-Os-valores-do-mundo-digital-chines-nao-sao-os-mesmos-que-os-nossos.-Sao-ate-rivais-recorda-embaixador-para-a-Diplomacia-Digital-52abf573 .
42 Internet Governance Forum (IGF). https://www.intgovforum.org/en/about .

políticas, divulgação e atividades comunitárias para promover a compreensão das oportunidades e riscos digitais. O trabalho do IGF culmina em reuniões anuais, onde os delegados discutem questões atuais, partilham as melhores práticas e trocam recomendações políticas. Os resultados são depois transmitidos aos órgãos de decisão globais e nacionais, não decorrendo de qualquer negociação. O IGF abrange uma vasta gama de questões de governação digital, desde a cibersegurança e o acesso aberto, sem discriminação, até à privacidade de dados e à IA. As áreas de foco variam a cada ano, de acordo com as submissões recebidas durante o pedido público de contribuições temáticas do IGF, garantindo que a ênfase está alinhada com os temas que as partes interessadas, incluindo os governos e os seus constituintes, procuram abordar. O modelo multissetorial do IGF incentiva a participação ativa dos governos, do setor comercial, da sociedade civil, de especialistas académicos e da comunidade tecnológica.

Em Portugal existe a Iniciativa Portuguesa do Fórum da Governação da Internet (IPFGI)[43], que se constitui como uma plataforma de diálogo a nível nacional, reunindo todas as partes interessadas/*Stakeholders*, públicos e privados, o meio académico, a comunidade técnica da Internet e a sociedade em geral e que acompanha os temas do UNIFG. Face à crescente relevância da internet nos panoramas nacional e internacional, esta plataforma tem em vista informar, refletir e debater de forma aberta e interativa, a governação da Internet.

ii) União Europeia

Em 2020 a Comissão Europeia apresentou o seu "*Shaping Europe's digital future*"[44] que se constitui como uma estratégia para cinco anos (2020-2025), visando a promoção de soluções tecnológicas para ajudar a Europa a seguir o seu próprio caminho para uma transformação digital. Esta estava centrada em três objetivos principais: tecnologia a funcionar para as pessoas; uma economia justa e competitiva; e uma sociedade aberta, democrática e sustentável.

Por sua vez, em 2021, através da Bússola Digital[45] a Comissão Europeia apresentou a sua visão, objetivos e estratégias para alcançar uma transformação digital na Europa até 2030. A intenção era fazer-se uma transição para uma economia neutra em termos de clima,

43 Iniciativa Portuguesa do Fórum da Governação da Internet (IPFGI). https://governacaointernet.pt/ .
44 European Commission. https://commission.europa.eu/document/download/84c05739-547a-4b86-9564-76e834dc7a49_en?filename=communication-shaping-europes-digital-future-feb2020_en.pdf .
45 European Commission - Press release. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_21_983/IP_21_983_EN.pdf .

circular e resiliente, alcançando a soberania digital dentro de uma estrutura global aberta e interligada. Concomitantemente, pretendia implementar políticas digitais que permitissem aos indivíduos e às empresas adotar um futuro digital centrado no ser humano, sustentável e mais próspero. Isto envolve mitigar vulnerabilidades e dependências, enquanto se acelerava o investimento.

Em 2022, com a publicação da Bússola Estratégica[46], é reforçada a necessidade de haver uma UE que esteja mais apta a prevenir, dissuadir e responder a ciberataques, situação que seria atingida com a promulgação da *EU's Cyber Defence Policy* [47]. Esta orientação política, juntamente com a ciberdiplomacia, serão elementos importantes na ação externa da UE[48]. A UE pretende proteger e assegurar um ciberespaço global, aberto, estável e seguro para que todos possam viver uma vida online segura. Para tal, o aumento da cibersegurança é essencial para que a UE se torne uma União resiliente, verde e digital.

No campo digital são vários os assuntos a serem tratados, e para se compreender a cibersegurança (visão holística) na UE, são apresentados pelo menos 25 documentos[49], em áreas tão diversas que vão desde as redes de comunicações, à parte financeira, aos mercados digitais, à IA, à saúde, etc.

No contexto do presente documento e da diplomacia, a análise será mais focada em dois pontos anteriormente referidos, concretamente a diplomacia digital/tecnológica e a ciberdiplomacia. (1) Para a diplomacia digital/tecnológica releva-se o Conselho da União Europeia, de 2022, que nas suas conclusões institui uma estratégia para a diplomacia digital da UE[50], estabelecendo uma base para o envolvimento externo da UE em questões digitais. Esta estratégia enfatiza a necessidade de haver uma abordagem coordenada e coerente para lidar com as oportunidades e riscos das tecnologias digitais na política externa. Apresenta diversos objetivos, indicando-se aqui três grandes linhas: o reforço do papel global da UE nos assuntos digitais, a promoção de uma Internet aberta, livre e segura e a contribuição para os Objetivos de Desenvolvimento Sustentável (ODS) da

46 European Commission. A Strategic Compass for Security and Defence. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf .
47 European Commission. Cyber Defence: EU boosts action against cyber threats. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642 .
48 European External Action Service (EEAS). Cyber Diplomacy and Cyber Defence: EU External Action. https://www.eeas.europa.eu/eeas/cyber-diplomacy-and-cyber-defence-eu-external-action_en .
49 Cyber Diplomacy Toolkit Links. https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy_Links.html .
50 Council Conclusions on EU Digital Diplomacy (2022). https://data.consilium.europa.eu/doc/document/ST-11406-2022-INIT/en/pdf .

ONU. Esta estratégia envolve colaboração com parceiros internacionais, o fortalecimento de redes diplomáticas e o desenvolvimento de capacidades para analisar as tendências digitais. E são reforçados dois pontos para as tecnologias digitais: (1) as novas oportunidades e riscos que trouxeram para a vida dos cidadãos da UE e das pessoas em todo o mundo; (2) a possibilidade de poderem alterar o equilíbrio geopolítico do poder através de parâmetros competitivos específicos. É ainda sublinhado que as políticas externas da UE em matéria de ameaças digitais, ciberameaças e de combate às ameaças híbridas, incluindo a manipulação e interferência estrangeira de informações (FIMI), devem ser totalmente coerentes e reforçar-se mutuamente.

No ano seguinte, em 2023, as conclusões do Conselho sobre a Diplomacia Digital da UE[51], propõem um conjunto de ações prioritárias necessárias para uma política e ação da UE mais fortes, com uma visão estratégica, de forma coerente e eficaz em matéria de assuntos digitais globais. Estas Conclusões recomendam ainda à UE e aos Estados-Membros (E-M) uma abordagem conjunta e comprometida de "Team Europe" para implementação das ações prioritárias: (1) assegurar uma coordenação reforçada e um envolvimento estratégico em relação a fóruns multilaterais e multissectoriais; (2) desenvolver ainda mais parcerias bilaterais e regionais, particularmente no que diz respeito a tecnologias críticas e emergentes; (3) reforçar o envolvimento e a cooperação com os parceiros internacionais na conectividade digital, (4) aumentar a liderança da UE em matéria de regras digitais globais e (5) aumentar a eficiência dos recursos digitais da UE e dos E-M.

Em 2024[52], foi feita uma avaliação aos progressos alcançados com a Diplomacia Digital da UE. Releva-se as áreas de governança digital, das infraestruturas digitais, da estratégia de dados, das competências digitais, da transição verde e digital, e da dimensão internacional da política digital da UE. De notar que as questões digitais passaram de questões puramente técnicas para questões de importância estratégica e política, com implicações imediatas na democracia, economia e sociedade da UE e dos seus E-M. Destaca-se a importância das questões digitais e das tecnologias emergentes para uma política externa integrada da UE, sendo reafirmada a necessidade de se trabalhar em conjunto no conceito "*Team Europe*". Mantém-se ainda o objetivo de criar um mercado

51 Council Conclusions on EU Digital Diplomacy (2023). https://data.consilium.europa.eu/doc/document/ST-11088-2023-INIT/en/pdf .
52 Council Conclusions on EU Digital Diplomacy (2024). https://data.consilium.europa.eu/doc/document/ST-9957-2024-INIT/en/pdf .

digital único europeu seguro, inclusivo e competitivo, alinhado com os valores da UE e os direitos fundamentais, sendo ainda enfatizada a importância da soberania digital europeia num contexto global em rápida mudança. A este respeito pode relembrar o já aqui referido relatório "*The future of european competitiveness*"[53], conhecido como Relatório Draghi, apresentado em setembro de 2024; recomendando que a UE desenvolva ainda mais a sua "diplomacia de recursos" para as matérias-primas críticas.

Uma outra iniciativa da União Europeia no contexto do ciberespaço, mas no que ao combate às ameaças no ciberespaço diz respeito, e tendo em conta a questão da diplomacia, é o Quadro para uma Resposta Diplomática Conjunta da UE a Atividades Maliciosas no ciberespaço (*Cyber Diplomacy Toolbox*)[54], adotado em 2017, tendo em vista aumentar a sua capacidade de prevenir, desencorajar, dissuadir e responder a este tipo de atividades. Estas têm tido um aumento significativo nos últimos tempos, permitindo a aprendizagem e, por conseguinte, o aumento da chamada ciber-resiliência. Aqui está contemplado o aumento das capacidades para o conhecimento situacional, a solidariedade e a assistência mútua, a aplicação do quadro das Nações Unidas para um Estado responsável e medidas diplomáticas. A *Cyber Diplomacy Toolbox* integra a visão holística da UE para o ciberespaço tendo em vista a promoção e prevenção de conflitos, a cooperação e a estabilidade no ciberespaço, numa visão europeia de ciberespaço global, aberto, livre, estável e seguro, baseado no Estado de direito.

Ao mesmo tempo, a ciberdiplomacia e as questões ligadas ao ciberespaço têm ganho relevância como componente da Política Externa e de Segurança Comum (PESC) da UE, face ao ritmo da digitalização e da magnitude dos desafios no ciberespaço e respetivos cenários de ameaças.

A ciberdiplomacia facilita que as nações, dentro do seu quadro de alianças e coligações, enfrentem de forma colaborativa preocupações comuns ligadas à segurança do ciberespaço. Os Estados podem utilizar os canais diplomáticos para coordenar as respostas às ciberameaças, trocar as melhores práticas e aproveitar as capacidades coletivas para reforçar a dissuasão no ciberespaço. Um exemplo ilustrativo é a decisão do

53 European Commission (2024). The future of European competitiveness, a competitiveness strategy for Europe.

54 Council of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32019D0797 .

Conselho da União Europeia[55] contra dois indivíduos e uma organização implicados ou responsáveis pelo ciberataque ao Parlamento Federal Alemão (Bundestag) entre abril e maio de 2015, ligados à Rússia. O sistema de informação do parlamento foi alvo de um ciberataque, resultando no roubo de uma quantidade significativa de dados e no comprometimento de inúmeras contas de correio eletrónico, incluindo a da ex-chanceler alemã Angela Merkel, deixando o sistema inutilizável durante vários dias[56]. Outro exemplo, mais recente, de junho de 2024, são as medidas aprovadas pelo Conselho[57] contra seis pessoas envolvidas em ciberataques que afetaram sistemas de informação relacionados com infraestruturas críticas, funções críticas do Estado, o armazenamento ou tratamento de informações classificadas e equipas da administração pública de resposta a emergências nos E-M da UE. De relevar que pela primeira vez foram aplicadas medidas restritivas contra membros dos grupos Callisto, Armageddon e Wizard Spider, que utilizaram campanhas de *ransomware*[58] para atacar serviços críticos, como a saúde e a banca. Desta forma, verifica-se que a ciberdiplomacia pode exercer pressão normativa sobre os atores estatais e não estatais para aderirem a regras e normas de comportamento estabelecidas no ciberespaço. Ao reforçar o consenso internacional sobre o comportamento responsável do Estado e ao condenar as violações, as iniciativas diplomáticas podem moldar as perceções de conduta aceitável e as estratégias de dissuasão no ciberespaço. Um outro exemplo pode ser o esforço dos países ocidentais para acabar com a indústria tecnológica russa devido à invasão da Ucrânia em fevereiro de 2022 como uma ação de retaliação de punição[59]. Igualmente, a partir de 2022, devido a esta guerra, foi sentida uma deterioração da segurança no ciberespaço, tendo a UE e muitos dos seus E-M sido vítimas de atividades maliciosas no ciberespaço, conforme apresentado em vários relatórios da Agência da UE para a Cibersegurança (ENISA)[60].

---

55 Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L:2020:351I:FULL .

56 Council of the European Union. https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/ .

57 Council of the European Union. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401779 .

58 *Ransomware* - tipo de software malicioso, ou malware, que ameaça uma vítima ao destruir ou bloquear o acesso a dados ou sistemas críticos até que um resgate seja pago. https://www.microsoft.com/pt-pt/security/business/security-101/what-is-ransomware .

59 Jesus, Helder (2024). How important is the cyberdiplomacy to the deterrence in cyberspace? *IDN Brief*. https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2024/IDN%20brief%20junho%202024%20Cyberdiplomacy.pdf .

60 ENISA (2024). ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Importa ressalvar que a resposta diplomática da UE se baseia no quadro das Nações Unidas para a conduta responsável dos Estados no ciberespaço, decorrente dos relatórios dos UNGGE e OEWG.

Através do *Revised Implementing Guidelines of the Cyber Diplomacy* Toolbox[61] (Jun 2023) são apresentadas orientações que visam a melhoria das medidas desta CDT face às aprendizagens entretanto obtidas tanto de respostas diplomáticas como em exercícios, para garantir uma abordagem estratégica face aos agentes de ciberameaças (*advanced persistent threat* – APT), e fornecer medidas de resposta adicionais para melhorar a tomada de decisões atempadas.

iii) Estados Unidos da América

Face à atual competição estratégica, apresenta-se de seguida a situação de um dos competidores, no caso concreto dos EUA, no que ao ciberespaço e diplomacia diz respeito, num horizonte de há cinco anos a esta parte.

Tal como acontece com as outras vertentes diplomáticas, a ciberdiplomacia visa a construção de parcerias estratégicas com outros países do mundo para melhorar a ação conjunta e a cooperação contra ameaças partilhadas, reunindo coligações com ideias e valores semelhantes em questões políticas vitais, partilhando informação tendo em vista a proteção face a atores com visões diferentes do mundo[62]. E a ciberdiplomacia deverá ser um elemento transversal aos outros instrumentos do poder nacional, pela particularidade de o ciberespaço ser igualmente transversal e a toda a sociedade.

Em 2020, Christopher Ashley Ford, que foi o *Assistant Secretary* for International Security and Nonproliferation entre 2018 e 2021, numa intervenção no *Center for Strategic and International Studies* (CSIS), abordou a crescente ameaça de atividades maliciosas no ciberespaço e a resposta estratégica dos EUA, focando na diplomacia e na dissuasão, tendo por base a 2018 *National Cyber Strategy*[63], onde uma das ações prioritárias era a criação de uma *Cyber Deterrence Initiative* (CDI). Esta visava a criação de uma coligação de Estados e o desenvolvimento de estratégias para impor consequências para comportamentos maliciosos no ciberespaço, onde o envolvimento da

61 Council of the European Union. https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf .
62 Painter, Chris (2018). The rise of the internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century. https://afsa.org/diplomacy-cyberspace .
63 White House - National Cyber Strategy. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf .

diplomacia se constitui como um elemento relevante. Ao abordar a parte da diplomacia mencionou as normas voluntárias, destacando aplicabilidade do Direito Internacional, dando como exemplo o reconhecimento, em relatórios da ONU, de que o direito internacional, incluindo a Carta das Nações Unidas, tem aplicabilidade no ciberespaço. Referiu ainda as Normas de Comportamento Responsável, através da articulação de princípios para comportamentos em situações que não chegam a ser conflito armado, onde se inclui a proibição de ataques a infraestruturas críticas. Na parte da dissuasão, ele releva a CDI, como uma iniciativa que ele apelidou de "Diplomacia de Imputação", através do aumento da capacidade de imputar ciberataques e mobilizar parceiros para condenar as atividades maliciosas, aumentando os custos e os riscos para os perpetradores. Nesta iniciativa podem inserir-se a imposição de sanções pelos EUA e pela União Europeia em casos de cibercrime graves. De notar que na estratégia acima referida está contemplada a utilização de uma série diversificada de ferramentas, onde se incluem sanções económicas, como parte de uma estratégia de dissuasão mais ampla para os executores de atividades maliciosas no ciberespaço, assim como para aqueles que as patrocinam/suportam, numa atividade designada de *Proxy*.

Numa vertente menos institucional, Emily O. Goldman[64], conhecida consultora do Departamento de Estado e do Departamento de Defesa, defende que os EUA precisariam de adotar uma postura mais proativa e competitiva na ciberdiplomacia para combater as campanhas persistentes e coordenadas de adversários como a China e a Rússia. Isto porque os adversários atuam deliberadamente abaixo do limiar do conflito armado internacionalmente aceite e nunca cruzam fisicamente as fronteiras dos EUA, minimizando assim os riscos para si próprios enquanto colhem os benefícios cumulativos do seu comportamento no ciberespaço. Ela considera que as normas são construídas através da prática "normal" estabelecida em acordos internacionais. Mas, os EUA, ao se envolverem persistentemente e contestando a agressão no ciberespaço, podem traçar parâmetros em torno do que é aceitável, incómodo, inaceitável e intolerável. Por outro lado, Goldman critica a ênfase na dissuasão como estratégia central na ciberdiplomacia dos EUA, argumentando que a dissuasão falhou em prevenir as agressões no ciberespaço fora do conflito armado e que uma estratégia baseada na resposta após um incidente significativo não é suficientemente flexível para lidar com a maioria das atividades

64 Goldman, Emily (2020). From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy. *The Strategist 84, Texas National Security Review: Volume 3, Issue 4 (Fall 2020)*. https://tnsr.org/wp-content/uploads/2020/09/TNSR-Vol3-Iss4-Goldman.pdf .

maliciosas. Assim, ela apresenta sete recomendações para melhorar a ciberdiplomacia dos EUA e garantir que o país possa competir eficazmente no ciberespaço, podendo referir-se, dessas, (1) a Integração da Diplomacia na Estratégia de Segurança do Ciberespaço, de modo a que os diplomatas sejam conhecedores das atividades dos EUA e possam explicar essas atividades aos parceiros estrangeiros e (2) o Reforço do Corpo Diplomático para os assuntos do ciberespaço, criando um quadro de diplomatas especializados em cibersegurança para o acompanhamento das tendências globais e identificar oportunidades de colaboração e competição.

Num esforço que já vem desde 2019, na intenção de se criar um *Bureau of Cyberspace Security and Emerging Technologies* (CSET), este passou a Bureau of Cyberspace and Digital Policy (CDP)[65], tendo sido estabelecido no âmbito do Departamento de Estado, em abril de 2022. Tem uma ênfase maior para a dimensão internacional e destina-se a acompanhar os desafios de segurança nacional, as oportunidades económicas e as implicações para os valores dos EUA associados ao ciberespaço, às tecnologias digitais e à política, sendo este organismo chefiado pelo Embaixador Nathaniel C. Fick.

Já a 2023 *National Cybersecurity Strategy*[66], apresenta cinco pilares para construir e melhorar a colaboração entre entidades responsáveis para a Cibersegurança. Mas, estranhamente, e ao contrário da estratégia anterior, de 2018, não aborda tanto a questão da dissuasão, apesar de referir que para restringir eficazmente os seus adversários e combater atividades maliciosas abaixo do limiar do conflito armado serão utilizadas todas as ferramentas do governo, onde se incluem, entre outras, o isolamento diplomático e os custos económicos. No fundo falamos do emprego dos elementos do poder nacional (DIME)[67].

Atualmente, os EUA reconhecem que se está num ponto de viragem nas relações internacionais[68], tendo o Departamento de Estado publicado uma estratégia para o ciberespaço e política digital, em maio de 2024. Tal decorre da assunção que existe uma competição feroz entre países, num contexto de desafios globais, e para os quais a

65 US Department of State. https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/ .
66 White House - National Cybersecurity Strategy. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf .
67 DIME - *diplomacy, information, military, and economic*. https://www.networkdiplomacy.org/principles-of-pd/principles-ch-1/
68 US Department of State. https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf .

tecnologia vai tendo um papel cada vez mais importante. Com este documento, os EUA pretendem modernizar a diplomacia, com a prioridade ao desenvolvimento dos conhecimentos e competências em tecnologias digitais e no ciberespaço. Dando continuidade e alinhando com as 2022 *National Security Strategy* e 2023 *National Cybersecurity Strategy*, o Departamento de Estado, em colaboração com outras agências federais, desenvolveu esta nova estratégia, a 2024 *United States International Cyberspace & Digital Policy Strategy*, focada na construção de uma ampla solidariedade digital através de três princípios orientadores. Destes, no âmbito da presente análise, destaca-se o terceiro, que visa a implementação de uma abordagem política abrangente que utilize as ferramentas adequadas de diplomacia e diplomacia internacional em todo o ecossistema digital. Este ecossistema inclui, entre outros, hardware, software, protocolos, normas técnicas, fornecedores, operadores, utilizadores e cadeias de abastecimento que abrangem redes de telecomunicações, cabos submarinos, computação em nuvem, centros de dados e infraestruturas de redes de satélites, tecnologias operacionais, aplicações, plataformas web e tecnologias de consumo, bem como a Internet das Coisas (IoT), a IA e outras tecnologias críticas e emergentes. Nesta estratégia é estabelecido que a grande maioria das questões de política externa serão moldadas pelos atuais investimentos no ciberespaço e na diplomacia para a tecnologia digital. Por sua vez, o Departamento de Estado irá ainda liderar o processo interinstitucional para definir, coordenar e integrar esforços da ciberdiplomacia e da diplomacia tecnológica digital para promover os interesses e valores nacionais dos EUA na próxima década.

Assim, pode ver-se que existem duas tendências de terminologia, que têm a ver com os contextos, e já anteriormente referido: "ciberdiplomacia" num contexto de negociações viradas para as questões de cibersegurança, onde a vertente legal tem uma grande primazia e "diplomacia tecnológica digital", numa vertente mais técnica e económica, de relacionamento empresarial, visando ambas a defesa dos interesses dos EUA no cenário internacional. Mas tudo integrado numa mesma entidade, o ”*Bureau of Cyberspace and Digital Policy*”, de modo a garantir ao alinhamento da ação externa, no que ao ciberespaço diz respeito. Relativamente à dissuasão, a única alusão é referindo que o Departamento de Estado fornece orientação em política externa e utiliza compromissos diplomáticos para apoiar os esforços do Departamento de Defesa (DoD) para fazer campanha no e através do ciberespaço abaixo do nível do conflito armado para reforçar a dissuasão e frustrar os seus adversários.

III. ELEMENTOS DE ECONOMIA PARA A GEOPOLÍTICA DO CIBERESPAÇO

A crise financeira de 2008, a guerra comercial entre os EUA e a China, a pandemia de COVID-19 e a guerra às portas da Europa, entre a Federação Russa e a Ucrânia, carimbam a desaceleração de uma época de globalização[69]. Mas em vez de uma completa desglobalização, Ralf Roloff considera que estamos a assistir a uma *fragmentegration*[70] da economia global, processo que se carateriza por uma fragmentação e integração simultâneas da economia global. A fragmentação através da reorganização das cadeias de valor globais, com empresas a adotarem práticas para reduzir vulnerabilidades e aumentar a resiliência e a integração continua a estar presente, evidenciando-se pelo aumento do comércio global e pela interconexão dos principais blocos comerciais regionais: América do Norte, União Europeia e Ásia-Pacífico. Por outro lado, verifica-se que vivemos um contexto de crescente competição estratégica entre grandes potências. Esta competição leva à instrumentalização das interdependências económicas, transformando a economia global num campo de batalha geopolítica, colocando desafios significativos ao sistema multilateral[71]. Tal é visível na crescente militarização do ciberespaço, com a criação de comandos para a condução de operações militares[72], mas igualmente pelo controlo da produção e cadeia de abastecimento de produtos tecnológicos. E neste caso podemos falar de três grandes áreas: a 5ª geração de telecomunicações (5G), os semicondutores (chips) e a IA, que são cruciais para a economia global e para a competitividade. A liderança em chips e IA trará enormes ganhos económicos e militares[73], definindo normas e tendências tecnológicas globais. Complementarmente a esta situação tem-se com a conectividade internacional no mundo, a qual é sustentada pelos cabos submarinos e onde passam cerca de 99% do tráfego Intercontinental[74].

---

69 Goldberg, Pinelopi (2024). Globalization in crisis- Confronting a new economic reality. *United Nations University World Institute for Development Economics Research*. https://bpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/6/3741/files/2024/06/UNU-WIDER_Goldberg.pdf .

70 Roloff, Ralf (2024). Goodbye Globalization? Hello "Fragmentegration".

71 Wyne, Ali (2022). The Evolving Geopolitics of Economic Interdependence between the United States and China. *Asia Policy Vol. 17, No. 3 (July 2022)*, pp. 81-105. https://www.jstor.org/stable/27227221 .

72 https://hungarian-presidency.consilium.europa.eu/en/events/eu-cyber-commanders-conference/ .

73 Winter-Levy, S. (2025). With Its Latest Rule, the U.S. Tries to Govern AI's Global Spread. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/emissary/2025/01/ai-new-rule-chips-exports-diffusion-framework?lang=en .

74 Mauldin, Alan (2023). Do Submarine Cables Account For Over 99% of Intercontinental Data Traffic? https://blog.telegeography.com/2023-mythbusting-part-3 .

Um outro elemento nesta competição estratégica é o surgimento de novos atores, naquilo que Joseph Nye referiu como a "difusão de poder"[75]. Esta carateriza-se pelos Estados continuarem a ser o ator dominante na cena internacional, mas onde o seu palco que tinha o foco apontado para os líderes políticos passará a ser partilhado com novos atores, cada vez mais poderosos, e que poderão ser concorrentes e difíceis de controlar. Como exemplo tem-se o caso das grandes empresas tecnológicas, como as *Big Tech* (GAMAM[76]) ou Elon Musk, com as suas empresas Starlink ou a SpaceX, entre outros.

A preocupação com esta realidade está patente no Parlamento Europeu, que no "*The geopolitics of technology: Charting the EU's path in a competitive world*"[77], apresenta uma análise à geopolítica da tecnologia, tendo como foco a crescente rivalidade tecnológica sino-americana e nas suas implicações para a União Europeia. Refere que o mundo está a atravessar uma fase de desglobalização, marcada pelo protecionismo, pela fragmentação e pelo aumento das tensões geopolíticas. Esta mudança coincide com a digitalização acelerada das economias e sociedades, colocando a tecnologia no centro da luta pelo poder global. Neste ponto, elenca a competição por duas tecnologias cruciais para a sociedade em geral, como a IA e os semicondutores, mas também na sua utilização para efeitos de operações militares no ciberespaço (*cyberwarfare*), interferência em processos eleitorais e campanhas de desinformação. No que aos chips e à IA diz respeito, é afirmado que a UE se encontra numa posição vulnerável, dependente de outros atores globais para a produção de semicondutores e com défice de investimento em IA. A UE é ainda apresentada como tentando encontrar um equilíbrio entre autonomia e abertura, promovendo padrões tecnológicos democráticos e construindo parcerias com países afins, enquanto enfrenta desafios como dependências estratégicas e medidas extraterritoriais dos EUA. Esta situação é reforçada no Instituto Montaigne, no seu "*Extraterritoriality - a Blind Spot in the EU's Economic Security Strategy*"[78], onde é afirmado que a capacidade da UE para recuperar e manter-se competitiva a longo prazo está em risco. Neste estudo é referido que nas últimas décadas, a UE enfrentou desafios sem precedentes,

---

75 Nye, Joseph (2011). *The Future of Power*. New York: Public Affairs.

76 GAMAM- *Google*, Apple, Meta, Amazon, Microsoft. As cinco companhias big tech e antes conhecidas pelo acrónimo GAFAM *Google*, Apple, Facebook, Amazon, Microsoft .

77 European Parliament (2023). The geopolitics of technology: Charting the EU's path in a competitive world. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762384/EPRS_BRI(2024)762384_EN.pdf .

78 Institut Montaigne (2024). Extraterritoriality: a Blind Spot in the EU's Economic Security Strategy. *Institut Montaigne Issue Paper - January 2024.* https://www.institutmontaigne.org/ressources/pdfs/publications/extraterritoriality-blind-spot-eus-economic-security-strategy.pdf .

nomeadamente as alterações demográficas, uma revolução digital com impacto na economia e na sociedade europeia, num ambiente imprevisível. E carateriza a atual realidade da UE, cujo continente está novamente em guerra, enfrentando simultaneamente uma série de problemas como fluxos de imigração, crescimento económico lento, inflação crescente e uma rivalidade intensificada entre os EUA e a China. Refere ainda que o crescente envolvimento dos governos na economia de mercado está a representar uma ameaça à ordem pós-Segunda Guerra Mundial criada pelo ocidente, a qual estimulou a competitividade global. Verifica-se uma substituição das estratégias comerciais convencionais por disputas tarifárias e a promulgação de políticas industriais tendo em vista a redução dos riscos tecnológicos. E releva que os governos estão a utilizar cada vez mais a pressão económica ao aplicarem as suas leis a nível internacional para proteger os seus próprios interesses, naquilo que é referido como a "extraterritorialidade."

i) Breve contextualização aos semicondutores/chips

Os semicondutores, ou chips, são pequenos dispositivos eletrónicos que são essenciais no nosso dia a dia. Desde os interruptores de luz, a smartphones ou a aviões de combate, estas tecnologias impulsionam tudo. Os centros de dados, os dispositivos de consumo, os automóveis, as infraestruturas críticas e quase todos os sistemas militares dependem de semicondutores. Para além de serem componentes fundamentais da IA, da biotecnologia e das energias renováveis, estas tecnologias terão um papel fundamental na formação do futuro das sociedades. Como refere Sameh El Namaki, consultor do Banco Mundial, da Comissão Europeia e de outras organizações internacionais, a tecnologia levou a indústria do simples estado de “poucos transístores numa pastilha de silício” para o estado de vários milhões de transístores no mesmo perfil de pastilha de silício[79].

Desta forma, os semicondutores são a base fundamental da economia moderna, assente na tecnologia, nos dados e na informação. São igualmente o "novo motor do equilíbrio geopolítico"[80], na medida em que são a base das outras tecnologias emergentes críticas,

79 Namaki, MSS (2023). Tomorrow’s Chip Industry: Threats, Opportunities and Strategy Framework. Scholedge International Journal of Business Policy & Governance, 10(4), 30-37. https://dx.doi.org/10.19085/sijbpg100401.
https://www.researchgate.net/publication/382422888_Tomorrow%27s_Chip_Industry_Threats_Opportunities_and_Strategy_Framework .

80 Tuteja, Akhilesh (2024). Semiconductor: The new driver of geopolitical balance, economic growth. *Business Standard*. https://www.business-standard.com/economy/news/semiconductor-the-new-driver-of-geopolitical-balance-economic-growth-124010401187_1.html .

como a IA e o 5G, bem como da computação quântica, entre outras. Os EUA e a UE não têm capacidade para produzir semicondutores avançados à escala, especificamente os dos chips de 2 e 3 nanómetros (nm)[81]. A capacidade está localizada principalmente em Taiwan e com alguma presença na Coreia do Sul. Esta zona do globo está a tornar-se cada vez mais importantes para a transformação digital das economias europeias e mundiais, assim como do ponto de vista da soberania geopolítica e tecnológica.

"*Ao contrário do petróleo que pode ser comprado a muitos países, a nossa produção da capacidade computacional está totalmente dependente de uma séria de pontos de estrangulamento: ferramentas, químicos e software, que são habitualmente produzidos por um punhado de companhias - e às vezes apenas por uma. Não existe nenhuma outra área da economia que seja tão dependente de um número tão reduzido de firmas. Os chips de Taiwan são responsáveis por 37% de toda a capacidade computacional em cada ano. Duas companhias coreanas produzem 44% dos Chips de memória no mundo. A companhia holandesa AMSL constrói 100% de todas as máquinas de litografia ultravioleta extrema, sem as quais os chips de ponta seriam simplesmente impossíveis de fazer. Os 40% do petróleo mundial detidos pela OPEP, em comparação, não parecem muito."* [82] (Chris Miller, 2023, p36).

Nenhum país pode alcançar a autossuficiência ou a supremacia em todos os aspetos da produção de semicondutores. As cadeias de valor são globais e complexas, e apenas alguns países detêm o domínio nos seus segmentos: os EUA no design de chips, o Japão nos materiais e Taiwan na manufatura[83]. A *Taiwan Semiconductor Manufacturing Company* (TSMC) produz pelo menos 90% dos chips de computador mais avançados do mundo, naquilo que o *think thank* SNV considera como "o ponto único de falha mais crítico" na cadeia de abastecimento de semicondutores[84]. Atualmente, as empresas de Taiwan já detêm uma quota no mercado dos chips de 68%[85], o que é muito significativo.

---

81 Shivakumar, Sujai; Wessner, Charles & Howell, Thomas (2024). A World of Chips Acts: The Future of U.S.-EU Semiconductor Collaboration. *Center for Strategic & International Studies*.https://www.csis.org/analysis/world-chips-acts-future-us-eu-semiconductor-collaboration .

82 Miller, Chris. (2023). *A Guerra dos Chips: O Combate pela Tecnologia mais Crucial do Mundo*. Portugal: Dom Quixote.

83 European Parliament (2023) .

84 Kleinhans, Jan-Peter & Baisakova, Nurzat (2020). The global semiconductor value chain: A technology primer for policy makers. Stiftung Neue Verantwortung. https://www.interface-eu.org/storage/archive/files/the_global_semiconductor_value_chain.pdf .

85 Hilton, Isabel (2024). Taiwan Makes the Majority of the World's Computer Chips. Now It's Running Out of Electricity. *WIRED*. https://www.wired.com/story/taiwan-makes-the-majority-of-the-worlds-computer-chips-now-its-running-out-of-electricity/ .

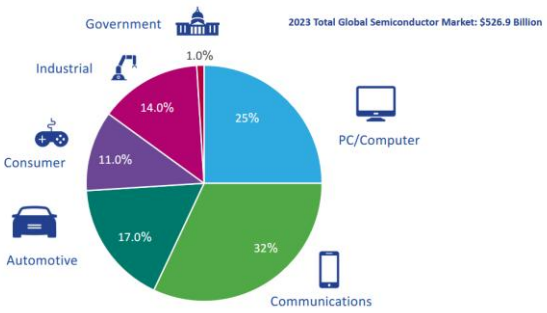

Figura 1 – Mercado Global dos Semicondutores em 2023 ($526.9 Mil Milhões de dólares)[86]

A construção de um ecossistema forte de fabrico de semicondutores requer infraestruturas significativas, a formação de trabalhadores e investimentos em I&D. A construção de uma fábrica de produção de semicondutores pode custar entre 15 a 20 mil milhões de dólares, sendo que a escassez de talento é outro problema. O KPMG *Global Semiconductor Industry Outlook 2023* refere que 67% dos profissionais do setor priorizam o desenvolvimento e a retenção de pessoal. A indústria necessita de cerca de 1 milhão de trabalhadores qualificados até 2025[87]. Esta preocupação volta a estar patente no KPMG *Global Semiconductor Industry Outlook 2024* [88], ao referir-se que esta indústria de alta tecnologia sofre de escassez de trabalhadores qualificados, cujo risco de talento é visto como o principal problema enfrentado pelo setor. A situação é ainda agravada pelo facto de empresas adjacentes aos semicondutores (como as *Big Tech*, as empresas automóveis, etc.) terem vindo a desenvolver as suas próprias capacidades de design de chips nos últimos anos.

Esta questão da escassez de talento e profissionais qualificados também é realçada no relatório "*Global Cybersecurity Outlook 2025*"[89] do Fórum Económico Mundial, neste caso mais ligado às questões da Cibersegurança, constituindo-se como um desafio crítico que aumenta a vulnerabilidade das organizações. Neste relatório é enfatizada a necessidade de uma mentalidade de segurança, da colaboração entre o público e o

86 SIA Factbook (2024). https://www.semiconductors.org/wp-content/uploads/2024/05/SIA-2024-Factbook.pdf .
87 Tuteja, Akhilesh (2024). Semiconductor: The new driver of geopolitical balance, economic growth. *Business Standard*. https://www.business-standard.com/economy/news/semiconductor-the-new-driver-of-geopolitical-balance-economic-growth-124010401187_1.html .
88 KPMG (2024). Semiconductor outlook buoyed by AI and automotive. https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2024/global-semiconductor-industry-outlook.pdf .
89 WEF (2025). Global Cybersecurity Outlook 2025. Insight Report https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf .

privado, bem como de investimentos estratégicos para construir ecossistemas resilientes, podendo incluir-se nestes os chips.

Os valores associados à indústria dos semicondutores começaram, entretanto, a levantar dúvidas, pela sua exorbitância. Kumar Priyadarshi, questiona o aumento exponencial dos custos de design dos chips, com o custo de um chip de 2nm estimado em 725 milhões de dólares, comparativamente com os 249 milhões de dólares para um chip de 7nm. Ele argumenta que este aumento se deve principalmente aos custos de desenvolvimento de software e verificação, agravados pela necessidade de talento especializado e tecnologias avançadas de fotolitografia. Indica ainda que as estratégias de gestão de custos variam na indústria de semicondutores. Assim, podemos dizer que importa seguir um possível caminho ajustado a cada realidade industrial, decorrente das necessidades de uma nação, organização ou empresa, e que não seja enviesado apenas por um *State of the art* específico, muitas vezes impostos por outros, os quais irão requerer custos incomportáveis.

De notar ainda que a *World Semiconductor Trade Statistics* (WSTS), uma organização independente fundada em 1986, sem fins lucrativos que representa a grande maioria da indústria mundial de semicondutores, apresenta dois relatórios por ano, com previsões, em maio e em novembro. No último de 2024[90], e perspetivando 2025, está previsto um crescimento de 11,2%, elevando a avaliação do mercado global para uma estimativa de 697 mil milhões de dólares. Este crescimento será impulsionado essencialmente pelos setores da Lógica e da Memória, num total de 400 mil milhões de dólares em valor.

O ano de 2025 perspetiva-se ser um ano de confronto conceptual para a área dos semicondutores. Isto porque a abordagem entre os dois grandes rivais, EUA e China, é diferente[91]. Assim, à medida que os EUA apostavam na limitação de exportações de semicondutores, a China investia extensivamente no seu sector nacional. A China irá concentrar-se no desenvolvimento de semicondutores essenciais e menos avançados, designados de "nós maduros", fundamentalmente para utilização económica. De referir que até ao momento, a IA tem sido executada em *data centers* robustos, mas em 2025, será expectável o surgimento de "fábricas de IA", as quais serão concebidas

90 WSTS (2024). https://www.wsts.org/esraCMS/extension/media/f/WST/6765/WSTS_FC-Release-2024_11.pdf .
91 Kurbalija, Jovan (2025). The year of AI clarity: 10 AI Forecasts for 2025. *Diplo*. https://www.diplomacy.edu/blog/10-forecasts-for-ai-and-digitalisation-in-2025/#technology .

especificamente para treinar modelos de IA. E neste sentido, a Nvidia está a desenvolver uma nova GPU *Blackwell* destinada à computação de IA.

ii) o US CHIPS Act e implicações associadas

Os EUA continuam a destacar-se no design, investigação e desenvolvimento de semicondutores[92], mas ficou para trás no fabrico, representando apenas 10% da produção comercial global. Atualmente, nenhum chip lógico e de tecnologia avançada, que operam em computadores, telemóveis e supercomputadores, é produzido à escala comercial nos EUA. Além disso, vários componentes da cadeia de abastecimento de semicondutores estão geograficamente concentrados, o que os torna suscetíveis a perturbações e colocam em risco a economia global e a segurança nacional dos EUA. As interrupções na cadeia de abastecimento causadas pela pandemia de COVID-19, levando a uma escassez significativa destes materiais, relevaram a produção limitada de semicondutores nos EUA[93].

Assim, em agosto de 2022 os EUA adotaram a lei *Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act*[94]*,* conhecida por *CHIPS Act*, que visa impulsionar a indústria de semicondutores norte-americana. Esta lei prevê investimentos significativos em investigação e desenvolvimento (I&D) e fabrico de semicondutores, criando empregos e fortalecendo as cadeias de abastecimento. O objetivo é aumentar a produção nacional de chips, reduzir a dependência da Ásia Oriental e assegurar a liderança tecnológica dos EUA, onde se incluem iniciativas para promover a inovação e o desenvolvimento de tecnologias futuras. Esta lei contempla um investimento de 280 mil milhões de dólares[95] para reforçar a capacidade de semicondutores dos EUA, catalisar a I&D e criar centros regionais de alta tecnologia e desenvolvimento de uma força de trabalho maior e mais inclusiva.

---

92 NIST (@2025). CHIPS for America. *National Institute of Standards and Technology (NIST)*. https://www.nist.gov/chips .

93 Patel, Prachi (2023). U.S. Universities are building a new Semiconductor Workforce. *IEEE Spectrum*.https://spectrum.ieee.org/chips-act-workforce-development .

94 A informação aqui apresentada encontrava-se disponível no sitio da Casa Branca em https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/, local este que deixou de estar acessível em 23Jan2025, após a presidência de Donald Trump. No entanto, esta informação ainda está presente em https://kr.usembassy.gov/081022-fact-sheet-chips/ .

95 Mckinsey (2024). The CHIPS and Science Act: Here's what's in it. https://www.mckinsey.com/industries/public-sector/our-insights/the-chips-and-science-act-heres-whats-in-it .

Empresas como a Intel *Corporation*, a TSMC e a Micron estão a aproveitar o dinheiro do CHIPS Act para construir novas ou expandir instalações de fabrico de semicondutores nos EUA[96]. Complementarmente estão a colaborar com universidades e consórcios para desenvolver currículos revistos nas atuais escolas de engenharia e para estabelecer novos programas de graduação ou certificação com instituições interessadas. Por exemplo, a Intel está a construir duas instalações avançadas de fabrico de chips em Ohio e a colaborar com a Universidade Estadual de Ohio para estabelecer um consórcio neste estado. O estabelecimento deste ecossistema educativo leva o seu tempo, e gerar um número suficiente de graduados para satisfazer a procura continuará a ser um esforço contínuo durante os próximos anos.

Em outubro de 2022 os EUA emitiram regras[97] tendo em vista restringir a capacidade da República Popular da China (RPC) em comprar chips de computação avançados e fabricar chips avançados, que são essenciais para a vantagem militar. Estas regras sublinham o claro foco em abordar estrategicamente as ameaças à segurança nacional colocadas pela China, controlando os itens necessários para permitir o desenvolvimento e a produção de tecnologias, como a IA, utilizadas em aplicações militares.

Por seu lado, a China preparou um pacote de 143 mil milhões de dólares para as suas empresas de semicondutores em resposta às restrições impostas pelos EUA[98]. Isto indica uma estratégia mais assertiva da China para influenciar o futuro de uma indústria que se tornou um ponto focal geopolítico devido à crescente procura de chips, a qual Pequim considera fundamental para a sua supremacia tecnológica. Naturalmente que esta situação aumentou as preocupações nos EUA e nos seus aliados relativamente à rivalidade da China no sector dos semicondutores.

Os Países Baixos e o Japão são países importantes no processo dos chips, tendo a China como um dos países de exportação dos seus produtos[99]. Para que a estratégia dos EUA

---

96 Sloun, Sherry (2023). U.S. Investment in Semiconductor Manufacturing: Building the Talent Pipeline. *Council on Foreign Relations*.https://www.cfr.org/blog/us-investment-semiconductor-manufacturing-building-talent-pipeline .

97 BISC (2023). Export Controls on Semiconductor Manufacturing Items. *Bureau of Industry and Security, Commerce*. https://www.federalregister.gov/documents/2023/10/25/2023-23049/export-controls-on-semiconductor-manufacturing-items .

98 CNBC (2022). China readying $143 billion package for its chip firms in face of U.S. curbs, sources say. https://www.cnbc.com/2022/12/14/china-readying-143-billion-package-for-its-chip-firms-reuters.html .

99 Allen, Gregory; Benson, Emily & Putnam, Margot (2023). Japan and the Netherlands Announce Plans for New Export Controls on Semiconductor Equipment. *Center for Strategic & International Studies* (CSIS). https://www.csis.org/analysis/japan-and-netherlands-announce-plans-new-export-controls-semiconductor-equipment .

relativamente à restrição de chips para a China tivesse sucesso, os meios diplomáticos americanos constituem-se como um elemento preponderante. Assim, surgiram novos controlos de exportação de um conjunto diversificado de tecnologia de semicondutores destes dois países, e que coincidentemente cobrem as exportações para a China. Como tal, os Países Baixos e o Japão juntaram-se aos EUA na restrição de exportação de equipamentos[100], apesar de nenhum destes países ter nomeado explicitamente a China como alvo dos controlos de exportação, nem indicado que as suas ações estivessem relacionadas com um qualquer acordo com os EUA.

Em 2023 foi publicada nos EUA a *The Vision for the National Advanced Packaging Manufacturing Program* (NAPMP)[101], que detalha a visão, a missão e os objetivos do programa de embalagens avançadas criado pelo CHIPS Act. O NAPMP é um dos quatro programas de I&D do CHIPS *for America* que, em conjunto, estabelecem o ecossistema de inovação necessário para garantir que as instalações americanas de fabrico de semicondutores, incluindo as financiadas pelo *CHIPS Act*, produzem as tecnologias mais sofisticadas e avançadas do mundo.

Como parte do programa do *CHIPS Act*, o *CHIPS for America*[102] atribui ao Departamento do Comércio o valor de 50 mil milhões de dólares para financiar uma variedade de iniciativas destinadas a revitalizar a I&D e as capacidades de fabrico de semicondutores dos EUA, bem como o reforço da criação de emprego para cidadãos norte-americanos. Neste valor estão contempladas duas áreas: o *CHIPS Program Office* com 39 mil milhões de dólares para incentivos de investimento em instalações e equipamentos nos EUA, e o *CHIPS Research and Development Office* com 11 mil milhões de dólares, que se destinam à construção de um forte ecossistema nacional de I&D.

Já em janeiro de 2025, e a uma semana antes de deixar o cargo, a administração Biden emitiu novas restrições à exportação de chips desenvolvidos nos EUA[103] que alimentam

---

100 Reuters (2023). Japan, Netherlands to join U.S. in restricting chip equipment exports to China https://www.reuters.com/technology/japan-netherlands-join-us-china-chip-controls-bloomberg-2023-01-27/ .

101 NIST (2023). CHIPS for America Releases Vision for Approximately $3 Billion National Advanced Packaging Manufacturing Program. https://www.nist.gov/news-events/news/2023/11/chips-america-releases-vision-approximately-3-billion-national-advanced .

102 NIST (n.d.). CHIPS FOR AMERICA. https://www.nist.gov/chips .

103 BIBS (2025). Ensuring U.S. Security and Economic Strength in the Age of Artificial Intelligence. *Benton Institute for Broadband & Society*. https://www.benton.org/headlines/ensuring-us-security-and-economic-strength-age-artificial-intelligence .

Informação da Casa Branca anteriormente disponível em https://www.whitehouse.gov/briefing-room/statements-releases/2025/01/13/fact-sheet-ensuring-u-s-security-and-economic-strength-in-the-age-of-artificial-intelligence/ .

sistemas de IA, num esforço final para impedir que rivais como a China acedam a esta tecnologia avançada. Esta decisão envolve uma estrutura global de exportação com três níveis de países para exportar chips e tecnologia de IA avançada[104]. Num primeiro grupo estão os aliados mais próximos e com maior preponderância no processo de fabricação dos chips. Num segundo nível estão a China e a Rússia, já proibidas de comprar chips avançados, e que vão agora enfrentar restrições à venda de poderosos modelos de IA "fechados". O terceiro grupo, que compreende a maior parte do mundo, terá em breve novos limites na sua capacidade computacional, mas que poderá solicitar quotas adicionais sujeitas a requisitos de segurança. Esta mudança tem como objetivo impedir a China de aceder aos chips de IA através de países terceiros, principalmente no Médio Oriente, cujas restrições estão a ser anunciadas num cenário global de crescente procura por chips de IA produzidos por empresas como a Nvidia, AMD e Intel.

A nova estrutura regulamentar do governo dos EUA sobre a exportação de chips de computação avançada utilizados para desenvolver IA, afetará cerca de 120 países, muitos dos quais são membros da UE[105], como a imagem abaixo ilustra. O que realmente poderá ser um pouco estranho é a posição de Portugal neste quadro, face à posição anteriormente assumida sobre o 5G, em que foi um dos 10 países da UE que seguiu as orientações de Bruxelas[106] e alinhada com os EUA. Assim, nesta decorrência, estabeleceu critérios objetivos de avaliação dos riscos para a segurança das redes e serviços nacionais decorrentes do uso da tecnologia 5ª Geração de telecomunicações em Portugal[107], onde a presença de fornecedores chineses desta geração móvel ficou limitada. Posição esta que contrasta de forma clara com a posição assumida por Espanha[108], a qual pelos vistos não deverá ter tido reflexos nesta recente decisão do governo dos EUA, colocando o país vizinho no nível de países de maior confiança.

---

104 Carvajal, Nikki & Liu, Juliana (2025). Biden unveils last round of AI chip curbs aimed at China, Russia. *CNN*. https://edition.cnn.com/2025/01/13/tech/china-us-biden-chips-ai-curbs-hnk-intl/index.html .

105 WAM (2025). EU criticises US restrictions on AI chip exports. *Emirates News Agency*.https://www.wam.ae/article/bhopap1-criticises-restrictions-chip-exports .

106 Brito, Ana (2024). Bloqueio à Huawei divide Europa, Espanha afasta-se de Portugal. *Público*. https://www.publico.pt/2024/03/09/economia/noticia/bloqueio-huawei-divide-europa-espanha-afastase-portugal-2083075 .

107 https://www.gns.gov.pt/docs/cas-deliberacao-1-2023.pdf .

108 Rodrigues, José (2024). Espanha rejeita excluir Huawei do 5G. *Dinheiro Vivo*. https://dinheirovivo.dn.pt/espanha-rejeita-excluir-huawei-do-5g .

Figura 2 – Mapa dos Estados-Membros da UE, conforme as restrições aplicadas[109]

Esta nova situação originou uma declaração conjunta[110] da Vice-Presidente Executiva Henna Virkkunen e do Comissário do Comércio e Segurança Económica, Relações Interinstitucionais e Transparência Maroš Šefčovič referindo que

"*Acreditamos que é também do interesse económico e de segurança dos EUA que a UE adquira chips avançados de IA aos EUA sem limitações: cooperamos estreitamente, em especial no domínio da segurança, e representamos uma oportunidade económica para os EUA, e não um risco para a segurança*."

A abordagem americana na defesa dos seus interesses mostra que este tipo de decisões vão ter impacto na coesão europeia, podendo contribuir para uma certa conflitualidade interna entre os Estados Membros. E vem ainda mostrar que é independente do tipo de administração nos EUA, seja ela democrata ou republicana, sendo de esperar que com a nova administração de Donald Trump na Casa Branca se agravem os conflitos com a UE. Assim, a liderança da UE terá de ser mais firme na defesa dos seus valores e dos seus cidadãos, para manter a sua soberania e respeito internacional.

Em termos de conclusão pode argumentar-se que em tempos de prosperidade a produção é concentrada em locais onde os custos de produção são baixos e tempos de instabilidade

109 https://www.reddit.com/r/MapPorn/comments/1i2vgfh/us_tier_1_and_tier_2_division_of_ai_chip_export/#lightbox .

110 EC (2025). Joint Statement by Executive Vice-President Henna Virkkunen and Commissioner Maroš Šefčovič . https://ec.europa.eu/commission/presscorner/api/files/document/print/en/statement_25_255/STATEMENT_25_255_EN.pdf .

adota-se o protecionismo e o "*Techno-nationalism*"[111]. Este ocorre quando as nações lutam para garantir o acesso a fontes críticas de fornecimento para si próprias, enquanto procuram sufocar o acesso de concorrentes e rivais. O CHIPS Act, afastando-se das normas liberais, representa uma mudança significativa nas relações comerciais internacionais, levando a consequências imprevisíveis, ao nível de preços e da cadeia logística. Isto porque os consumidores podem enfrentar perturbações à medida que as empresas procuram fornecedores alternativos, resultando em custos mais elevados e produtos de menor qualidade. Por sua vez, as interrupções na cadeia de abastecimento podem também atrasar o lançamento de novos produtos, e as ações comerciais de retaliação podem afetar vários setores.

iii) A Europa no caminho intrincado dos semicondutores

Os ideais fundamentais da UE sempre incluíram o comércio aberto, um sistema multilateral e padrões globais. Para proteger estes princípios e para fazer face a este novo ambiente, complexo, dividido e hostil, a UE tem vindo a trabalhar num conjunto de ferramentas políticas. Por outro lado, tem sido frequentemente líder na regulamentação de tecnologias vitais em desenvolvimento, tendo em vista proteger o seu mercado interno e lidar com as vulnerabilidades tecnológicas e dependências estratégicas.

A cadeia de abastecimento de semicondutores é global, especializada e muito interdependente. Cerca de 80% dos fornecedores e 63% dos clientes das empresas da cadeia de valor da UE estão fora deste espaço, o que revela uma grande vulnerabilidade e dependência geopolítica, fazendo com que a UE esteja dependente de jurisdições estrangeiras[112]. As matérias-primas, a água e a dependência energética constituem-se como potenciais vulnerabilidades no caso surgirem riscos naturais ou provocados pelo homem.

No briefing do Parlamento Europeu anteriormente mencionado é referido que a China, os EUA e a UE são rivais globais no comércio, na geopolítica, na área militar, na economia e na tecnologia. Refere que a *Belt and Road Initiative* (BRI) da China vai desafiar o domínio tradicional dos EUA e da UE e que a atual política comercial dos EUA visa impedir que a China se torne um líder tecnológico global, particularmente na transição

111 Hyatt, Katherine; Ryle, Patrick & McKnight, Mark (2025). Semiconductor production, geopolitics and the CHIPS ACT of 2022: a theoretical analysis. *Digital Policy, Regulation and Governance*.
112 Cerutti, Isabella & Nardo, Michela (2023). Semiconductors in the EU. *Publications Office of the European Union, Luxembourg*. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC133850/JRC133850_01.pdf .

verde e na IA. Por sua vez, é indicado que os EUA estão a encorajar a UE a seguir uma política semelhante. Este documento refere ainda que a indústria de semicondutores da UE está bem posicionada para servir os setores automóvel, aeroespacial e de automação industrial. E reforça que a UE tem uma posição de liderança em termos de sustentabilidade, sendo este um motor de crescimento a longo prazo, e que empresas da UE são líderes globais na produção de equipamentos de fabrico de chips e na sua cadeia de abastecimento associada.

Em 2022, a UE adotou o seu próprio pacote de incentivos a esta nova tecnologia através do *European Chips Act*,[113] que visa reforçar o ecossistema de semicondutores na UE, garantir a resiliência das cadeias de abastecimento e reduzir as dependências externas. É um passo fundamental para a soberania tecnológica da UE, tendo em vista a meta da década digital de duplicar a quota da UE no mercado global de semicondutores para 20%. Serão mobilizados 43 mil milhões de euros[114] em investimentos públicos e privados e estabelecidas medidas para preparar, antecipar e responder rapidamente a quaisquer futuras perturbações na cadeia de abastecimento, juntamente com os Estados-Membros e os nossos parceiros internacionais, sendo estes fundamentais.

O EU *Chips Act* apresenta cinco 5 objetivos estratégicos, nomeadamente (1) reforçar a liderança em investigação e tecnologia; (2) desenvolver e reforçar a capacidade da Europa para inovar na conceção, fabrico e embalagem de chips avançados; (3) implementar um quadro adequado para aumentar a produção até 2030; (4) encontrar solução para a escassez de competências e atrair novos talentos e (5) desenvolver uma compreensão profunda das cadeias globais de fornecimento de semicondutores.

No anúncio oficial do *European Chips Act*, Ursula Von Der Leyen, presidente da Comissão Europeia[115], refere que:

"Esta Lei Europeia dos Chips chega absolutamente na hora certa. E tem dois objetivos principais: o primeiro objetivo é, a curto prazo, aumentar a nossa resiliência a crises futuras, antecipando e, assim, evitando interrupções na cadeia de abastecimento. E a

113 EC (n.d.). European Chips Act**.** https://digital-strategy.ec.europa.eu/en/policies/european-chips-act .
114 EC (n.d.). European Chips Act**.** https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en .
115 EC (2022). Statement by President von der Leyen on the European Chips Act. https://ec.europa.eu/commission/presscorner/detail/en/statement_22_866 .

segunda parte é, naturalmente, olhar para o médio prazo e fazer da Europa um líder industrial neste mercado tão estratégico".

Assim, verifica-se que a UE está a empenhada em atrair novas empresas de semicondutores e em incentivar as empresas existentes a expandir ou estabelecer novas instalações para esta tecnologia. Um exemplo é o programa *European Chips Skills 2030 Academy*[116] que pretende produzir uma força de trabalho de 500 000 especialistas em microeletrónica, essenciais para a implementação do *European Chips Act*[117]. Na ausência de indivíduos altamente competentes, existem preocupações de que a Europa possa ficar muito aquém das suas metas de capacidade de fabrico até 2030.

Por sua vez, a Intel, um dos principais produtores de semicondutores, anunciou um investimento inicial de mais de 33 mil milhões de euros para I&D e fabrico na UE[118]. Este investimento destina-se a promover o ecossistema de semicondutores de classe mundial na Europa, abrangendo França, Alemanha, Irlanda, Itália, Polónia e Espanha.

Na Alemanha, a Intel vai receber do Governo alemão 10 mil milhões de euros para produzir semicondutores em Magdeburgo[119]. A previsão da empresa era a criação de 3 000 postos de trabalho diretos, que poderia chegar aos 10 000. Esta situação constitui-se como o maior investimento estrangeiro direto na Alemanha desde o fim da II Guerra Mundial, e a empresa prometeu elevar a fatura para os 30 mil milhões. A construção irá ocupar 400 hectares de 1000 hectares previstos para um novo parque de tecnologia que o ministro da Economia deste estado, Sven Schulze, disse ver como o futuro "coração europeu da indústria dos chips". O projeto inicial contempla duas fábricas, com um custo total de 68 mil milhões de euros, naquilo que seria o maior investimento isolado de um privado estrangeiro em toda a Europa.

Importa aqui referir que em 2022 a Intel continuava com a construção de várias fábricas pelo mundo inteiro, onde um dos seus focos era a construção de instalações no Ohio e no

116 ECSA (2024. European Chips Skill Academy. https://chipsacademy.eu/ .
117 Pelé, Anne-Françoise (2023). SEMI Europe Secures €4M to Address Skills Shortage. *EE Times Europe*. https://www.eetimes.eu/semi-europe-secures-e4m-to-address-skills-shortage/ .
118 Intel (2022). Intel Announces Initial Investment of Over €33 Billion for R&D and Manufacturing in EU. https://www.intel.com/content/www/us/en/newsroom/news/eu-news-2022-release.html .
119 Ferreira, Victor (2023). A aposta da Intel "é boa para a Alemanha", mas sem a UE "vale nada". *Público*.https://www.publico.pt/2023/07/03/economia/entrevista/aposta-intel-boa-alemanha-ue-vale-nada-2055373.

Arizona, nos EUA, enquanto na Europa a grande aposta era na Alemanha.[120] Neste esforço está o Intel 18A, que se constitui como uma iniciativa de desenvolvimento da Intel para a próxima geração de tecnologia de semicondutores[121]. Os chips que utilizam este processo serão baseados num tamanho de nó de 1,8 nanómetros (nm), colocando a Intel ligeiramente à frente do processo N2 da TSMC, que opera a 2 nm[122]. A estratégia para o Intel 18A inclui também o desenvolvimento de uma nova arquitetura conhecida como *Ribbon Field Effect Transistor* (RibbonFET), que a Intel diz oferecer mais desempenho por watt do que os projetos de arquitetura de chips anteriores. Assim, tenciona superar a concorrência, como a TSMC e a Samsung e voltar à liderança destes processos em 2025[123].

Entretanto, em setembro de 2024, a Intel e a *Amazon Web Services* (AWS) expandem a sua colaboração estratégica, com um plano multianual e multibilionário, na promoção do fabrico de chips nos EUA[124]. Estas empresas vão investir no design de chips personalizados, tendo em vista ajudar os clientes a executar as suas tarefas e acelerar o desempenho das aplicações de IA. O Intel 18A, o elemento mais poderoso que a Intel possui e com o qual se quer afirmar novamente como líder na fabricação de semicondutores, vai ter o seu emprego de IA para a AWS.

Nesta decorrência, a Intel anunciou o adiamento da construção da fábrica de chips em Magdeburg, Alemanha, e de um outro investimento na Polónia por dois anos[125]. Como efeito direto desta decisão da Intel, o programa dos chips da UE implode[126]. Esta decisão prejudica seriamente a ambiciosa meta da UE de aumentar a sua quota de mercado global de microchips até 2030. A estratégia da Comissão Europeia, liderada anteriormente por

---

120 Pplware (2023). Intel recebe um enorme pedido para chips 18A: será que a Nvidia deixou a TSMC? https://pplware.sapo.pt/gadgets/hardware/intel-recebe-um-enorme-pedido-para-chips-18a-sera-que-a-nvidia-deixou-a-tsmc/ .

121 Kerner, Sean (2025). Intel's dramatic decline highlights its struggle to compete in a rapidly evolving tech landscape, as its market value lags giants such as Nvidia and AMD. https://www.techtarget.com/whatis/feature/Intels-rise-and-fall-A-timeline-of-what-went-wrong .

122 Trefis Team (2024). Trump, 18A Make Intel's Foundry More Valuable Than Ever. *Nasdaq*. https://www.nasdaq.com/articles/trump-18a-make-intels-foundry-more-valuable-ever .

123 Walker, Matthew (2024). Intel 18A Node Explained: How RibbonFET Boosts AI Scalability. *Electropages*. https://www.electropages.com/blog/2024/10/intel-18a-future-semiconductor-technology-ribbonfet-and-powervia .

124 Amazon (2024). Intel and AWS Expand Strategic Collaboration, Helping Advance U.S.-Based Chip Manufacturing. https://press.aboutamazon.com/aws/2024/9/intel-and-aws-expand-strategic-collaboration-helping-advance-u-s-based-chip-manufacturing .

125 Intel (2024). Pat Gelsinger on Foundry Momentum, Progress on Plan. https://www.intel.com/content/www/us/en/newsroom/news/foundry-momentum-progress-plan.html#gs.fafv46 .

126 Haeck, Pieter (2024). The EU's chips plan implodes as Intel pauses investments. *Politico*. https://www.politico.eu/article/intel-germany-chips-plant-competitiveness-eu-ambition/ .

Thierry Breton, sofre um duro golpe com esta notícia, apesar das tentativas de Ursula von der Leyen de minimizar o impacto. O sucesso do plano agora depende em grande parte de investimentos menores e em tecnologia menos avançada, colocando em dúvida a capacidade da Europa de competir com os EUA, China e Coreia do Sul. A posição da Europa no fabrico global de microchips depende agora da instalação de uma fábrica da TSMC em Dresden e de vários projetos mais pequenos, concentrados principalmente no setor automóvel. No entanto, estes chips não representam as iniciativas inovadoras que a estratégia pretendia promover. As dificuldades dos semicondutores na UE são, assim, um mau presságio para os planos de política industrial.

Por seu lado, a Intel afirmou o seu compromisso de manter a sua expansão nos EUA nos Estados do Arizona, Novo México, Oregão e Ohio[127]e garantiu grandes contratos com a tecnologia Intel 18A[128], nomeadamente com o Departamento de Defesa dos EUA para o programa RAMP-C, que procura trazer tecnologia de semicondutores de ponta para o mercado interno. Outros clientes importantes incluem, para além da Amazon, a Microsoft, que pretendem conceber chips personalizados, incluindo aceleradores de IA.

IV. ELEMENTOS CONCLUSIVOS

Face ao acima exposto, verifica-se que existe uma complexa interação entre a geopolítica, a economia e a tecnologia e onde a indústria dos semicondutores se constitui um bom exemplo num contexto de "*Slowbalization*". A crescente competição entre grandes potências, como os EUA e a China, é um fator que influencia a dinâmica tecnológica e a geopolítica, cada vez mais marcada por uma "*Fragmentegration*". As tensões internacionais são alimentadas pela busca de vantagem tecnológica, onde os governos utilizam a diplomacia, as barreiras comerciais, os controlos de exportação e políticas industriais para remodelar a produção e as cadeias de abastecimento adotando o "*Techno-nationalism"*. Por sua vez, esta competição entre grandes potências manifesta-

127 King, Ian (2024). Intel to Make Custom AI Chip for Amazon, Delay German Plant. Bloomberg. https://www.bloomberg.com/news/articles/2024-09-16/intel-to-make-custom-ai-chip-for-amazon-delay-german-plant?leadSource=uverify%20wall .
128 Trefis Team (2025). New Fab Process Can Boost Intel Stock. *Forbes*. https://www.forbes.com/sites/greatspeculations/2025/01/09/18a-process-can-boost-intel-stock/ .

se através de atividades na "*grey zone*", num contexto cada vez mais híbrido, que é viabilizado pela tecnologia.

Assim, pode dizer-se que o ciberespaço é um novo campo de batalha, uma vez que o ciberespaço deixou de ser uma questão meramente técnica para se tornar um palco de competição geopolítica e económica, com impactos na segurança e na soberania dos estados. Esta situação contribuiu para uma fragmentação da internet, a qual representa uma ameaça às sociedades, para as suas economias, bem como aos direitos humanos e à liberdade de expressão.

Estes desenvolvimentos tiveram reflexo na diplomacia, a qual está a evoluir para enfrentar os desafios da era digital, através da criação de novos cargos de embaixador, da adoção de novas ferramentas e da crescente necessidade de colaboração internacional. Na rivalidade tecnológica, um dos destaques vai para a indústria de semicondutores, a qual é essencial para a economia e para a segurança, com grandes implicações para as operações militares, com uma produção concentrada em poucos países e sujeita a tensões geopolíticas. A competição tecnológica entre EUA, China e outros países está a remodelar a ordem mundial, com a necessidade de garantir a segurança da cadeia de abastecimento e a soberania digital, levando à criação dos *US Chips Act*, do *EU Chips Act*, bem como de um programa similar na China. Esta realidade afasta-se das normas liberais que têm regido o mundo num passado relativamente recente, e representa uma alteração substancial nas relações comerciais internacionais.

Por um lado, a indústria dos semicondutores comporta muitos milhares de milhões de dólares/euros, com lucros muito substanciais, com algumas matérias a rondar o quase monopólio, o que gera o interesse de grandes empresas na área da produção, bem como de investidores internacionais. Por outro lado, a valorização desta indústria e os custos na continuidade de se atingir um desenvolvimento desenfreado, começa a levantar dúvidas, até por alguns eventuais interesses obscuros associados. A diversidade de áreas onde os chips são necessários, terão obviamente requisitos diferenciados, pelo que uma boa estratégia pode ser a de se aproveitar a rivalidade atual entre os EUA e a China, não sendo necessário para todas as áreas ter-se um *State of the Art* de aplicação em situações muito específicas, como aquelas associadas à indústria do armamento.

Neste ambiente volátil entre os EUA e a China, a UE enfrenta um enorme dilema e grandes desafios para alcançar os seus objetivos de autonomia digital e de competitividade no mercado de semicondutores. Isto porque os EUA, ao diferenciarem

Estados-Membros para a exportação de chips, vão dificultar a ação conjunta e integrada da UE. Por outro lado, verifica-se que empresas dos EUA adotam as suas prioridades de forma unilateral face aos compromissos assumidos com a UE, situação que limita o cumprimento de objetivos por esta traçados para o seu posicionamento internacional. Assim, não sendo necessário "inventar a roda", é importante a clarificação de uma estratégia holística e integrada entre os Estados-Membros, com uma aposta direcionada para a inovação, a investigação e o desenvolvimento. Concomitantemente, a UE deveria assumir uma ação concertada para garantir uma posição credível e sustentada neste cenário global, procurando novos mercados e novos parceiros, tendo em vista salvaguardar os cidadãos e a economia europeia, onde a diplomacia terá naturalmente uma palavra importante.

Finalizando, pode dizer-se que os desenvolvimentos futuros das tecnologias, a evolução da ciência dos dados e as correntes resultantes da geopolítica irão induzir mudanças significativas. Uma mistura destas forças irá expor a indústria dos chips a ameaças reais, bem como a eventuais oportunidades, situações que serão observadas e sentidas na sociedade.

CYBERLAW

BY CIJIC

DA SEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS PELO PODER JUDICIAL EM PORTUGAL E NO BRASIL [1] [2]

MANUEL DAVID MASSENO [3]

1 Com pequenos ajustes terminológicos, este texto constitui uma versão do escrito para a Obra coletiva em homenagem ao Ministro [Juiz Conselheiro] Ricardo Villas Bôas Cueva, por ocasião dos 13 anos que completou no Superior Tribunal de Justiça em junho de 2024, devendo ter por referência peças processuais ou trabalhos académicos dele, in casu o estudo "Segurança da informação e proteção de dados pessoais" In FRANCOSKI, Denise de Souza Luiz & TASSO, Fernando Antonio (coord.). A Lei Geral de Proteção de Dados Pessoais: aspectos práticos e teóricos relevantes no setor público e privado: LGPD. São Paulo: Thomson Reuters / Revista dos Tribunais, 2021. pp. 539-550. A Obra de qua é coordenada por Ana Frazão et al. e a sua publicação está prevista para abril de 2025, pela Editora Mizuno, de São Paulo, com cerca de 9 meses de atraso relativamente ao inicialmente projetado.

2 A redação de este estudo contou com o apoio de vários Colegas que contribuíram para o mesmo com conteúdos não disponíveis publicamente e / ou com leituras preliminares como Alexandre Sousa Pinheiro, Cleórbete Santos, José Joaquim Martins, Karine Borges de Liz e Valéria Reani Rodrigues Garcia, aos quais deixo os devidos agradecimentos, tal como aos organizadores da Obra pelo honroso convite. Obviamente, todos os erros e omissões são da minha exclusiva responsabilidade.

3 Professor Adjunto e DPO do Instituto Politécnico de Beja, onde também coordena o Laboratório UbiNET – Segurança Informática e Cibercrime e o MESI; é ainda Investigador Colaborador do CEG-UAb e Membro Convidado do CDPC, lecionando há mais duma década sobre Proteção de Dados em diversas instituições universitárias de topo e colaborando com a OAB no Brasil e a EDEN da Europol. Para contacto: masseno@ipbeja.pt

RESUMO:

Prima facie, os regimes previstos para o tratamento de dados pessoais pelo Poder Judicial no Regulamento Geral sobre Dados Pessoais da União Europeia (RGPD) e na Lei Geral sobre Proteção de Dados Pessoais (LGPD) brasileira são muito semelhantes, incluindo a previsão da especificidade da Justiça criminal. Porém, para além da persistente omissão do legislador brasileiro no referente à "LGPD Penal", as profundas divergências quanto ao enquadramento legislativo relativamente à autonomia normativa e administrativa do Poder Judicial em Portugal e no Brasil resultam em realidades muito distintas, mormente no que se refere à responsabilidade relativa à segurança no tratamento dos dados. O presente artigo analisa, detalhada e criticamente, ambos regimes, sobretudo aplicando a metodologia própria do Direito Comparado.

Palavras-chave: Brasil; Comparação; Poder Judicial; Portugal; Proteção de Dados Pessoais.

ABSTRACT:

Prima facie, the legal regimes of personal data processing by the Judiciary at the General Data Protection Regulation of the European Union (GDPR) and the Brazilian General Personal Data Protection Law (LGPD) are quite similar, including a specific regime for the processing for law enforcement. However, notwithstanding the enduring omission of the Brazilian legislative regarding the "Criminal LGPD", the deep differences regarding the regulatory and administrative autonomy of the Judiciary in Portugal and in Brazil led to very diverse realities, mostly concerning the responsibilities related to security in data processing. This paper analyses, in a detailed and critical manner, both legal regimes, mainly applying the methodologies of Comparative Law research.

Keywords: Brazil; Portugal; Comparison; Judiciary; Personal Data Protection.

I. O TRATAMENTO DE DADOS PESSOAIS PELO PODER JUDICIAL EM PORTUGAL E NO BRASIL, ALGUMAS QUESTÕES PRELIMINARES

Começando por uma pré-compreensão dos problemas[1], inclusive antecipando as conclusões, podemos adiantar que os dois Ordenamentos partem de referências comuns e têm passado por vicissitudes semelhantes. Embora seguindo vias paralelas, sobretudo por força dos distintos contextos institucionais, e sendo problemática a sua convergência. Efetivamente, tanto um quanto o outro assentam nos regimes gerais aplicáveis à Proteção de Dados Pessoais, embora prevejam também disciplinas suscetíveis de melhor responderem às diferentes necessidades sociais a serem satisfeitas através do exercício da judicatura.

Assim, relativamente a tais tratamentos, se em Portugal vigora o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, *relativo à proteção das pessoas singulares* [físicas] *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*) – o *RGPD*[2], complementado pela Lei n.º 58/2019, de 8 de agosto; no Brasil, é aplicável a Lei n.º 13.709, de 14 agosto de 2018, *Lei Geral de Proteção de Dados Pessoais* – a *LGPD*[3].

---

1 Para um enquadramento transversal das questões relativas à Proteção de Dados pela Justiça, além das considerações presentes na generalidade dos estudos referidos neste texto, têm um especial interesse as reflexões de DONEDA (2022), produzidas por solicitação da UNESCO - Organização das Nações Unidas para a Educação, a Ciência e a Cultura.

2 Concretamente, o *Considerando* (20) do *RGPD* explicita, que, "Na medida em que o presente regulamento é igualmente aplicável, entre outras, às atividades dos tribunais e de outras autoridades judiciais, poderá determinar-se no direito da União ou dos Estados-Membros quais as operações e os procedimentos a seguir pelos tribunais e outras autoridades judiciais para o tratamento de dados pessoais. A competência das autoridades de controlo não abrange o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional, a fim de assegurar a independência do poder judicial no exercício da sua função jurisdicional, nomeadamente a tomada de decisões. Deverá ser possível confiar o controlo de tais operações de tratamento de dados a organismos específicos no âmbito do sistema judicial do Estado-Membro, que deverão, nomeadamente, assegurar o cumprimento das regras do presente regulamento, reforçar a sensibilização os membros do poder judicial para as obrigações que lhe são impostas pelo presente regulamento e tratar reclamações relativas às operações de tratamento dos dados.". A este propósito, são de atender as considerações breves de CASTRO (2020, 11-13), de MARTINS (2022, 114-117) e de WENGOROVIUS (2023, 448-449).

3 A propósito do sentido e das especificidades da aplicabilidade da *LGPD* ao Poder Judicial enquanto "Poder Público", têm muito interesse as considerações de ROCHA (2021), de SANTOS (2021, 94 e 99-101) e de BAIÃO & TEIVE (2022). O que é hoje incontroverso, como mostram as iniciativas do próprio Judicial, a serem abordadas, assim como o "Guia Orientativo sobre o Tratamento de Dados Pessoais pelo Poder Público", da ANPD – Autoridade Nacional de Proteção de Dados, publicado em junho de 2023, cuja versão 2.0 está acessível, https://bit.ly/3QWN1iY. Ainda que extravasando manifestamente o objeto de este estudo, é de acrescentar que esta questão não é confundível com a relativa aos fundamentos de legitimação do tratamento (Artigo 7º da LGPD), como ocorre em parte da Doutrina brasileira.

Do mesmo modo, em ambos os casos é feita uma diferenciação entre os dados tratados pela Justiça no exercício da sua função administrativa e os tratados no da jurisdicional, em sentido estrito (Artigos 2.º n.º 1 e 9.º n.º 1 f), 23.º n.º 1 f), i) e j), 37.º n.º 1 a) e 55.º n.º 3 do *RGPD*, assim como, Artigos 1º, 7.º VI e 23.º *caput* da *LGPD*). Embora essa destrinça seja objetivamente difícil de estabelecer, como mostrou o Acórdão do TJUE – Tribunal de Justiça da União Europeia (Primeira Secção), de 24 de março de 2022, no Processo C-245/20 – X e Z contra *Autoriteit Persoonsgegevens*[4], além de ser de difícil efetivação quanto à segurança dos dados, sobretudo por razões de ordem técnica.

Igualmente, dos correspondentes âmbitos objetivos ficou excluída a Justiça Criminal (Artigos 2.º n.º 2 c) do *RGPD* e 4º III d), este *a contrario*, da *LGPD*). Com efeito, para o tratamento de tais dados estão previstas disciplinas diferenciadas, atendendo aos direitos dos titulares dos dados e às finalidades em causa. Em Portugal, a correspondente previsão foi efetivada através da Lei n.º 59/2019, de 8 de agosto, que *aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais* (transpondo a Diretiva (UE) 2016/680 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*

4 Como concluiu o TJUE, "O artigo 55.º, n.º 3, do [*RGPD*] deve ser interpretado no sentido de que o facto de um órgão jurisdicional disponibilizar temporariamente a jornalistas documentos dos autos de um processo judicial, que contêm dados pessoais, a fim de lhes permitir informar melhor sobre o desenrolar desse processo decorre do exercício, por esse órgão jurisdicional, da sua «função jurisdicional», na aceção desta disposição.". O que decorre de entender que, "(33) […] a preservação da independência do poder judicial pressupõe, de maneira geral, que as funções jurisdicionais sejam exercidas com total autonomia, sem que os órgãos jurisdicionais estejam submetidos a vínculos hierárquicos ou de subordinação nem recebam ordens ou instruções seja de que origem for, estando assim protegidas de qualquer intervenção ou pressão externa suscetível de prejudicar a independência de julgamento dos seus membros e de influenciar as suas decisões. O respeito das garantias de independência e de imparcialidade exigidas pelo direito da União pressupõe a existência de regras que permitam afastar qualquer dúvida legítima, no espírito dos litigantes, quanto à impermeabilidade da instância em causa em relação a elementos externos e à sua neutralidade relativamente aos interesses em confronto [v., neste sentido, designadamente, Acórdãos de 27 de fevereiro de 2018, *Associação Sindical dos Juízes Portugueses*, C-64/16, EU:C:2018:117, n.º 44; de 25 de julho de 2018, *Minister for Justice and Equality* (Falhas do sistema judicial), C-216/18 PPU, EU:C:2018:586, n.º 63; de 24 de junho de 2019, *Comissão contra a Polónia* (Independência do Supremo Tribunal), C-619/18, EU:C:2019:531, n.º 72; e de 21 de dezembro de 2021, *Euro Box Promotion* e o., C-357/19, C-379/19, C-547/19, C-811/19, C-840/19, EU:C:2021:1034, n.º 225]. (34) Como tal, a referência às operações de tratamento efetuadas pelos órgãos jurisdicionais «no exercício da sua função jurisdicional» […] deve ser entendida, no contexto deste regulamento, no sentido de que não se limita aos tratamentos de dados pessoais levados a cabo pelos órgãos jurisdicionais no âmbito de processos concretos, mas sim no sentido de que visa, de maneira mais ampla, o conjunto das operações de tratamento efetuadas pelos órgãos jurisdicionais no âmbito da sua atividade judicial, pelo que estão excluídas da competência da autoridade de controlo as operações de tratamento cuja fiscalização é suscetível, direta ou indiretamente, de ter uma influência na independência dos seus membros ou de pesar nas suas decisões. [Consequentemente,] (35) A este respeito, embora a natureza e a finalidade do tratamento efetuado por um órgão jurisdicional estejam principalmente ligadas ao exame da legalidade deste último, podem constituir indícios que podem revelar que esse tratamento decorre do exercício, por esse órgão jurisdicional, da sua «função jurisdicional»." Sobre este aresto, contamos com o comentário concordante de WENGOROVIUS (2023, 466-471).

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)[5]-[6]; ao passo que, no Brasil, esse desiderato ainda está por concretizar, decorridos quase seis anos desde a publicação da *LGPD*[7].

Da mesma maneira, os dois Ordenamentos postulam a garantia da segurança no tratamento dos dados, como um dos seus "Princípios" (o da «integridade e confidencialidade» do Artigo 5.º n.º 1 f) do *RGPD*, cujo conteúdo é replicado no Artigo 4.º n.º 2 n.º 1 f) da Lei n.º 59/2019, transpondo o Artigo 4.º n.º 1 f) da Diretiva, o qual corresponde ao da "segurança" do Artigo 6º VII da *LGPD*). Aliás, as redações e os conteúdos de ambos enunciados são muito semelhantes:

> "*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 ", no RGPD; ou com a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão*", na *LGPD*.

---

5 Como ocorre com o *RGPD*, o *Considerando* (80) da Diretiva *de qua* esclarece que, "Embora a presente diretiva se aplique também às atividades dos tribunais nacionais e outras autoridades judiciais, a competência das autoridades de controlo não deverá abranger o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional, a fim de assegurar a independência dos juízes no desempenho das suas funções jurisdicionais. Esta exceção deverá ser estritamente limitada às atividades judiciais relativas a processos judiciais, não se aplicando a outras atividades a que os juízes possam estar associados por força do direito do Estado-Membro. Os Estados-Membros podem também prever a possibilidade de a competência das autoridades de controlo não abranger o tratamento de dados pessoais efetuado por outras autoridades judiciais independentes no exercício da sua função jurisdicional, nomeadamente o Ministério Público. Em todo o caso, o cumprimento das regras da presente diretiva pelos tribunais e outras autoridades judiciais independentes deverá ficar sempre sujeito a uma fiscalização independente nos termos do artigo 8.º, n.º 3, da Carta.". A este propósito, são de atender as considerações de MARTINS (2022, 117-118) e de WENGOROVIUS (2023, 465-466).

6 A propósito da distinção e da articulação entre ambos regimes, sobretudo quanto à diferença entre os Direitos Fundamentais protegidos e aos interesses sociais em causa, CASTRO (2020, 15-16) e MASSENO (2022, 2-8), enquanto OLIVEIRA (2019, 160-163) entende não se justificar a duplicação de regimes.

7 Sobre a comummente chamada *LGPD Penal*, apenas deixo notícia de que, em 2020, uma Comissão de Juristas sobre Segurança Pública, nomeada pelo Presidente da Câmara dos Deputados, Rodrigo Maia, presidida pelo Ministro do Superior Tribunal de Justiça Nefi Cordeiro e tendo como Relatora Laura Schertel Mendes, elaborou um "Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal". Depois, sem se basear no "Anteprojeto", a 7 de junho de 2022, o deputado Coronel Armando (PL-SC) apresentou o Projeto de Lei nº 1.515/22, ementado como "Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais", com o então Presidente da Câmara, Arthur Lira, a determinar a criação de Comissão Especial para analisar a matéria, a 20 do mesmo mês. Não tendo ocorrido mais desenvolvimentos, desde essa data. A este propósito, AZEVEDO *et al*. (2022) e FERNANDES & RESENDE (2023, 485-489).

No entanto, os pontos de partida são muito distintos. Assim, em Portugal vigorava, e vigora ainda, a Lei n.º 34/2009, de 14 de julho, que *estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial*, especificando a, ao tempo vigente, Lei n.º 67/98, de 26 de outubro, a *Lei da Proteção Dados Pessoais*, a qual transpusera 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 dados pessoais e à livre circulação desses dados*, embora esta não pretendesse ter um alcance tão amplo, deixando os tratamentos feitos pelos Poderes Públicos de fora do seu âmbito[8].

Por seu turno e na falta de uma Lei sobre proteção de dados pessoais, no Brasil estas questões tinham sido reguladas pela Resolução n.º 215, de 16 de dezembro de 2015, do CNJ – Conselho Nacional de Justiça, a qual *dispõe, no âmbito do Poder Judiciário, sobre o acesso à informação e a aplicação da Lei 12.527, de 18 de novembro de 2011*, explicitamente apenas para as atividades de natureza administrativa do mesmo[9].

Entretanto, ambas as disciplinas passaram, e ainda passam, por processos de transição. Em Portugal e em 2019, a Assembleia da República aprovou o Decreto n.º 333/XIII, alterando a Lei n.º 34/2009, de modo a adequá-la ao *RGPD*[10]. Porém, o mesmo foi "devolvido sem promulgação", ou seja, foi vetado politicamente, pelo Presidente da República, no final de julho, ainda que por razões não relacionadas com a segurança no

---

8 Ao delimitar negativamente o seu âmbito de aplicação, o Artigo 3.º n.º 2 dispunha que "A presente directiva não se aplica ao tratamento de dados pessoais: - efectuado no exercício de actividades não sujeitas à aplicação do direito comunitário, tais como as previstas nos títulos V e VI do Tratado da União Europeia, e, em qualquer caso, ao tratamento de dados que tenha como objecto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse tratamento disser respeito a questões de segurança do Estado), e as actividades do Estado no domínio do direito penal.". Até porque o objetivo estava focado nos tratamentos de dados para fins empresariais, enquanto pressuposto para o funcionamento do Mercado Interno da União Europeia, como mostram os seus *Considerandos* iniciais: "(3) Considerando que o estabelecimento e o funcionamento do mercado interno no qual, nos termos do artigo 7º A do Tratado [*que institui a Comunidade Europeia*, o *Tratado de Roma*, de 25 de março de 1957, na redação resultante do *Tratado de Maastricht*, de 7 de fevereiro de 1992], é assegurada a livre circulação das mercadorias, das pessoas, dos serviços e dos capitais, exigem não só que os dados pessoais possam circular livremente de um Estado-membro para outro, mas igualmente, que sejam protegidos os direitos fundamentais das pessoas; [e] (4) Considerando que o recurso ao tratamento de dados pessoais nos diversos domínios das actividades económicas e sociais é cada vez mais frequente na Comunidade; que o progresso registado nas tecnologias da informação facilita consideravelmente o tratamento e a troca dos referidos dados;", o que era também confirmado pela indicação do Artigo 100.º-A como base, o qual aplicava-se à "[…] aproximação das disposições legislativas, regulamentares e administrativas dos Estados-membros, que têm por objectivo o estabelecimento e o funcionamento do mercado interno." (n.º 1 *in fine*).

9 O que suscita a questão relativa ao alcance do Poder Regulamentar do CNJ, como nos dão conta os estudos de PIZZOL (2019, 312-323) e de MIRANDA (2020, 76949-76958), sem esquecer os apontamentos críticos de STRECK, SARLET & CLÈVE (2006).

10 A múltipla documentação correspondente a este processo legislativo está disponível, em acesso aberto, https://bit.ly/3USuPs2.

tratamento de tais dados[11]. Contudo, não havendo o mesmo sido reapreciado pelo Parlamento até ao final da Legislatura, a iniciativa caducou. Desde esse momento, não foi retomado o processo legislativo, nem há notícias de qualquer movimentação dos Governos os dos Deputados com esse objetivo[12].

No Brasil, porque a *LGPD* apenas entraria em vigor em agosto de 2020[13], o CNJ, pela Portaria n.º 63, de 26 de abril de 2019, começou por criar um Grupo de Trabalho destinado à elaboração de estudos e propostas voltadas à política de acesso às bases de dados processuais dos tribunais.

II. ENQUADRAMENTO DA SEGURANÇA NA PROTEÇÃO DE DADOS NOS DOIS SISTEMAS JUDICIAIS

Em termos gerais, como referimos, em Portugal continua vigente a Lei n.º 34/2009, sempre e quando não contrarie o disposto no *RGPD*. Ao estar explicito, neste diploma legislativo, como já verificámos, que,

> *"Na medida em que o presente regulamento é igualmente aplicável, entre outras, às atividades dos tribunais e de outras autoridades judiciais, poderá determinar-se no direito da União ou dos Estados-Membros [constituído ou a constituir] quais as operações e os procedimentos a seguir pelos tribunais e outras autoridades judiciais para o tratamento de dados pessoais."* (*Considerando* (20)).

O que coloca problemas muito complexos e controversos, em especial quanto à garantia da segurança no tratamento dos dados, sobretudo no respeitante à determinação do(s) responsável(eis) pelo tratamento dos dados [controlador(es)], isto é,

> "[…] *a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as*

11 Sobre a atual situação das Fontes em Portugal, são de atender as considerações sintéticas de CASTRO (2020, 13-15), de MARTINS (2022, 117-118) e de WENGOROVIUS (2023, 448-451 e 471-474).

12 Sendo certo que o CSM, na Sessão Plenária de 4 de outubro de 2022, criou um "grupo de trabalho para elaboração de projeto de alteração do regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial", o qual ainda não foi divulgado e apenas poderá ser tido como um contributo suscetível de espoletar o debate a este respeito; tal como ocorreu com a "Agenda da Reforma da Justiça - Uma reflexão aberta e alargada do judiciário", de março de elaborada por um "Think Tank" constituído pela Associação Sindical dos Juízes Portugueses, com a coordenação do Juiz Conselheiro Nuno Coelho, com recurso a especialistas externos, e em cujo subgrupo de trabalho "Justiça Digital e Inteligência Artificial nos Tribunais", coordenado pelo Juiz de Direito José Joaquim de Oliveira Martins, tivemos o gosto e a honra participar.

13 Por força do seu Artigo.º 65.º II. Embora, essa vigência haja ocorrido no dia 18 de setembro desse ano, após a devido à aprovação pelo Senado da MP 959/2020 (PLV 34/2020) e ao declarado regimentalmente pelo seu Presidente.

finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro [como é o caso], o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro" (Art.º 4.º 7) do *RGPD*)[14]

De uma tal determinação decorrem a(s) correspondente(s) responsabilidade(s) proativa (*accountability*), civil e contraordenacional [administrativa], designadamente no que importa à segurança dos dados[15].

Ora, ainda vigorando a Lei n.º 34/2009, essa responsabilidade cabe ao CSM – Conselho Superior da Magistratura, para todos os tribunais comuns, assim como ao CSTAF – Conselho Superior dos Tribunais Administrativos e Fiscais e à Procuradoria-Geral da República para todo o Ministério Público, sendo cada uma a "entidade responsável pela gestão dos dados" (Artigo 24.º n.ºs 1, 2 e 3, especificamente). Cabendo-lhes, quanto ao nosso objeto, "b) Garantir o cumprimento de medidas necessárias à segurança da informação e dos tratamentos de dados; [e] c) Assegurar o cumprimento das regras de acesso e de segurança referentes ao arquivo electrónico." (Artigo 24.º n.º 2).

O que deverá ser articulado com o *Código de Processo Civil* (Artigo 132.º n.º 4, na redação introduzida pelo Decreto-Lei n.º 97/2019, de 26 de julho, o qual é também aplicável nos Tribunais Administrativos e aos Tribunais Tributários, *ex vi*, Artigos 1.º e 2.º c) e e) dos respetivos *Códigos de Processo*)[16], em cujos termos,

"A tramitação eletrónica dos processos [a regra, sendo excecional e transitória a práticas de atos em papel] deve garantir a respetiva integralidade, autenticidade e inviolabilidade, bem como o respeito pelo segredo de justiça e pelos regimes de proteção e tratamento de dados pessoais e, em especial, o relativo ao tratamento de dados referentes ao sistema judicial."

Do mesmo modo, no respeitante ao regime material, temos que o disposto no *RGPD* quanto à "Segurança do tratamento" (Artigo 32.º)[17] deve ser integrado com as "Medidas

---

14 No mesmo sentido, com considerações adicionais, argumenta WENGOROVIUS (2023, 458-459).

15 Respectivamente, Artigos 5.º n.º 2, 24.º, 25.º, 32.º a 34.º, 82.º e 83.º do *RGPD*, bem como Artigos 47.º a 56.º da Lei n.º 34/2009, incluindo a responsabilidade penal, como é facultado pelo Artigo 84.º *RGPD*, a mesma não abrange a matéria da segurança dos dados. Para um enquadramento articulado da *accountability* com as demais responsabilidades, são sobretudo de atender as considerações de BARBOSA (2018), além das de MASSENO, MARTINS & FALEIROS Jr. (2020).

16 Aprovados pela Lei n.º 15/2002, de 22 de fevereiro, e pelo Decreto-Lei n.º 433/99, de 26 de outubro, A propósito destas questões, são muito pertinentes as reflexões breves, assim como as referências bibliográficas, de TEIXEIRA (2019, 4-8) e de MARTINS (2022, 117-118).

17 "1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos

de segurança" previstas na Lei n.º 34/2009 (Artigo 42.º)[18], as quais são plenamente compatíveis e até o adaptam às finalidades próprias da função jurisdicional, embora devam ser lidas na pespectiva da neutralidade tecnológica intertemporal, em atenção ao período já transcorrido[19].

Neste âmbito, uma questão crucial prende-se com a obrigatoriedade de realização de uma AIPD – avaliação [relatório] de impacto sobre a proteção de dados,

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

---

e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado: a) A pseudonimização e a cifragem dos dados pessoais; b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento. 2. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.". Sobre a disciplina da segurança no tratamento de dados pessoais no Sector Público, remeto para o meu estudo técnico detalhado (MASSENO 2024), tendo também interesse a perspectiva, aliás não coincidente, de ALVES (2021).

18 Assim, "1 - Tendo em vista a segurança dos dados, são objecto de controlo: a) A entrada nas instalações utilizadas para o armazenamento de dados, a fim de impedir o acesso às mesmas por pessoa não autorizada; b) Os suportes utilizados, a fim de impedir que possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada; c) A consulta dos dados, a fim de assegurar que é efectuada apenas por pessoas autorizadas e que se processa nos termos da presente lei; d) A inserção, a alteração, a eliminação e a realização de qualquer outra operação sobre os dados, de forma a verificar-se que operações foram realizadas, quando e por quem, e para impedir a introdução, assim como qualquer tomada de conhecimento, alteração ou eliminação não autorizadas dos mesmos; e) Os sistemas de tratamento automatizado de dados, para impedir que possam ser utilizados por pessoas não autorizadas, através de instalações de tratamento de dados; f) A transmissão de dados, para garantir que o envio destes, através de instalações de transmissão de dados, se limite às entidades autorizadas; g) A transmissão de dados e o transporte de suportes de dados, para impedir que os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada; h) O acesso aos dados a partir de fora das instalações físicas onde se encontram armazenados, de modo a garantir a sua segurança. 2 - O controlo da consulta dos dados e das operações realizadas sobre os dados, previsto nas alíneas c) e d) do número anterior, é feito através do registo electrónico referido no n.º 3 do artigo 29.º, devendo esse registo ser periodicamente comunicado aos responsáveis pela gestão dos dados, para fins de auditoria aos acessos. 3 - Para as finalidades referidas no número anterior é também mantido um registo das permissões de acesso atribuídas a cada utilizador, devendo os dados constantes de tal registo ser eliminados 10 anos após a data do seu registo. 4 - Tendo em vista a segurança e a preservação da informação, são feitas, periodicamente, cópias de segurança da mesma."

19 Aliás, a este propósito, importa atender também à "Atualização dos Critérios de seleção e pseudonimização das decisões Judiciais", relativamente aos aprovados a 23 de março de 2021, aprovada por deliberação do Plenário do CSM, de 11 de abril de 2023; estando disponível o Parecer cujo conteúdo foi adotado, https://bit.ly/3V9KvIG.

elevados semelhantes, pode ser analisado numa única avaliação." (Artigo 35.º n.º 1 do *RGPD*)

Uma exigência que resulta de uma mudança muito significativa relativamente ao modelo anterior de proteção de dados pessoais, na União Europeia e em Portugal, tendo também importantes projeções quanto à segurança dos dados pessoais tratados na atividade jurisdicional. Especificamente e pelo menos, uma AIPD deverá ser feita sempre que estiverem em causa de categorias especiais de dados [dados sensíveis][20] ou for intentada a introdução de tecnologias novas, como ocorre com os sistemas dotados de Inteligência Artificial no apoio à judicatura[21].

Em qualquer caso, atendendo à exclusão das "operações de tratamento efectuadas por tribunais que atuem no exercício da sua função jurisdicional" do âmbito das atribuições das autoridades de controlo, *in casu* a Comissão Nacional de Proteção de Dados (Artigo 55.º do *RGPD*), estará fora de causa a realização de uma consulta prévia[22], pelo menos até existir uma base legal própria que o determine, como já ocorre na Justiça Penal.

No entanto, se aprofundarmos a análise, tornam-se evidentes as consequências de uma decisão de base no que se refere ao funcionamento do Sistema Judicial português, a do controle dos meios materiais afetos ao Órgão de Soberania tribunais por parte do Governo, através do Ministério da Justiça. O que coloca em risco o próprio *Princípio da Separação de Poderes* e a inerente "Independência" da Justiça (Artigos 2.º, 111.º n.º 1, 288.º j) e 203.º da *Constituição da República Portuguesa*). Sem esquecer que a "defesa da independência judiciária e dos processos judiciais" é até suscetível de legitimar a limitação, pelo "direito da União ou dos Estados-Membros", de direitos dos titulares dos dados e dos responsáveis pelo tratamento ou dos subcontratantes [controladores ou processadores], "[…] desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática […]" (Artigo 23.º n.º 1 f)[23].

---

20 Ou seja, de "dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como […] 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." (Artigo 9.º n.º 1 do *RGPD*).

21 Para uma exposição dos pressupostos, conteúdo e procedimentos relativos à realização de uma AIPD, assim como do correspondente enquadramento regulatório, em termos gerais, basta indicar o texto de LOPES (2022, 114-136).

22 "[…] antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados nos termos do artigo 35.º indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco" (Artigo 36.º n.º 1 do *RGPD*).

23 A propósito do sentido e do alcance destas limitações, MARTINS (2022, 120-121) e WENGOROVIUS (2023, 454-56).

Retomando a questão inicial, como foi repetidamente evidenciado aquando do processo legislativo conducente à aprovação parlamentar do Decreto n.º 333/XIII, designadamente pelo CSM, os meios informáticos afetos ao Sistema Judicial continuam sob a dependência do Ministério da Justiça, especificamente do IGFEJ – Instituto de Gestão Financeira e Equipamentos da Justiça, I.P., e não dos Tribunais ou do binómio CSM / CSTAF, por força da respetiva *Lei Orgânica* (Decreto-Lei n.º 123/2011, de 29 de dezembro, Artigos 2.º n.º 1 i) e 14.º n.º 2 j) e l)).

O que é confirmado pela própria Lei n.º 34/2009, quanto às infraestruturas físicas, incluindo as linhas de transmissão e o arquivo eletrónico, ao estar explicito que o IGFEJ

> "[…] *assegura, através do departamento com competência para a matéria em causa, sem prejuízo dos regimes do segredo de justiça e do segredo de Estado, o desenvolvimento das aplicações informáticas necessárias à tramitação dos processos e à gestão do sistema jurisdicional, incluindo a necessária análise, implementação e suporte*" (Artigos 43.º n.º 1 e 26.º n.º 1).

Por isso mesmo e em atenção ao critério presente no *RGPD* para identificar o «Responsável pelo tratamento», *i.e.*, além das "finalidades", é quem determina "os meios" e aplica as "medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento" (Artigos 4.º 7), 24.º n.º 1, 25.º e 32.º n.º 1), temos que, no respeitante à segurança dos dados, este apenas poderá ser o Ministério da Justiça, com a inerente assunção de responsabilidades, incluindo a intervenção específica do respectivo EPD – Encarregado da Proteção de Dados. O que ocorrerá em termos dissociados das demais funções dos responsáveis pelo tratamento, sejam estes o CSM ou o CSTAF[24].

Entretanto, face ao impasse legislativo, foi intentada uma "via criativa", sobretudo destinada a legitimar a anterior situação *de facto*. Sendo certo que a via mais consentânea com a *Constituição* e o *RGPD* teria sido a da transferência das competências e dos meio materiais relativos aos sistemas e às redes informáticas da Justiça para o CSM e para o CSTAF.

Assim, no dia 5 de dezembro de 2023, foi assinado um "Acordo de Tratamento de Dados Pessoais", tendo por objeto tanto a Justiça Cível quanto a Criminal, pelos Presidentes do CSM e do IGFEJ, aliás coadjuvados pelas correspondentes EPDs. De fora ficou a Justiça Administrativa e Fiscal, continuando nesta desagregação entre a determinação das

24 Quanto a esta dissociação funcional, é de atender a posição crítica de MARTINS (2022, 120-121), aliás, em expressa consonância com a versão inicial deste estudo.

finalidades e dos meios de cada tratamento dos dados, com a inerente diferenciação das responsabilidades em matéria de segurança.

Conforme ao Acordo[25], o IGFEJ passou a assumir formalmente a posição de "subcontratante" [processador], tratando os dados por conta do CSM, enquanto "responsável pelo tratamento" [controlador] (Artigo 4.º 7) e 8) e 28.º n.ºs 1 e 3 do *RGPD*). Em especial, o primeiro assumiu obrigações quanto à aplicação de medidas técnicas e organizativas destinadas a efetivar a segurança dos dados objeto de tratamento, assim como no respeitante à notificação das violações de dados pessoais ao CSM, assistindo ainda este na comunicação de tais violações aos titulares dos dados (Cláusulas Sexta, Décima Primeira e Décima Segunda e Décima Terceira).

Por sua vez, no Brasil, a Lei nº 11.419, de 19 de dezembro de 2006, que *dispõe sobre a informatização do processo judicial*, explicita que (Artigo 12, *caput* e § 1º):

> *"A conservação dos autos do processo poderá ser efetuada total ou parcialmente por meio eletrônico.*
>
> *§ 1º Os autos dos processos eletrônicos deverão ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a preservação e integridade dos dados, sendo dispensada a formação de autos suplementares."*

O que pode facilmente ser enquadrado na *LGPD*, em articulação com o, referido, Princípio da "segurança" (Artigo 6º VII) e a disciplina que o densifica (Artigos 46 a 49)[26]. Porém, os poderes aí conferidos à ANPD – Autoridade Nacional de Proteção de Dados, nomeadamente para a definição de "padrões técnicos mínimos" (Artigos 55-J XIII e 46 § 1º), terão de considerar-se como prejudicados pelas competências regulamentares do CNJ, devido ao disposto na *Constituição Federal* com o objetivo de garantir a autonomia do "Poder Judiciário" (Artigos 99 e 103-B § 4º I).

No mesmo sentido, a Lei nº 11.419 determina que "Os órgãos do Poder Judiciário regulamentarão esta Lei, no que couber, no âmbito de suas respectivas competências" (Art. 18), também em função do previsto na Lei Complementar nº 35, de 14 de março de 1979, a *Lei Orgânica da Magistratura Nacional*.

---

25 Embora não tenha sido publicado, o Acordo *de quo* pode ser lido no seguinte endereço, https://bit.ly/3KgdnsC.

26 Quanto à disciplina disposta pela *LGPD* para a segurança no tratamento dos dados pessoais, são de atender as considerações comparatísticas de MASSENO, MARTINS & FALEIROS Jr. (2020) e também o estudo de ROSAS (2022), além do artigo sobre a matéria *de qua* do Ministro Ricardo Cueva (2021), referido *supra*.

Embora, um tal entendimento não afaste uma articulação entre a ANPD e o CNJ, até por maioria de razão relativamente ao disposto na *LGPD* a propósito das "autoridades reguladoras públicas" ou dos "outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais" (Artigos 55-J XXIII e 55-K parágrafo único, embora não podendo ser neste domínio a ANPD "o órgão central de interpretação desta lei e do estabelecimento de normas e diretrizes para a sua implementação.").

Aliás, o CNJ, através da sua Resolução nº 185, de 18 de dezembro de 2013, que *Institui o Sistema Processo Judicial Eletrônico - PJe como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento*, já estabelecera regras sobre a autenticação segura no acesso aos sistemas e a segurança destes (Artigos 4º, 6º, 27 e 28, nomeadamente).

Sempre por iniciativa do CNJ, está em andamento a aplicação da Resolução nº 363, de 12 de janeiro de 2021, que *Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais*[27].

Efetivamente, esta Resolução vai além do previsto na Recomendação nº 73, de 20 de agosto de 2020, que *Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD*, a qual indicara aos órgãos do Poder Judicial brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados, em especial[28],

> "*I - elaborar plano de ação que contemple, no mínimo, os seguintes tópicos: [d)] retenção de dados e cópia de segurança" [e, f) [um] plano de respostas a incidentes de segurança com dados pessoais" [assim como] "III - elaborar ou adequar, bem com publicar nos respectivos sítios eletrônicos, de forma ostensiva e de fácil acesso aos usuários […] b) os registros de tratamentos de dados pessoais contendo, entre outras, informações sobre: [as] 8) medidas de segurança adotadas; [e] 9) a política de segurança da informação."* (Artigo 1º)

Neste sentido e especificamente, a Resolução prevê que os Tribunais venham a,

---

27 A propósito da qual são de atender as considerações breves de SCODRO (2021, 88-90) e de MAIOLINO (2023, 453-454).

28 Sobre o seu conteúdo e contexto da sua adoção pelo CNJ, contamos com os apontamentos de SANTOS (2021, 102-106) e de SCODRO (2021, 87-88).

"*XI – implementar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, nos termos do art. 46 e seguintes da LGPD, por meio: a) da elaboração de política de segurança da informação que contenha plano de resposta a incidentes (art. 48 da LGPD), bem como a previsão de adoção de mecanismos de segurança desde a concepção de novos produtos ou serviços (art. 46, § 1º); b) da avaliação dos sistemas e dos bancos de dados, em que houver tratamento de dados pessoais, submetendo tais resultados à apreciação do CGPD para as devidas deliberações; c) da avaliação da segurança de integrações de sistemas; d) da análise da segurança das hipóteses de compartilhamento de dados pessoais com terceiros;", assim como a "XII – elaborar e manter os registros de tratamentos de dados pessoais contendo informações sobre: [o] g) prazo de conservação e medidas de segurança adotadas, nos termos do art. 37 da LGPD;"* (Artigo 1º)

Além de serem os Tribunais, e não o CNJ, a assumirem a qualidade de controladores, isto é, "pessoa natural ou jurídica [singular ou coletiva], de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (Artigos 5º VI da LGPD)[29], com o apoio de um Comitê Gestor de Proteção de Dados Pessoais, ao qual são assignadas funções explícitas em matéria de segurança (Artigo 1º I e XI b)), cabendo-lhes ainda "designar o encarregado pelo tratamento de dados pessoais" (Artigo 1º II)[30].

Cabe acrescentar que o Supremo Tribunal Federal seguiu uma via paralela, com a aprovação da Resolução STF nº 724, de 2 de março de 2021, que *Institui o Comitê Executivo de Proteção de Dados para identificar e implementar as medidas necessárias à adequação do Supremo Tribunal Federal às exigências da Lei n. 13.709, de 14 de agosto de 2019 (LGPD)*. A mesma foi logo seguida da Resolução STF nº 759, de 17 de dezembro de 2021, a qual *Institui a Política de Privacidade e de Proteção de Dados Pessoais no âmbito do Supremo Tribunal Federal*, em cujos termos,

---

29 Com as inerentes responsabilidades proativa e civil, ao ser problemática a aplicação de sanções administrativas pela ANPD aos tribunais (Artigos 37, 42 a 44, 50 e 52 a 54 da *LGPD*). A este propósito, além das considerações comparatísticas de MASSENO, MARTINS & FALEIROS Jr. (2020), são de atender os estudos de CAPANEMA (2020) e de GONDIM (2021), além das reflexões breves de MORAES (2019) e de ROSAS (2022).

30 A propósito da implementação da Resolução *de qua*, são interessantes os estudos, também empíricos, de ROCHA (2021), de SCODRO (2021, 90-99) e de MAIOLINO (2023, 457-460), além do metodológico de KEPPEN (2024).

"O STF dispõe de Política de Segurança da Informação, além de CCSI [Comitê Corporativo de Segurança da Informação], que especifica e determina a adoção de medidas técnicas e administrativas de segurança para a proteção de dados pessoais contra acessos não autorizados, situações acidentais ou incidentes culposos ou dolosos de destruição, perda, adulteração, compartilhamento indevido ou qualquer forma de tratamento inadequado ou ilícito." (Artigo 19), "[...] adotará boas práticas e governança em segurança da informação visando orientar comportamentos adequados e mitigar os riscos de comprometimento dos dados pessoais tratados em suas atividades jurisdicional e administrativa." (Artigo 20) e "*O Encarregado e o CEPD [Comitê Executivo de Proteção de Dados] deverão manter a Alta Administração do STF informada a respeito de aspectos e de fatos significativos para a integridade dos sistemas do Tribunal. Parágrafo único. Os membros do CEPD e o Encarregado deverão informar e ser informados pelo CCSI sobre os incidentes envolvendo dados pessoais." (Artigo 21); sendo que "Encarregado contará com apoio efetivo do [...] (CEPD) com a finalidade de estabelecer regras de segurança, de boas práticas, de governança, e de procedimentos envolvendo a proteção de dados pessoais para o adequado desempenho de suas funções."* (Artigo 16), *i.e.*, são-lhe atribuídas funções significativamente mais amplas que as previstas na *LGPD* (Artigo 5º VIII e 41 § 2º).

Ainda a este propósito, cumpre dar conta que, mesmo perante a falta de referências explícitas nas Resoluções do CNJ e do STF, o Poder Judicial brasileiro não ficou isento do dever de realizar um "relatório de impacto à proteção de dados pessoais: [*i.e.*, a] documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco." (Artigo 5º XVII da *LGPD*), embora esteja fora de causa que tal ocorra por determinação da ANPD (Artigo 38 da mesma lei), em razão do estatuto constitucional do Poder Judicial[31].

31 Quanto à disciplina predisposta em geral pela *LGPD*, tendo por referência a do *RGPD*, é de referir o texto de GOMES (2019), assim como os apontamentos sobre a sua aplicabilidade aos tribunais de CARDOSO (2022, 576-579), antecedidos de uma explanação do regime geral.

III. A SEGURANÇA NA PROTEÇÃO DE DADOS NA JUSTIÇA CRIMINAL, ESPECIFICIDADES

No respeitante a Portugal, também por imposição do disposto no *Tratado sobre o Funcionamento da União Europeia* (Artigo 83.º n.º 1), decorre que as "regras mínimas" relativas a "infrações penais" apenas podem resultar de "diretivas adotadas de acordo com o processo legislativo ordinário", excluindo os regulamentos.

O que também facilitou técnica, e até politicamente, uma compressão dos direitos dos titulares dos dados na Diretiva (UE) 2016/680 e na Lei n.º 59/2019, em contraste com o previsto no *RGPD* e, consequentemente, na Lei n.º 58/2019[32].

Por essa razão, embora, tal como no *RGPD* e por Princípio, os dados devem ser tratados "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 acidentais, recorrendo a medidas técnicas ou organizativas adequadas." (Artigos 4.º n.º 2 f) da Lei), é patente um maior rigor quanto aos "regist[r]os das atividades de tratamento", pois este, também,

> *"Deve conter: […] i) Uma descrição geral das medidas técnicas e organizativas em matéria de segurança referidas no artigo 31.º" (Artigo 26.º) e também quanto ao "registo cronológico" das atividades de tratamento, o qual deve "[…] permitir determinar o motivo, a data e a hora dessas operações, a identificação da pessoa que consultou ou divulgou dados pessoais e, sempre que possível, a identidade dos destinatários desses dados pessoais", servindo "[…] exclusivamente para efeitos de verificação da licitude do tratamento, autocontrolo, exercício do poder disciplinar e garantia da integridade e segurança dos dados pessoais, bem como no âmbito e para efeitos de processo penal."* (Artigo 27.º n.ºs 2 e 3).

Por seu turno, no tocante à "segurança do tratamento", em sentido próprio, enuncia que,

> "*O responsável pelo tratamento e o subcontratante [o controlador e o processador] adotam as medidas técnicas e organizativas apropriadas a fim de assegurarem um nível de segurança adequado ao risco*[33]*, em particular no que*

32 Sobre estas questões, permito remeter para o meu estudo recente (MASSENO 2022, 5-8), além de para os apontamentos de CASTRO (2020, 15).

33 Como explicitam o *Considerandos* (60) e (61) da Diretiva, "A fim de preservar a segurança e evitar o tratamento em violação da presente diretiva, o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e deverá aplicar medidas que os atenuem, como, por exemplo, a

diz respeito ao tratamento das categorias especiais de dados pessoais referidos no artigo 6.º"[34]

Em especial, o foco é posto no controle do acesso aos sistemas informáticos em casos de tratamento automatizado de dados, inclusive com um alto grau de detalhe[35] (Artigo 31.º n.ºs 1 e 2, respetivamente)[36]. A este propósito, há ainda a referir que a "omissão" pelo Legislador português quanto ao tratamento dever ocorrer "tendo em conta as técnicas mais avançadas, os custos da sua aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos de probabilidade e gravidade variáveis que este tratamento representa para os direitos e liberdades das pessoas singulares, apliquem medidas técnicas e organizativas adequadas a fim de assegurar um

---

cifragem. Estas medidas deverão assegurar um nível de segurança adequado, nomeadamente no que respeita à confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função do risco e da natureza dos dados pessoais a proteger. Ao avaliar os riscos para a segurança dos dados, deverão ser tidos em conta os riscos apresentados pelo tratamento dos dados, tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados, de dados pessoais transmitidos, conservados ou tratados de outro modo, riscos esses que podem conduzir, em particular, a danos físicos, materiais ou morais. O responsável pelo tratamento e o subcontratante deverão assegurar que o tratamento de dados pessoais não seja efetuado por pessoas não autorizadas.", pois "Se não forem tomadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, tais como a perda de controlo dos dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação de identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social importante para as pessoas singulares em causa".

34 Em termos análogos aos do Artigo 9.º n.º 1 do *RGPD*, o preceito refere-se a "dados sensíveis" como os "[…] dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, bem como dos dados genéticos, dos dados biométricos destinados a identificar uma pessoa singular de forma inequívoca, dos dados relativos à saúde ou dos dados relativos à vida sexual ou à orientação sexual." (Artigo 6.º n.º 1).

35 Assim, "[…], o responsável pelo tratamento ou o subcontratante [o controlador ou o processador], tendo em conta a avaliação dos riscos, devem aplicar medidas que: a) Impeçam o acesso de pessoas não autorizadas ao equipamento utilizado para o tratamento (controlo de acesso ao equipamento); b) Impeçam que os suportes de dados sejam lidos, copiados, alterados ou retirados sem autorização (controlo dos suportes de dados); c) Impeçam a introdução não autorizada de dados pessoais, bem como qualquer operação não autorizada relativamente a dados pessoais conservados (controlo da conservação); d) Impeçam que os sistemas de tratamento automatizado sejam utilizados por pessoas não autorizadas por meio de equipamento de comunicação de dados (controlo dos utilizadores); e) Assegurem que as pessoas autorizadas a utilizar um sistema de tratamento automatizado só tenham acesso aos dados pessoais abrangidos pela sua autorização de acesso (controlo do acesso aos dados); f) Assegurem que possa ser verificado e determinado a que organismos os dados pessoais foram ou podem ser transmitidos ou facultados utilizando equipamento de comunicação de dados (controlo da comunicação); g) Assegurem que possa ser verificado e determinado a posteriori quais os dados pessoais introduzidos nos sistemas de tratamento automatizado, quando e por quem foram introduzidos (controlo da introdução); h) Impeçam que, durante as transferências de dados pessoais ou o transporte de suportes de dados, os dados pessoais possam ser lidos, copiados, alterados ou suprimidos sem autorização (controlo do transporte); i) Assegurem que os sistemas utilizados possam ser restaurados em caso de interrupção (recuperação); j) Assegurem que as funções do sistema funcionam, que os erros de funcionamento sejam assinalados (fiabilidade) e que os dados pessoais conservados não possam ser falseados por funcionamento defeituoso do sistema (integridade)."

36 Com especial ênfase nos riscos acrescidos destes tratamentos e nos meios predispostos para os mitigar, remeto para o meu estudo (MASSENO 2022, 5-8).

nível de segurança adequado ao risco" (Artigo 31.º da Lei, em contrate com o 29.º n.º 1 da Diretiva), não poderá ter consequências atendendo ao "Princípio da interpretação conforme", enunciado pelo TJUE desde há quatro décadas[37].

Mais próximos do previsto no *RGPD* estão os enunciados a propósito da "notificação de uma violação de dados pessoais à autoridade de controlo" e da "comunicação de uma violação de dados pessoais ao titular dos dados" (Artigos 30.º e 31.º da Diretiva e 32.º e 33.º da Lei)[38], com a CNPD a assumir as correspondentes funções, em termos análogos ao previsto no *RGPD*. Para o efeito, a mesma conta com a incorporação de um magistrado judicial designado pelo CSM, o qual se ocupará do controle do acesso aos dados e aos registos cronológicos das operações de tratamento (Artigo 43.º).

Neste âmbito, cabe recordar que a aplicação das correspondentes medidas técnicas e organizacionais e a efetivação das obrigações de notificação e de comunicação é feita pelo CSM, enquanto responsável pelo tratamento[39], assistido para tanto pelo IGFEJ, por força do Acordo antes referido.

---

37 Desde os Acórdãos de 10 de abril de 1984, Processo 14/83, Sabine von *Colson e* Elisabeth *Kamann* contra Land Nordrhein-Westfalende, e, mais ainda, 13 de novembro de 1990, Processo C-106/89, *Marleasing* SA contra La Comercial Internacional de Alimentacion SA.

38 Como sublinham o *Considerando* (60) *in fine* e (61) da Diretiva, "[…] logo que o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, deverá comunicá-la à autoridade de controlo, sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar, em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares. Se não for possível efetuar a comunicação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem mais demora injustificada. [e] Caso a violação de dados pessoais seja suscetível de criar um elevado risco para os direitos e liberdades das pessoas singulares, estas deverão ser informadas sem demora injustificada, a fim de permitir que tomem as precauções necessárias. Da comunicação deverá constar a natureza da violação de dados pessoais e recomendações destinadas à pessoa singular em causa para atenuar potenciais efeitos adversos. A comunicação aos titulares dos dados deverá ser feita o mais rapidamente possível, em estreita cooperação com a autoridade de controlo, e de acordo com as orientações fornecidas por esta ou por outras autoridades competentes. Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá que se envie uma comunicação rápida aos titulares dos dados, enquanto a necessidade de aplicar medidas adequadas contra violações de dados recorrentes ou similares poderá justificar um prazo maior para a comunicação. Se não for possível, através do atraso ou da restrição da comunicação à pessoa singular em causa de uma violação de dados pessoais, evitar criar entraves a inquéritos, investigações ou procedimentos oficiais ou legais, evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais, salvaguardar a segurança pública, preservar a segurança nacional ou ainda proteger os direitos e as liberdades de terceiros, essa comunicação poderá, em circunstâncias excecionais, ser omitida.".

39 Nos termos do disposto no Artigo 3.º n.º 1 j) da Lei n.º 59/2019, «Responsável pelo tratamento» é a "entidade competente que […] no caso em que estes ["as finalidades e os meios de tratamento dos dados pessoais"] são determinados por lei, a autoridade nela indicada", o que nos leva de volta ao previsto no Artigo 24.º n.º 1 da Lei n.º 34/2009, também no respeitante à responsabilização civil, contraordenacional [Administrativa] e inclusive penal, Artigos 52.º a 66.º da Lei 59/2019, sendo a previsão da última facultada pelo Artigo 57.º da Diretiva (UE) 2016/680, embora nenhuma das previsões típicas consista no incumprimento de medidas de segurança por parte do responsável, ou responsáveis, pelos tratamentos de dados ou pelos subcontratantes [controladores ou processadores].

Adicionalmente, cumpre ainda dar conta da obrigatoriedade de realizar uma "avaliação de impacto", "No caso de um certo tipo de tratamento ser suscetível de representar um elevado risco para os direitos, liberdades e garantias das pessoas" (Artigo 29.º n.º 1 da Lei), nomeadamente por razões de segurança, a qual pode também conduzir a uma consulta prévia da CNPD,

> *"[…] antes de proceder ao tratamento de dados pessoais a integrar em ficheiro a criar nos casos em que: a) A avaliação de impacto prevista no artigo anterior indique que o tratamento resultaria num elevado risco, na ausência de medidas adequadas para atenuar esse risco; ou b) O tipo de tratamento envolva um elevado risco para os direitos, liberdades e garantias dos titulares dos dados, designadamente se utilizar novas tecnologias.*" (Art.º 30.º).

Quanto ao Brasil e enquanto não estiver em vigor "a legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal" (Artigo 4º IV § 1º da *LGPD*), no mínimo, deverão ser aplicadas as "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais" constantes das citadas Resoluções do CNJ, no quadro da *LGPD*, até porque essa futura legislação deverá observar "os princípios gerais de proteção e os direitos do titular previstos nesta lei". Embora em articulação com os *Princípios do Processo Penal*, o que exige um esforço suplementar por parte do Poder Judicial em cada tratamento dos dados pessoais[40].

Adicionalmente, deve ser explicitado que a previsão segundo a qual a ANPD "[…] *emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais*" (Artigo 4º IV § 3º da *LGPD*), não deve considerar-se aplicável ao Poder Judicial, atendendo ao seu estatuto constitucional. Mas, em todo o caso, o dever de realizar relatórios de impacto também é aplicável nestes tratamentos de dados, até por maioria de razão, atendendo à sua particular incidência em outros Direitos Fundamentais, incluindo o direito à liberdade.

40 Ainda que em termos necessariamente prospectivos, sobretudo atendendo aos riscos decorrentes de tratamentos automatizados de dados para estes fins, são muito pertinentes as considerações de FERNANDES & RESENDE (2023, 485-495).

REFERÊNCIAS

ALVES, Diogo Lopes. "O papel fundamental da Cibersegurança na Proteção de Dados Pessoais". *Anuário da Proteção de Dados – 2020* (2021), p. 121-154. Disponível em: https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/5.-Diogo-Lopes-Alves.pdf.

AZEVEDO, Cynthia Picolo Gonzaga de *et al*. *Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022*. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), (2022). Disponível em: https://irisbh.com.br/publicacoes/analise-comparativa-entre-o-anteprojeto-de-lgpd-penal-e-o-pl-1515-2022/.

BAIÃO, Renata Barros Souto Maior & TEIVE, Marcelo Muller. "O artigo 23 da LGPD como base legal autônoma para o tratamento de dados pessoais pelo poder judiciário". PALHARES, Felipe (coord.). *Temas Atuais de Proteção de Dados*. 2.ª ed. rev. e atual. São Paulo: Thomson Reuters / Revista dos Tribunais (2022), p. 287-302. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/1-introducao-capitulo-11-o-artigo-23-da-lgpd-como-base-legal-autonoma-para-o-tratamento-de-dados-pessoais-pelo-poder-judiciario-temas-atuais-de-protecao-de-dados-ed-2022/1643176497.

BARBOSA, Mafalda Miranda. "*Data controllers* e *data processors*: da responsabilidade pelo tratamento de dados à responsabilidade civil". *Revista de Direito Comercial*, n. 2, p. 423-493 (2018). Disponível em: https://www.revistadedireitocomercial.com/data-controllers-e-data-processors.

CAPANEMA, Walter Aranha. "A responsabilidade civil na Lei Geral de Proteção de Dados". *Cadernos Jurídicos* – Escola Paulista da Magistratura, (2020), a. 21 n. 53, p. 63-170. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf.

CARDOSO, Oscar Valente. "Relatório de Impacto à Proteção de Dados Pessoais nos Tribunais". LIMA, Ana Paula Canto de & ROSAS, Eduarda Chacon (coord.). *LGPD 2022. Debates e temas relevantes*. Recife: Editora Império (2022), p. 579-598. Disponível em: https://www.d2smart.com.br/wp-content/uploads/2022/10/LGPD_Ebook.pdf.

CASTRO, Raquel A. Brízida. "Proteção de Dados e a Diretiva UE 2016/680: o tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação,

deteção ou repressão de infrações penais ou execução de sanções penais". *Cibercriminalidade e Prova Digital*. Lisboa: Centro de Estudos Judiciários (2018, atualizado em 2020), p. 9-15. Disponível em: https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U%3d&portalid=30.

DONEDA, Danilo. *Diretrizes para Atores Judiciais sobre Privacidade e Proteção de Dados*. Paris: Organização das Nações Unidas para a Educação, a Ciência e a Cultura (2022). Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381298_por.

FERNANDES, Fernando Andrade & RESENDE, Ana Paula Bougleux Andrade. "Regulamentação do tratamento automatizado de dados pessoais em matéria penal". *Suprema - Revista de Estudos Constitucionais*, v. 3 n. 1 (2023), p. 471–500. Disponível em: https://www.researchgate.net/publication/372043124_Regulamentacao_do_tratamento_automatizado_de_dados_pessoais_em_materia_penal.

GOMES, Maria Cecília Oliveira. "Relatório de Impacto a Proteção de Dados Pessoais: uma breve análise da sua definição e papel na LGPD". *Revista do Advogado* - AASP, a. 39 n.144 (2019), p. 174-183. Disponível em: https://www.academia.edu/41160034/Relat%C3%B3rio_de_Impacto_a_Prote%C3%A7%C3%A3o_de_Dados_Pessoais_uma_breve_an%C3%A1lise_da_sua_defini%C3%A7%C3%A3o_e_papel_na_LGPD.

GODIM, Glenda Gonçalves. "A responsabilidade civil no uso indevido dos dados pessoais". *Revista IBERC*, v. 4 n. 1 (2021), p. 19–34. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/140.

KEPPEN, Mariana. "Dados em pauta: a adequação dos Tribunais de Justiça à LGPD". *Revista da ACONJUR – Associação dos Consultores Jurídicos do Poder Judiciário do Paraná* (2024), p. 34-49. Disponível em: https://www.aconjurpr.com.br/wp-content/uploads/2023/12/REVISTA-DA-ACONJUR-N.-5-LGPD-E-OS-TRIBUNAIS.pdf.

LOPES, Eliseu F. Pinto. "Avaliação de impacto sobre a proteção de dados". *Privacy and Data Protection Magazine*, n. 5 (2022), p. 101-142. Disponível em: https://www.europeia.pt/resources/media/documents/Revista_Privacy_Data_Protection_Magazine_N5.pdf.

MAIOLINO, Eurico Zecchin. "A LGPD e o Poder Judiciário: desafios de adequação e perspectivas". *Revista Jurídica Brasileira*, v. 3 (2023), p. 449-468. Disponível em: https://revistadaenfam.emnuvens.com.br/renfam/article/view/233.

MARTINS, José Joaquim. "Proteção de Dados e o Sistema Judicial Português – Uma síntese". BARZOTTO, Luciane Cardoso & COSTA, Ricardo Hofmeister de Almeida Martins (Eds.) *Estudos sobre LGPD – Lei Geral de Proteção de Dados – lei nº 13.709/2018: doutrina e aplicabilidade no âmbito laboral*. Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho da 4ª Região / Diadorim Editora (2022), p. 112-128. Disponível em: https://www.trt4.jus.br/portais/media/1063693/E-book-EstudosLGPD-Edjud4.pdf.

MASSENO, Manuel David: "Inteligencia Artificial y Protección de Datos: la "elaboración de perfiles" para la prevención de delitos graves y del terrorismo en las fuentes de la Unión Europea". *Revista Eletrônica do Curso de Direito da UFSM*, v. 17 n. 2 (2022), e83679. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/83679.

MASSENO, Manuel David. "Da Disciplina da Segurança na Proteção de Dados, Aplicada ao Poder Local". *CYBERLAW by CIJIC - Revista Científica sobre Cyberlaw do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa*, Edição XII (2024), p. 116-143. Disponível em: https://www.iuris.edu.pt/xms/files/Cyberlaw-by-CIJIC_12.pdf.

MASSENO, Manuel David; MARTINS, Guilherme Magalhães & FALEIROS Jr., José Luiz de Moura. "A Segurança na Proteção de Dados: Entre o RGPD Europeu e a LGPD Brasileira". Florianópolis. *Revista do CEJUR/TJSC: Prestação Jurisdicional*, v. 8 n. 1 (2020), pp. 1-28. Disponível em: https://doi.org/10.37497/revistacejur.v8i1.346.

MIRANDA, Gladson Rogério de Oliveira. "Ativismo judicial e poder normativo do CNJ". *Brazilian Journal of Development*, v. 6 n. 10 (2020), p. 76947–76959. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/18053.

MORAES, Maria Celina Bodin de. "LGPD: um novo regime de responsabilização civil dito 'proativo'". *Civilistica.com*, a. 8 n. 3 (2019), p. 1-6. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/448.

OLIVEIRA, Inês. "Os regimes especiais de proteção de dados pessoais: exemplos de poluição legislativa da União Europeia?". Lisboa. *Anuário da Proteção de Dados - 2019*, (2019), p. 157-172. Disponível em: https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/7.-Ines-Oliveira.pdf.

PIZZOL, Ricardo Dal. "Limites do poder regulamentar do Conselho Nacional de Justiça. Estudo de um caso: Resolução CNJ nº 236/16". PRETTO, Renato Siqueira de; KIM, Richard Pae & TERAOKA, Thiago Massao Cortizo (coord.). *Federalismo e Poder*

Judiciário. São Paulo: Escola Paulista da Magistratura (2019), p. 311-330. Disponível em: http://www.tjsp.jus.br/download/EPM/Publicacoes/ObrasJuridicas/14-federalismo.pdf?d=637006247774866622.

ROCHA, Willian Alessandro. "LGPD e os dados das secretarias das varas do trabalho". *Revista Síntese trabalhista e previdenciária*, v. 32, n. 386 (2021), p. 188–218. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/introducao-27-lgpd-e-os-dados-das-secretarias-das-varas-do-trabalho-reflexos-da-lgpd-no-direito-e-no-processo-do-trabalho/1590440896.

ROSAS, Eduarda Chacon & HAMAOKA, Sayuri Pacheco. "As medidas de segurança e a accountability do agente de tratamento de dados pessoais no âmbito extrajudicial". LIMA, Ana Paula Canto de & ROSAS, Eduarda Chacon (coord.). *LGPD 2022*, *cit*. (2022), p. 229-247. Disponível em: https://www.d2smart.com.br/wp-content/uploads/2022/10/LGPD_Ebook.pdf.

SANTOS, Luciano Alves dos. "A Lei Geral de Proteção de Dados Pessoais e os seus reflexos no Poder Judiciário brasileiro". *Privacy and Data Protection Magazin*e, n. 1 (2021), p. 92-107. Disponível em: https://www.europeia.pt/resources/media/documents/Revista_Privacy_and_Data_Protection_Magazine_N1.pdf.

SCODRO, Carolina Lopes. "Proteção dos Dados Pessoais nos Tribunais Brasileiros: Análise da influência da Resolução nº 363/2021 do CNJ no TJPR, TJSC, TJGO e TJDFT". *Revista de Política Judiciária, Gestão e Administração da Justiça*, v. 7 n. 1 (2021), p. 82-101. Disponível em: https://www.indexlaw.org/index.php/revistapoliticiajudiciaria/article/view/7853.

STRECK, Lênio L.; SARLET, Ingo W.; CLÈVE, Clèmerson M. "Os limites Constitucionais das resoluções do Conselho Nacional de Justiça (CNJ) e Conselho Nacional do Ministério Público (CNMP)". *Migalhas* (2006). Disponível em: https://www.migalhas.com.br/depeso/20381/os-limites-constitucionais-das-resolucoes-do-conselho-nacional-de-justica--cnj--e-conselho-nacional-do-ministerio-publico--cnmp.

TEIXEIRA, Isabel M.ª Curto. *Proteção de Dados e Processo Civil – Recentes Alterações Legislativas e Novas Problemáticas*. Lisboa. Conselho Superior da Magistratura - Rede Nacional de Juízes para apoiar a actividade da RJE Civil (2019). Disponível em: https://www.redecivil.csm.org.pt/wp-content/uploads/2020/01/PROTECÇÃO-DE-DADOS-E-PROCESSO-CIVIL-Isabel-C-teixeira.pdf.

WENGOROVIUS, Sofia. “Tribunais e Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a proteção de dados (RGPD)”. *O Direito*, A. 155, III (2023), pp. 447-481. Disponível em https://www.cidp.pt/Archive/Docs/f690761892770.pdf.

NOTA FINAL: *embora a versão final do texto date de 10 de maio de 2024, todas as hiperconexões voltaram a ser verificadas no dia 29 de março de 2025.*

CYBERLAW

BY CIJIC

OS DIREITOS FUNDAMENTAIS NA INTERNET: UMA NOVA ERA DE CONSTITUCIONALISMO DIGITAL

DIANA CAMÕES [1]

1 Assessora na Assembleia da República | Mestre em Direito Internacional e Europeu
https://orcid.org/0000-0001-8827-007X .

RESUMO:

A sociedade digital mudou o paradigma da difusão da informação, implicando novos desafios para a proteção dos direitos fundamentais. Progressivamente, as plataformas digitais adquiriram poderes quase ilimitados e são os principais atores da era tecnológica, dispondo da possibilidade de moldar conteúdos, definir os seus termos e condições e restringir os direitos dos seus utilizadores. Nos últimos anos, a legislação da União Europeia revelou uma intenção de garantir a proteção dos cidadãos na Internet, enquanto se garante o bom funcionamento do mercado e a livre inovação. Ainda assim, e considerando a evolução tecnológica ocorrida, o presente estudo procura refletir sobre o impacto que tal terá na proteção dos direitos fundamentais na era do constitucionalismo digital.

Palavras-chave: direitos fundamentais; internet; constitucionalismo digital; proteção de dados.

ABSTRACT:

Digital society changed the paradigm of the diffusion of the information, implying new challenges for the protection of fundamental rights. Progressively, digital platforms have acquired nearly unlimited powers, becoming the main players in this technological era, with the ability to shape content, define their own terms and conditions, and restrict user's rights. In recent years, the European Union's legislation revealed an intention to guarantee the protection of its citizens on the Internet, at the same ensuring the good functioning of the market and its free innovation. Still, and considering the technological evolution, this study aims to reflect on the impact that it will have on the protection of fundamental rights in this era of digital constitutionalism.

Key words: fundamental rights; internet; digital constitutionalism; data protection.

I. INTRODUÇÃO [1]

A sociedade digital[2] é a realidade do século XXI. O desenvolvimento sem precedentes das plataformas digitais[3] fez com que estas assumissem o papel de fórum público, contribuindo para a rápida difusão de informação. Ainda assim, não é possível ignorar os desafios que se colocam à proteção dos direitos fundamentais[4]. As plataformas digitais, na qualidade de entidades privadas, conquistaram a sua autonomia, dispondo de poderes quase absolutos no contexto digital, moldando conteúdos e restringindo os direitos fundamentais dos seus utilizadores[5]. Face aos desafios colocados nesta era de *big data,* emerge a necessidade de se adaptar os valores constitucionais aos desafios da sociedade digital[6]. Como denotam GREGORIO e RADU, "tal como a Internet continua a ser redefinida devido à evolução das tecnologias digitais, o mesmo acontece com o constitucionalismo para além do Estado[7]". Vivemos, assim, num período de "constelação digital[8]", que não deve ser encarado como "uma terra sem Direito[9]".

Neste sentido, a agenda regulatória da UE tem procurado dar uma resposta aos desafios colocados no mundo digital, procurando-se compatibilizar a inovação e a proteção dos direitos fundamentais. Se o RGPD constituiu um marco legislativo[10], antevê-se que o

---

1 Lista de siglas e abreviaturas: CEDH – Convenção Europeia dos Direitos Humanos; CDFUE – Carta dos Direitos Fundamentais da União Europeia; CNPD – Comissão Nacional de Proteção de Dados; CRP – Constituição da República Portuguesa; IA – Inteligência Artificial; n.º - número; p. – página; pp. Páginas; RGPD – Regulamento Geral sobre a Proteção de Dados; TJ – Tribunal de Justiça; UE – União Europeia.

2 POLLICINO, Oreste / BASSINI, Marco / GREGORIO, Giovanni de, *Internet Law and Protection of Fundamental Rights*, Bocconi University Press, Milan, 2022, p. 169.

3 *Vide* SOUSA, Simão Mendes de, *Constitucionalismo Digital – Uma Introdução*, Almedina, Coimbra, 2022. pp. 32-33. O autor evidencia que o surgimento das plataformas digitais reflete o ideal da sociedade liberal, por permitir o acesso a todos os indivíduos à informação que pretendam.

4 Como afirma SILVA, Nuno Sousa e, "Internet e Direitos Fundamentais: uma crescente interação", *Revista de Direito e de Estudos Sociais*, Ano LXII, n.º 4, 2024, pp. 203-233(211) "no contexto da Internet surgiram (e continuam a surgir) fenómenos próprios como as redes sociais, a computação em nuvem, ou o comércio eletrónico".

5 GREGORIO, Giovanni de, "The rise of digital constitutionalism in the European Union", *International Journal of Constitutional Law*, Volume 19, n.º 1, 2021, pp. 41-70(42).

6 Como denota BOTELHO, Catarina dos Santos, "Direito da Concorrência e Proteção de Dados nos contextos português e europeu", in Sofia Pais / Vicente Bagnoli (Coord.) *Temas Atuais de Direito da Concorrência – Economia Digital, Direitos Fundamentais e outros desafios*, Universidade Católica Editora, Porto, 2020, pp. 91-115(97), "tornou-se praticamente impossível viver alheado do mundo digital, sob pena de a pessoa se tornar socialmente alienígena".

7 Tradução nossa. GREGORIO, Giovanni de / RADU, Roxana, "Digital constitutionalism in the new era of Internet governance", *International Journal of Law and Information Technology*, Volume 30, n.º 1, 2022, pp. 68-87(69).

8 SOUSA, Simão Mendes de, *Constitucionalismo Digital…* cit., p. 60.

9 *Ibidem*.

10 Regulamento (UE) n.º 679/2016, de 27 de abril, 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).

mais recente Regulamento IA[11] venha a impactar significativamente o modelo de negócio de todos os que se encontrem abrangidos pelo diploma[12].

Tal contrasta, evidentemente, com o modelo liberal inicialmente apresentado. Acreditava-se, por isso, que as plataformas digitais seriam meramente neutras, limitando-se a armazenar na sua plataforma os conteúdos. Porém, nos últimos anos, elas foram reforçando os seus poderes, através do processamento sem precedentes de dados e a difusão massiva de informação[13]. Promoveu-se um efeito perverso. Aquando da sua proliferação, as plataformas digitais eram encaradas como meio de liberdade e rápida difusão de conteúdos. Destarte, têm sido cada vez mais usadas como mecanismo de desinformação, posições extremadas e, em muitos casos, são nocivas para a proteção dos direitos fundamentais[14]. Tal impacta, em primeira medida, os cidadãos e, claro está, o sistema democrático tal como o conhecemos. Na esteira de SIMÃO MENDES DE SOUSA, "na sociedade de massas atual é muito mais procurada a forma simples de aceder ao conteúdo e, com isso, a personalização se demonstra um trunfo, a democracia não deve ser encarada como uma realidade simples, que se constrói e alimenta autonomamente[15]".

Surge-nos, deste modo, o tema essencial do nosso trabalho. Como podemos assegurar a proteção dos direitos fundamentais na era digital? Quais os direitos que estão em causa? Poderemos falar na existência de uma nova geração de direitos? Essas são algumas das questões que pretendemos responder.

---

11 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.° 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial).

12 Podemos ainda salientar o Pacote legislativo sobre os serviços digitais, apresentado pela Comissão Europeu em dezembro de 2020, o qual inclui o Regulamento sobre os Serviços Digitais – Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais) e o Regulamento dos Mercados Digitais – Regulamento (UE) - Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho de 14 de setembro de 2022 relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828.

13 A salientar este ponto, *vide* GREGORIO, Giovanni, de, *Digital Constitutionalism in Europe – Reframing powers in the algorithmic society*, Cambridge University Press, Cambridge, 2022, p. 39.

14 Na esteira de CASTRO, Raquel Brízida, *Direito Constitucional: Ciberespaço e Tecnologia*, Coimbra, Almedina, 2023, p. 43, podemos afirmar que os novos desafios implicam uma "monstruosa tarefa de conciliação entre os mais sagrados corolários do Estado de Direito, designadamente, o respeito pelos direitos, liberdades e garantias e do seu regime de proteção".

15 SOUSA, Simão Mendes de, *Constitucionalismo Digital…* cit., p. 73.

II. UMA NOVA ERA: AS PLATAFORMAS DIGITAIS COMO ATORES ABSOLUTOS

O surgimento da Internet mudou o paradigma mundial. Estima-se que, em 2023, 63% da população mundial teve acesso à Internet[16]. Os desafios por ela colocados derivam do seu caráter "transnacional e descentralizado[17]". Assim, há uma contradição evidente entre aqueles que são os limites territoriais de jurisdição e a natureza iminentemente global da Internet[18]. Progressivamente, as plataformas digitais adquiriram uma dimensão inimaginável e ultrapassaram há muito tempo o caráter de armazenadoras de conteúdos. Aquando da sua criação, em 2004, jamais se imaginaria que o Facebook (atual "Grupo Meta") viria a ter o impacto que tem hoje. Ao nível das redes sociais, o mesmo se sucede com o Twitter ("X"[19]) ou, inclusive, com o Youtube e o Instagram[20]. As plataformas de *streaming*[21] e de *marketplace*[22] assumem uma enorme relevância no contexto de mercado, tendo revolucionado significativamente o nosso quotidiano.

Elas constituem a nova fonte de difusão de conteúdos, promovem serviços e procedem ao tratamento massivo de dados. Sabemos bem que, na era digital, os dados são o novo petróleo. Persiste, todavia, uma diferença relevantíssima, e que é referida por GIOVANNI DE GREGORIO. Ao passo que o petróleo[23] constitui um recurso natural de caráter limitado, o tratamento de dados é inesgotável, podendo o mesmo tratamento ser usado para múltiplas finalidades, bem como para estabelecer diferentes padrões[24]. Como denota EDOARDO CELESTE, "as multinacionais tecnológicas controlam as tecnologias digitais, e ao fazê-lo, definem inevitavelmente o nosso eu digital[25]". As informações que, consciente ou inconscientemente, divulgamos nas diversas plataformas são canalizadas para

16 Consultado em https://ourworldindata.org/internet (17.03.2025)
17 SILVA, Nuno Sousa e, "Internet e Direitos Fundamentais…" cit., p. 211.
18 POLLICINO, Oreste, *Judicial Protection of Fundamental Rights on the Internet – A road towards Digital Constitutionalism?* Oxford, Hart Publishing, 2021, p. 176.
19 O Twitter foi adquirido por Elon Musk em julho de 2023. Posteriormente à aquisição, a rede social mudou o seu nome para "X".
20 O Instagram pertence ao Grupo Meta.
21 Netflix, HBO Max, Hulu, Amazon Prime Video ou a Disney, por exemplo.
22 A Amazon é o exemplo mais paradigmático.
23 Como denota Cordeiro, CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019*, Reimpressão, Almedina, 2020, p. 29, "os dados irão representar na Era Digital um papel análogo ao desempenhado pelo petróleo e demais combustíveis fósseis a partir da Revolução Industrial".
24 GREGORIO, Giovanni, de, *Digital Constitutionalism in Europe*… cit., pp. 225-226.
25 CELESTE, Edoardo, *Digital Constitutionalism – the role of internet bill of rights, Routledge*, New York, 2023, p. 12.

tratamentos massivos de dados, permitindo-se obter, mediante a definição de perfis, informações detalhadas sobre os seus utilizadores.

Atualmente, estas plataformas são o novo fórum público, onde os indivíduos têm a oportunidade de difundir os seus pensamentos, bem como exercer os seus direitos e liberdades. Existiu, por isso, uma verdadeira emancipação face à esfera pública. Ao contrário dos atores públicos, torna-se muito mais complexo assegurar o pleno respeito pelas salvaguardas constitucionais, sobretudo estando em causa decisões relativas à organização das plataformas e à remoção de conteúdos online[26].

Perante os diversos desafios colocados nesta era digital, as plataformas digitais não podem ser encaradas como atores absolutos. No entanto, não podemos ignorar que estamos perante entidades privadas, cujos direitos legalmente reconhecidos não podem, sem mais, ser ignorados.

III. A ATUAÇÃO DA UE NA ERA DIGITAL – REGULAÇÃO SEM FIM?

Nos últimos anos, a UE tem adotado uma atitude cautelosa e proativa no sentido de regular praticamente tudo o que diz respeito ao mundo digital. Um comentário recorrente sobre o atual cenário denota que os "EUA inovam, a China copia e a UE regula[27]".

De facto, os maiores desenvolvimentos tecnológicos têm ocorrido fora do espaço da UE, incrementando-se a tensão entre as plataformas digitais, sendo que a maioria tem sede nos EUA, e aquele que é o escopo normativo vigente na União. Relembremos, a título de exemplo, a afirmação do anterior Comissário Europeu para o Mercado Interno, Thierry Breton, tendo este afirmado que o Twitter (atual "X") deveria obedecer às regras consagradas na UE ("o pássaro irá obedecer às regras da UE[28]").

Mais recentemente, o Presidente norte-americano, Donald Trump, acusou a UE de regular em demasia e criticou o Pacote dos Serviços Digitais, realçando que a intenção dos EUA passaria por proteger as grandes tecnológicas norte-americanas[29].

---

26 POLLICINO, Oreste / BASSINI, Marco / GREGORIO, Giovanni de, *Internet Law and Protection of Fundamental Rights…* cit., p. 13.

27 Tradução da expressão ("The United States invents, China imitate and Europe regulates") https://medium.com/enrique-dans/the-united-states-invents-china-imitates-and-europe-regulates-e465ff293d82 (20.03.2025)

28 Tweet disponível em https://x.com/thierrybreton/status/1585902196864045056

29"Trump fires back at EU tech regulation", Le Monde, https://www.lemonde.fr/en/economy/article/2025/03/09/trump-fires-back-at-eu-tech-regulation_6738972_19.html (20.03.2025)

Os últimos anos caracterizaram-se por um incremento substancial regulativo da UE, o que demonstra o objetivo de garantir que não se passa um cheque em branco às grandes tecnológicas, asseverando a proteção dos direitos fundamentais dos cidadãos. Ainda assim, não se pode olvidar a necessidade de garantir que a regulação não é um entrave à inovação. Numa era em que as fronteiras digitais se encontram cada vez mais diluídas, antevê-se o crescimento da tensão entre as principais plataformas digitais e o regime de proteção previsto na UE. Salientemos, a título de exemplo, alguns dos principais marcos legislativos a este respeito:

i. Regulamento (UE) n.º 679/2016, de 27 de abril relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais[30] e à livre circulação desses dados e que revoga a Diretiva 95/46/CE[31]. Em bom rigor, não podemos advogar que o direito da proteção de dados tenha surgido com o RGPD[32]. O que se sucede, e como evidencia A. BARRETO MENEZES CORDEIRO é que foi com o RGPD que se deu uma verdadeira revolução, não só por se tratar de um regulamento, o que implica a sua imediata aplicação a todos os cidadãos da UE sem necessidade de transposição[33], como pelo seu conteúdo inovador[34].

30 Este é o exemplo paradigmático. Ainda assim, importa salientar que a legislação da UE, ao nível da privacidade e da proteção de dados, é bastante diversa. Saliente-se, a título de exemplo, 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, o 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, 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.

31 Regulamento (UE) n.º 679/2016, de 27 de abril 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.

32 Portugal procedeu à sua execução pela Lei n.º 58/2019, de 8 de agosto, a qual procedeu à revogação da Lei n.º 67/98, de 26 de outubro. Saliente-se que a versão final do diploma não se encontra isenta de críticas, devido às contradições expressas com o disposto no RGPD. A CNPD, na qualidade de autoridade de controlo, alertou o legislador português para este facto. Fê-lo durante o processo legislativo, através do Parecer n.º 20/2018. Como subsistiram várias incongruências, a CNPD, através da Deliberação 2019/494, declarou desaplicar, em ordem a assegurar o princípio do primado e a efetividade do RGPD, as seguintes normas: n.os 1 e 2 do art. 2.º, n.º 1 do art. 20.º, art. 23.º, al. a) do n.º 3 do art. 28.º, al. a), h) e k) do n.º 1 do art. 37.º, n.º 2 do art. 37.º, al. b) do n.º 1 do art. 38.º, n.º 2 do art. 38.º, n.os 1 e 3 do art. 39.º, n.º 2 do art. 61.º, n.º 2 e n.º 2 do art. 62.º Sobre o tema na doutrina *vide* CORDEIRO, A. Barreto Menezes - "A Interpretação dos Regulamentos Europeus das correspondentes leis de execução: o caso paradigmático do RGPD e da Lei n.º 58/2019", *Revista de Direito e Tecnologia,* Volume 1, N.º 2, 2019, pp. 175-200(194-195) e, igualmente, CALVÃO, Filipa Urbano - "A Lei n.º 58/2019, de 8 de agosto: incongruências e insuficiências na execução do RGPD", *Revista de Direito Administrativo,* Ano III, n.º 8, 2020, pp. 45-53.

33 Contrariamente às Diretivas.

34 Desde logo, e como salienta o autor, o RGPD permitiu a densificação dos direitos dos titulares dos dados, o agravamento dos deveres dos responsáveis pelo tratamento, o reforço das competências das autoridades

ii. Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724, mais conhecido por Regulamento Governação de Dados[35] (*Data Governance Act*). Este estabelece as condições para a reutilização na União de determinadas categorias de dados detidas por organismos públicos, um regime de notificação e supervisão para a prestação de serviços de intermediação de dados, um registo voluntário das entidades que recolhem e tratam dados disponibilizados para fins altruístas e um regime para a criação de um Comité Europeu da Inovação de Dados[36].

iii. Regulamento (UE) 2024/1689 que estabelece regras harmonizadas em matéria de Inteligência Artificial[37]. O Regulamento IA constitui o primeiro instrumento normativo de regulamentação geral e uniforme para a IA, o que por si só já é um marco histórico na luta pela maior humanização do processo, tendo sido alvo de sucessivas propostas e alterações. Este visa alcançar um elevado nível de proteção dos diversos direitos fundamentais, dimensão que se afigura essencial para a proteção dos cidadãos, incluindo a democracia e o Estado de Direito[38].

iv. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022, também conhecido por Regulamento dos Serviços Digitais ("Digital Services Act"). Como sabemos, a participação dos utilizadores deixou de ser meramente passiva, sendo que estes passaram a assumir cada vez mais o papel de criadores dos conteúdos[39]. Esta realidade fomentou a disseminação de conteúdos ilegais[40] justificando-se, desse modo,

---

de controlo e a obrigatoriedade de designação do encarregado de proteção de dados. *Vide* CORDEIRO, A. Barreto Menezes, *Direito da*… cit., p. 29.

35 Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724, mais conhecido por Regulamento Governação de Dados.

36 Alíneas a), b), c) e d) do artigo 1.º do Regulamento (UE) 20227868. Para uma análise especial desta temática, remetemos para MONIZ, Graça Canto, *A Estratégia da UE para os Dados - Que Contributos para a Regulação dos Dados?,* Coimbra, Almedina, 2024.

37 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.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial).

38 Artigo 1º, n.º 1, do Regulamento IA.

39 LEITÃO, Luís Menezes, *Digital Services Act* (DSA) – O Regulamento Europeu 2022/2065 sobre os serviços digitais, Coimbra, Almedina, 2023, p.10.

40 A regulação estava, assim, e como evidencia SILVA, Nuno Sousa e, "Novas regras para a internet: notas breves sobre iniciativas europeias de regulação de plataformas digitais", *Revista de Direito Intelectual*, n.º

o estabelecimento de regras harmonizadas para um ambiente em linha seguro. Tal como afirma DOMINGOS SOARES FARINHO, "as plataformas em linha são os guardiões de muitas das características essenciais da vida quotidiana[41]".

v. Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho de 14 de setembro de 2022 relativo à disputabilidade e equidade dos mercados no setor digital. À semelhança do Regulamento dos Serviços Digitais, este também integra o Pacote dos Serviços Digitais. O Regulamento dos Mercados Digitais visa assegurar uma concorrência leal nas diversas plataformas digitais, tendo como missão assegurar o bom funcionamento do mercado interno mediante a previsão de regras harmonizadas que assegurem para todas as empresas a disputabilidade e equidade dos mercados no setor digital.

A UE tem realizado, assim, um esforço no sentido de não criar um vácuo no espaço digital, pretendendo salvaguardar a proteção dos direitos fundamentais dos cidadãos. Doravante, cumprirá ajuizar se a proatividade da UE não poderá ser um entrave à inovação e se, efetivamente, constitui um mecanismo adequado para o ambiente digital.

IV. OS DIREITOS FUNDAMENTAIS NA ERA DIGITAL

Analisaremos o impacto que os diversos direitos fundamentais apresentam no atual contexto. Atualmente, "os direitos fundamentais para o universo digital estão ainda numa fase embrionária da sua formação", como afirma JORGE PEREIRA DA SILVA[42]. Importa, antes de analisarmos a sua adequação ao contexto digital, compreender as sucessivas gerações de direitos fundamentais, sendo possível identificar quatro distintas. Desde logo, na 1.ª geração (período liberal) os direitos fundamentais eram perspetivados como liberdades individuais e direitos de defesa dos indivíduos. Fundamenta-se, assim, no contexto das revoluções liberais[43], pretendendo-se impor ao Estado um dever de abstenção na restrição destes direitos inalienáveis. Falamos, a título de exemplo, do direito à vida e do direito à propriedade privada. A ideia de um Estado mínimo surge com

1, 2021, pp. 75-102(79) a "regulação estava pensada para a web 1.0 (cujo paradigma era de consumo passivo de conteúdo por parte dos internautas) e não para a web 2.0 (de cariz participativo)".

41 FARINHO, Domingos Soares, "Fundamental rights and conflict resolution in the Digital Services Act Proposal: a first approach", *e-Publica*, Volume 9, n.º 1, 2022, pp. 76-103(78).

42 SILVA, Jorge Pereira da – *Direitos Fundamentais para o Universo Digital,* Lisboa, Fundação Francisco Manuel dos Santos, 2024, p. 21.

43 Saliente-se como exemplo paradigmático a Revolução Francesa de 1789 e a Revolução Liberal Portuguesa de 1820.

o fim Antigo Regime[44], visando-se quebrar abruptamente com os ditames da época anterior. Deste modo, liberdade, segurança e propriedade foram os motes da construção da sociedade durante este período, afirmando-se como defesa inalienável dos indivíduos face ao poder estatal[45].

Por sua vez, a 2.ª geração caracterizou-se pelo alargamento dos direitos políticos, pretendendo-se promover uma democracia participativa. Estão em causa direitos positivos, implicando desta feita uma atitude positiva do Estado, assegurando-se a superação das discriminações vigentes. No seguimento do movimento sufragista, acentuou-se a necessidade de serem reforçados e defendidos os diversos direitos políticos. Mencionemos, por exemplo, o direito ao voto, a liberdade de associação e religiosa e o direito à igualdade. Como denota VIEIRA DE ANDRADE, os direitos fundamentais deixam de assumir uma vertente exclusivamente subjetiva, para passar a ser reconhecida igualmente uma dimensão objetiva. Podemos, por isso, afirmar que "a democracia torna-se, neste contexto, numa *condição* e numa *garantia* dos direitos fundamentais e, em geral, da própria liberdade do homem[46]".

Adicionalmente, após a grande depressão da década de 30, acentuaram-se as desigualdades sociais e económicas. A visão liberal, patente na primeira geração de direitos fundamentais, revelou-se insuficiente. Assim, a visão do Estado abstencionista fracassou durante a grave crise socioeconómica. Os direitos fundamentais passam, assim, a assumir uma visão coletivista, exigindo-se ao Estado prestações sociais aos seus cidadãos. Ganha-se a consciência de que uma atitude abstencionista não é suficiente, reclamando-se a atribuição de prestações positivas a favor dos cidadãos. Surge, assim, uma nova categoria de direitos, denominada por "direito a prestações[47]", os quais configuravam direitos concretizáveis através do Estado. Consequentemente, cria-se a ideia de "Estado Social", que perdura até aos nossos dias.

Finalmente, fala-se na doutrina de uma quarta geração de direitos fundamentais, a qual visará dar resposta aos desafios colocados atualmente, acompanhando igualmente a

44 Cfr. sobre o tema, *vide* SILVA, Nuno Sousa e, "Novas regras…" cit., pp. 206-208, ANDRADE, José Vieira de, *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, Almedina, 6.ª edição, 2019, pp. 51-70, VAZ, Afonso et. al., *Direito Constitucional: o sistema constitucional português*, 1.ª Edição, Porto, 2015, Universidade Católica Editora, pp. 207 e ss., MIRANDA, Jorge, *Manual de Direito Constitucional* Volume II, Tomo IV, Coimbra, Coimbra Editora, 2014, pp. 32 e ss e SILVA, Jorge Pereira da, *Direitos Fundamentais para o Universo Digital…* cit., pp. 33 e ss.

45 Como relembra ANDRADE, José Vieira de, *Os Direitos Fundamentais na Constituição*… cit., p. 51.

46 *Ibidem*, p. 54. As palavras assinaladas a itálico foram assim colocadas pelo autor.

47 ANDRADE, José Vieira de, *Os Direitos Fundamentais na Constituição*… cit., p. 56.

evolução do conceito de Estado[48]. Falamos, especificamente, no desenvolvimento do direito o ambiente[49] ou do direito dos consumidores[50], ambos com consagração constitucional. Fala-se, a este propósito, da seguinte trilogia: segurança, diversidade e solidariedade[51].

Nos últimos anos, foi amplamente debatida a Carta Portuguesa dos Direitos Humanos na Era Digital[52], visando-se salvaguardar que a "República Portuguesa participa no processo mundial de transformação da Internet num instrumento de conquista de liberdade, igualdade e justiça social e num espaço de promoção, proteção e livre exercício dos direitos humanos, com vista a uma inclusão social em ambiente digital[53]".

Nesta nova era digital, somos confrontados com uma questão relevante: o que fazer aos direitos que, embora não formalmente consagrados, apresentem uma enorme relevância para a devida proteção dos cidadãos no espaço digital? Sabemos que o artigo 16.º prevê uma cláusula aberta de direitos fundamentais, de acordo com o qual "os direitos fundamentais consagrados na Constituição não excluem outros constantes das leis e das regras aplicáveis de direito internacional[54]". Assim, o catálogo da CRP não pode ser percecionado como exaustivo, podendo ser encontrados direitos provenientes de fontes distintas, "na perspetiva mais ampla da Constituição material[55]".

Importa, por isso, definir qual é o critério material usado para este efeito. Apontamos o critério tríplice, na linha do que é defendido por VIEIRA DE ANDRADE[56], sendo necessária a verificação de três requisitos:

(i) Terá de ser identificado um radical subjetivo, isto é, estarão em causa direitos que atribuem aos indivíduos posições jurídicas subjetivas consideradas fundamentais;

(ii) Em segundo lugar, a função será a proteção e a garantia constitucional de determinados bens jurídicos;

48 SILVA, Nuno Sousa e – "Novas regras…" cit., p. 208.
49 *Vide* artigo 66.º da CRP.
50 Artigo 60.º da CRP.
51 ANDRADE, José Vieira de, *Os Direitos Fundamentais*… cit., p. 61.
52 Aprovado pela Lei n.º 27/2021, de 17 de maio.
53 Artigo 2.º, n.º 1, da Carta Portuguesa dos Direitos Humanos na Era Digital.
54 Artigo 16.º da CRP.
55 MIRANDA, Jorge, *Manual de Direito Constitucional*… cit., p. 195.
56 ANDRADE, José Carlos Vieira, *Os Direitos Fundamentais*… cit., p. 77.

(iii) Por último, estarão em causa direitos cuja intenção específica é a de "explicitar o que não pode de deixar de pertencer ao ser humano[57]" e cuja manifestação jurídica radica no princípio da dignidade da pessoa humana[58].

4.1. O Direito à Autodeterminação Informativa

Portugal foi pioneiro na consagração do *direito à autodeterminação informativa*. Nos termos do artigo 35.º, n.º 1, da CRP[59], "todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei[60]". Para GOMES CANOTILHO e VITAL MOREIRA, consagra-se a proteção efetiva para os cidadãos perante "o tratamento de dados pessoais informatizados[61]", advogando que este direito radica de alguns "direitos-mãe[62]" em sede de direitos, liberdades e garantias.

Por sua vez, CATARINA DOS SANTOS BOTELHO postula que se visa "impedir a instrumentalização da pessoa e mero objeto de informações[63]", garantindo-se a necessária adaptação aos desafios colocados nesta nova era digital. Embora numa fase embrionária, o direito em causa denota uma intenção clara e evidente do legislador constituinte em dar a abertura suficiente à CRP para permitir a tutela dos cidadãos no espaço digital. Considerando o seu conteúdo, o direito à autodeterminação informativa pressupõe o exercício de faculdades distintas, mormente: (i) o direito de acesso aos dados informatizados que lhe digam respeito, podendo exigir a sua retificação e atualização[64], (ii) a remissão para a definição legal das condições aplicáveis ao tratamento automatizado, conexão, transmissão e utilização, garantindo a proteção através de uma entidade administrativa independente[65], (iii) a proibição do acesso de dados a terceiros[66],

57 VAZ, Manual Afonso et. al., *Direito Constitucional…* cit., p. 213.
58 Defendendo esta posição, *vide* ANDRADE, José Carlos Vieira, *Os Direitos Fundamentais…* cit., pp. 76-78 e VAZ, Manual Afonso et. al., *Direito Constitucional…* cit., p. 213. Sobre a clausula aberta, *vide* MIRANDA, Jorge / MEDEIROS, Rui, *Constituição Portuguesa Anotada – Volume I*, 2.ª Edição Revista e atualizada, Lisboa, Universidade Católica Editora, 2017, pp. 21-222.
59 Tema que já tivemos a oportunidade de desenvolver no âmbito do nosso estudo sobre o direito ao esquecimento. *Vide* CAMÕES, Diana, "O direito ao esquecimento: uma realidade inevitável do novo (mundo) digital, *Revista Jurídico Luso-Brasileira*, Ano 9, n.º 4, 2023, pp. 503-534.
60 Artigo 35.º, n.º 1, da CRP.
61 CANOTILHO, Gomes / MOREIRA, Vital, *Constituição da República Portuguesa Anotada – Artigos 1.º a 107.º*, Coimbra, Coimbra Editora, 2007, p. 550.
62 *Ibidem*, p. 551.
63 BOTELHO, Catarina dos Santos, "Novo ou Velho Direito? – O Direito ao Esquecimento e o Princípio da Proporcionalidade no Constitucionalismo Global", *Revista do Instituto do Conhecimento AB*, Ano V, n.º 7, 2017, pp. 50-71(53-54).
64 Artigo 35.º, n.º 1, da CRP.
65 Sabemos que em Portugal é a CNPD. Artigo 35.º, n.º 2, da CRP.
66 Salvo nos casos expressamente previstos na lei. Artigo 35.º, n.º 4, da CRP.

(iv) a proibição de atribuição de número nacional único aos cidadãos[67], (v) a garantia do livre acesso às redes informáticas de uso público[68] e (vi) a consagração da proteção idêntica aos dados constantes de ficheiros manuais[69].

O legislador constituinte deu um passo à frente daquilo que seria expectável, demonstrando uma preocupação clara em conferir aos cidadãos uma tutela da utilização da informática[70], algo que ainda é mais assinalável, considerando que a *norma normarum* foi aprovada em 1976, muito antes do advento da vaga tecnológica que atualmente conhecemos[71].

4.2. Liberdade de expressão

O direito à liberdade de expressão é uma das pedras basilares do sistema democrático. Pressupõe-se, num contexto verdadeiramente livre, que cada cidadão tenha a possibilidade de se exprimir livremente, sem receio de represálias ou consequências. A era digital veio introduzir novas características na difusão da informação. Se, durante o século XX, os meios de comunicação social (jornais e televisões, por exemplo) eram essenciais para a difusão dos conteúdos, nos nossos dias, praticamente tudo passa pelas plataformas digitais (em particular, as redes sociais). Em 2009, JACK M. BALKIN alertou que os maiores desafios à liberdade de expressão não seriam colocados pelo direito constitucional, mas sim pela política do conhecimento, informação e dos modelos de negócio digitais[72]. Deste modo, esta nova era "fornece um elemento de (pelo menos, aparente) democraticidade e de confusão entre consumo e produção da informação[73]".

Os consumidores passaram a ser, simultaneamente, produtores de conteúdo e recetores da informação. Sabemos, do mesmo modo, que estas plataformas têm sido usadas para efeitos de campanha política. O espaço digital esbateu fronteiras e democratizou o acesso à informação e, em algumas circunstâncias, contribuiu para a disseminação da desinformação. Inversamente, as plataformas digitais adquiriram, nos últimos anos, o papel de tribunais digitais: estas, considerando a política dos termos e condições, decidem

67 Artigo 35.º, n.º 5, da CRP.
68 Artigo 35.º, n. º 6, da CRP.
69 Artigo 35.º, n.º 7, da CRP.
70 A este propósito, PINHEIRO, Alexandre Sousa, *Privacy e Proteção de Dados Pessoais: a Constituição dogmática do direito à identidade informacional,* Lisboa, AAFDL, 2015, p. 777.
71 O artigo foi alvo de três alterações em três revisões constitucionais (Lei Constitucional n.º 1/82, Lei Constitucional n.º 1/89 e Lei Constitucional n.º 1/97).
72 BALKIN, Jack M., "The Future of Freedom of Expression in a Digital Age", *Pepperdine Law Review*, Volume 36, Issue 2, pp. 427-444(427-428).
73 BRAVO, Jorge dos Reis, "Liberdade de Expressão na Era Digital: A reconfiguração de um Direito Humano?", *R. EMERJ,* volume 23, n.º 1, 2021, pp. 81-95(83).

aquilo que pode, ou não, ser considerado admissível para publicação. Em determinados casos, as plataformas são o "lápis azul" do quotidiano, removendo arbitrariamente conteúdos que não respeitam os seus termos e condições.

Usando a sistematização proposta por JORGE PEREIRA DA SILVA, podemos identificar duas situações de controlo de conteúdos[74]: (i) o controlo suave, no qual se determina a prioridade na publicação e (ii) o controlo duro, decidindo-se o que pode, ou não, ser publicado, com a consequência de bloqueio ou remoção[75].

Esta última forma de controlo é a mais preocupante. Considerando a evolução mais recente, as plataformas utilizam sistemas automatizados para efeitos de moderação de conteúdos, o que apresenta determinados riscos. Em primeira linha, poderemos ter "falsos positivo[76]", isto é, conteúdos que sejam erradamente considerados ilegais pelo algoritmo. Adicionalmente, haverá sempre a possibilidade de serem promovidas práticas discriminatórias, ou seja, conteúdos produzidos por determinadas minorias terem maior probabilidade de ser objeto de uma decisão de remoção do conteúdo.

O Regulamento dos Serviços Digitais introduziu disposições importantes a este respeito, visando-se garantir que não há um cheque em branco para as grandes plataformas, enquanto se reage contra a disseminação de conteúdos ilegais[77]. Uma das preocupações residiu, precisamente, na moderação de conteúdos[78].

---

74 SILVA, Jorge Pereira da, *Direitos Fundamentais para o Universo Digital*… cit., p. 119.

75 *Ibidem*, p. 119.

76 GREGORIO, Giovanni de / DUNN, PIETRO, "Profiling under Risk-based Regulation: Bringing together the GDPR and the DSA", *Web Summit*, 2021, https://assets.ctfassets.net/iapmw8ie3ije/5EuxLPaUIsgGt7R6PgeuFK/c9269e55e10bb2a7a0b392624c08f4d0/De_Gregorio_Dunn_My_Data_is_Mine__1_.pdf (16.03.2025), p. 8. Sobre o tema, *vide* GREGORIO, Giovanni de, *Digital Constitutionalism in Europe…* cit., pp. 157-215.

77 Os conteúdos ilegais correspondem, de acordo com o disposto no artigo 3.º, alínea h), do Regulamento dos Serviços Digitais, 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.

78 A moderação de conteúdos, nos termos do artigo 3.º, alínea t), do Regulamento dos Serviços Digitais, corresponde às "atividades, automatizadas ou não, empreendidas por prestadores de serviços intermediários, destinadas em especial a detetar, identificar e combater os conteúdos ilegais ou informações incompatíveis com os seus termos e condições fornecidos pelos destinatários do serviço, incluindo as medidas tomadas que afetam a disponibilidade, visibilidade e acessibilidade desses conteúdos ilegais ou dessas informações, como a despromoção, a desmonetização, a desativação do acesso ou a supressão dos mesmos, ou que afetem a capacidade de os destinatários do serviço fornecerem essas informações, como a cessação ou suspensão da conta de um destinatário". Como prescreve o Considerando 51 do Regulamento dos Serviços Digitais, "tendo em conta a necessidade de ter devidamente em conta os direitos fundamentais garantidos pela Carta de todas as partes interessadas, qualquer medida tomada por um prestador de serviços de alojamento virtual na sequência da receção de uma notificação deverá ser estritamente direcionada, no sentido de que deverá servir para suprimir ou bloquear o acesso a elementos específicos de informação considerados conteúdos ilegais, sem afetar indevidamente a liberdade de expressão e de informação dos destinatários do serviço".

O artigo 7.º do Regulamento dos Serviços Digitais introduziu a cláusula do bom samaritano ("*good samaritan clause"*[79]), nos termos da qual os prestadores dos serviços intermediários[80] não deverão ser considerados inelegíveis para beneficiar das isenções de responsabilidade apenas por realizarem, de boa-fé e de forma diligente, investigações voluntárias por iniciativa própria ou por tomarem outras medidas destinadas a detetar, identificar e suprimir ou bloquear o acesso a conteúdos ilegais.

Não obstante, recairá sobre os prestadores de serviços intermediários uma obrigação de reação contra os conteúdos ilegais, devendo os utilizadores das suas plataformas ser devidamente informados sobre como se opera a decisão da moderação de conteúdos.

Desde logo, os seus termos e condições deverão incluir as informações necessárias quanto às políticas, procedimentos, medidas e instrumentos utilizados para efeitos de moderação de conteúdos, incluindo a tomada de decisões algorítmicas e a análise humana, bem como as regras processuais do respetivo sistema interno de gestão de reclamações[81]. O dever de informação assume uma grande relevância no contexto digital, assegurando que os utilizadores têm a oportunidade de conhecer como é que é efetuada a atividade de moderação de conteúdos.

O Regulamento dos Serviços Digitais exige às plataformas em linha e aos motores de pesquisa em linha de muito grande dimensão[82] a realização de uma avaliação de riscos sistémicos na UE decorrentes da conceção ou do funcionamento do serviço, incluindo os sistemas algorítmicos. Tal avaliação deverá incidir sobre a difusão de conteúdos ilegais[83] e os efeitos negativos reais ou previsíveis no exercício dos direitos fundamentais, em particular os direitos fundamentais relativos à dignidade do ser humano, entre outros[84].

Ainda no que respeita a esta matéria, os prestadores de serviços intermediários deverão disponibilizar ao público, num formato legível por máquina e de forma facilmente acessível, pelo menos uma vez por ano, relatórios claros, facilmente compreensíveis sobre qualquer atividade de moderação de conteúdos em que tenham participado durante o

---

79 Detalhadamente sobre este tema, *cfr.* CASTRO, Raquel Brízida Castro, *Direito Constitucional…* cit., pp. 235 e ss e REXHEPI, Rrita, "Content Moderation: How the EU and the U.S. Approach Striking a Balance between Protecting Free Speech and Protecting Public Interest", *Trento Student Law Review,* Volume 5, n.º 1, 2023, pp. 69-98.

80 São considerados os seguintes prestadores de serviços intermediários: simples transporte, armazenagem temporária e o alojamento virtual.

81 Artigo 14.º, n.º 1, do Regulamento dos Serviços Digitais.

82 Importa recordar o que devemos entender por plataformas em linha e motores de pesquisa em linha de muito grande dimensão.

83 Artigo 34.º, n.º 1, alínea a), do Regulamento dos Serviços Digitais.

84 Artigo 34.º, n.º 1, alínea b), do Regulamento dos Serviços Digitais.

período pertinente[85]. No caso das plataformas em linha e dos motores de pesquisa em linha de muito grande dimensão, deverá existir o cuidado de se promover a atenuação de riscos, adaptando-se os respetivos processos de moderação de conteúdos e, sendo caso disso, a rápida supressão dos conteúdos notificados ou a rápida desativação do seu acesso[86].

Existiu uma preocupação do legislador no sentido de abordar a problemática da moderação de conteúdos. Ainda assim, não podemos deixar de evidenciar que para as plataformas em linha o seu cumprimento poderá não ser fácil, considerando ainda para mais que os Estados-Membros poderão apresentar disposições adicionais sobre esta matéria[87]. Por conseguinte, poderemos correr o risco de apelar às plataformas para integrarem no seu funcionamento mecanismos de censura, tornando-as "guardiãs do conteúdo online e da informação[88]", o que poderá não ser de todo desejável.

A Liberdade de Expressão, direito fundamental essencial para a vitalidade do sistema democrático, não deve ser ignorada. Isso não quer dizer que, em seu nome, se possa dizer absolutamente tudo. Como sabemos, e na linha do que já nos ensinou a melhor doutrina, nem todas as faculdades correspondem ao exercício típico do direito. O insulto ou a injúria não integram o núcleo essencial da liberdade de expressão. A UE tem revelado uma preocupação em mitigar a disseminação do conteúdo ilegal. Espera-se, doravante, que tal não resulte numa maior desproteção dos cidadãos na era digital[89].

4.3. Direito à proteção de dados pessoais

O Direito à proteção de dados pessoais está consagrado no artigo 8.º da CDFUE, prescrevendo-se que "todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito[90]". A invocação deste direito tem sido feita, na maioria dos casos, conjuntamente com o direito à reserva sobre a intimidade da vida privada (artigo 7.º da CDFUE[91]).

---

85 Artigo 15.º, n.º 1, do Regulamento dos Serviços Digitais.
86 Artigo 35.º, n.º 1, alínea c), do Regulamento dos Serviços Digitais.
87 ATTORI, Marcella, "The Digital Services Act and the Freedom of Expression in the European Union: A Political Perspective", SSRN, 2024, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4887181 (17.03.2025).
88 *Ibidem*, p. 9.
89 Será relevante mencionar que, do ponto de vista multinível, a CDFUE consagra no seu catálogo a Liberdade de expressão e informação (artigo 11.º). O mesmo se sucede com a CEDH (artigo 10.º).
90 Artigo 8.º, n.º 1, da CDFUE.
91 A inclusão desses direitos no catálogo de direitos fundamentais não significa que eles atribuam uma proteção ilimitada. *Vide,* a este propósito, RÜCKER, Daniel / KUGLER, Tobias, *New European General Data Protection Regulation*, Hart, Oxford, 2018, p. 5.

A proteção conferida por este direito refere-se, claro está, aos dados pessoais, isto é, às informações relativas a uma pessoa singular identificada ou identificável[92]. Não se encontram aqui incluídos os dados não pessoais[93]. Relativamente a esta última categoria, "a perspetiva já não será de proteção, mas sim de maximização da respetiva utilidade[94]".

A primeira grande decisão em matéria de proteção de dados foi proferida pelo Tribunal Constitucional Alemão, em 1983, no célebre caso *Volkszählungsurteil* (Caso do censo demográfico), onde se reconheceu e garantiu proteção contra a recolha, armazenamento, uso e transmissão ilimitados de dados pessoais. Trata-se, conforme postula ALEXANDRE SOUSA PINHEIRO, do "*leading case,* não só alemão, mas também internacional, no domínio da proteção de dados pessoais[95]".

Durante muitos anos, o direito à proteção de dados era encarado como uma decorrência do direito à privacidade[96]. Porém, o crescimento exponencial do tratamento de dados pessoais realçou a importância de se proceder à autonomização do direito. A. BARRETO MENEZES CORDEIRO considera que a produção legislativa realizada se justificou, sobretudo, pela necessidade de "regular o seu tratamento[97]", englobando duas áreas distintas: a proteção de dados pessoais e a segurança de dados pessoais. Os dados tornaram-se, assim, num recurso essencial para o crescimento económico, a criação de emprego e o progresso da sociedade, apresentando um valor inigualável na era da digitalização. Atualmente, e considerando a sua inserção no catálogo da CDFUE, o direito à proteção de dados encontra-se totalmente autonomizado do direito à privacidade[98]. Sendo os dados pessoais o novo petróleo, com um valor económico transversal, a sua autonomização faz todo o sentido. Vejamos.

O direito à privacidade apresenta um caráter muito mais amplo, referindo-se a todas as componentes da dignidade da pessoa humana. A privacidade compreende, assim, direitos e valores distintos, tais como a vida privada e familiar, a personalidade e a intimidade de

92 Artigo 4.º, n.º 1, do RGPD.
93 Os dados não pessoais referem-se, *a contrario*, aos dados que não dizem respeito a uma pessoa singular identificada ou identificável ou a dados inicialmente pessoais, mas posteriormente tornados anónimos e que não podem ser atribuídos de nenhuma forma a uma pessoa específica.
94 SILVA, Jorge Pereira da, *Direitos Fundamentais para o Universo Digital…* cit., p. 94.
95 PINHEIRO, Alexandre, *Privacy e Proteção de Dados Pessoais…* cit., p. 479.
96 CUSTERS, Bart / MALGIERI, Gianclaudio, "Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data", Computer Law & Security Review, 45, 2022, pp. 1-11(6). Como afirma FLAHERTY, David H., "On the utility of constitutional rights to privacy and data protection", *Case Western Reserve Law Review,* Volume 41, pp. 831-855(831) "a privacidade é como a Liberdade: não a reconhecemos a sua importância até que nos seja retirada".
97 CORDEIRO, A. Barreto Menezes, *Direito da*… cit., pp. 33-35.
98 TZANOU, Maria, "Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right", *International Data Privacy Law*, Volume 3, n.º 3, 2013, pp. 88-99(90).

casa indivíduo[99]. Determinadas violações do direito à privacidade não implicarão necessariamente uma violação do direito à proteção de dados pessoais[100]. Este último, com um caráter fundamental, incide precisamente sobre a natureza de proteção do tratamento de dados pessoais. Nem todas as violações do direito à privacidade acarretam a violação do direito à proteção dos dados pessoais. Na esteira de JORGE PEREIRA DA SILVA, podemos afirmar que "a proteção de dados tem uma função instrumental de tutela em relação a outros direitos para além da privacidade em sentido estrito[101]".

O legislador português optou na CPDHED por consagrar um "direito à privacidade em ambiente digital", o qual se subdivide em duas vertentes distintas: (i) o direito a comunicar eletronicamente usando a criptografia e outras formas de proteção da identidade ou que evitem a recolha de dados pessoais, designadamente para exercer liberdades civis e políticas sem censura ou discriminação[102] e (ii) o direito à proteção de dados pessoais, incluindo o controlo sobre a sua recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição, é assegurado nos termos legais[103].

4.3.1 O Direito ao esquecimento

O direito ao esquecimento tem sido, nos últimos anos, alvo de uma ampla querela doutrinal e jurisprudencial. Em Portugal, a CPDHED consagrou um direito ao esquecimento, de acordo com o qual "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[104]". Este poderá ser exercido a título póstumo "por qualquer herdeiro do titular do direito, salvo quando este tenha feito determinação em sentido contrário[105]".

99 *Ibidem*, p. 90.
100 Vide artigo 26.º da CRP.
101 SILVA, Jorge Pereira da, *Direitos Fundamentais para o Universo Digital…* cit., p. 95.
102 Artigo 8.º, n.º 1, da Lei n.º 27/2021, de 17 de maio.
103 Artigo 8.º, n.º 2, da Lei n.º 27/2021, de 17 de maio.
104 Artigo 13.º, n.º 1 da Lei n.º 27/2021, de 17 de maio.
105 Artigo 13.º, n.º 2 da Lei n.º 27/2021, de 17 de maio.

O TJ não analisou a existência de um direito ao esquecimento no caso *Google Spain c. Costeja González*[106] e no caso *Google c. CNIL*[107], mas sim sobre o alcance do direito à supressão de referências, mais concretamente a extraterritorialidade do RGPD.

O artigo 17.º do RGPD refere-se ao "direito ao apagamento dos dados («direito a ser esquecido»)", prescrevendo que o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais quando se aplique um dos seguintes motivos:

(i) os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento[108];

(ii) o titular retire o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9., n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento[109];

(iii) o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2[110];

(iv) 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[111];

(v) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1[112].

Em todos os processos, não se deve ignorar a necessidade de salvaguardar os diversos interesses e direitos dos prestadores dos serviços, algo que em determinadas circunstâncias parece ter sido esquecido. ORESTE POLLICINO e GRAZIELLA ROMEO consideram mesmo que o TJ, no caso *Google c. Costeja* González, protegeu em demasia o direito do titular dos dados, não fazendo a ponderação necessária com outros direitos em confronto (como, por exemplo, a liberdade de expressão[113]). No referido caso, o TJ

106 *Google Spain c. Agencia Española de Protección de Datos* (AEPD) e Costeja González, C-131/12, de 13 de maio de 2014.
107 *Google c. CNIL*, C-507/17, de 24 de setembro.
108 Artigo 17.º, n.º 1, alínea a), do RGPD.
109 Artigo 17.º, n.º 1, alínea b), do RGPD.
110 Artigo 17.º, n.º 1, alínea c), do RGPD.
111 Artigo 17.º, n.º 1, alínea d), do RGPD.
112 Artigo 17.º, n.º 1, alínea e), do RGPD.
113 POLLICINO, Oreste, ROMEO, Graziella, "Concluding remarks – Internet Law, protection of fundamental rights and the role of constitutional adjudication", in Oreste Pollicino, Graziella Romeo (Ed)

considerou que o tratamento de dados pessoais em causa, realizado pelo motor de busca, seria suscetível de afetar os direitos fundamentais pelo respeito à vida privada e à proteção de dados pessoais, já que referido tratamento permitiria a qualquer "internauta obter, com a lista de resultados, uma visão global estruturada das informações sobre essa pessoa, que se podem encontrar na Internet, respeitantes, potencialmente, a numerosos aspetos da sua vida privada[114]". O operador do motor de busca seria, assim, obrigado a suprimir da lista de resultados, exibida na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, as ligações a outras páginas web publicadas por terceiros e que contenham informações sobre essa pessoa também na hipótese de esse nome ou de essas informações não serem prévia ou simultaneamente apagadas dessas páginas web, mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita[115].

No caso *Google c. CNIL*, esteve em causa a problemática da eficácia extraterritorial do RGPD, relativamente a uma pessoa singular que apresentou um pedido de supressão da lista de resultados exibida após uma pesquisa do seu nome. O TJ seguiu uma tese intermédia, defendendo que a supressão deveria ocorrer apenas mediante a solicitação de endereços de IP e utilizadores dentro da UE[116].

De todo o modo, não estamos perante situações em que tenha sido consagrado o direito ao esquecimento. Do ponto de vista legal, devemos distinguir entre o direito ao apagamento *lato sensu* e o direito ao apagamento *stricto sensu*. A primeira situação incluirá, necessariamente, o direito ao apagamento e o direito ao esquecimento. Sobre esta matéria, o disposto no artigo 17.º, n.º 2, prescreve que sempre que o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los, deverá tomar as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.

The Internet and Constitutional Law – The Protection of fundamental rights and constitutional adjudication in Europe, Routledge, 2020, pp. 234-250(248).

114 *Google Spain c. Agencia Española de Protección de Datos* (AEPD) e Costeja González, C-131/12, de 13 de maio de 2014, parágrafo 80.

115 Sobre este caso, CALVÃO, Filipa, "A Proteção de Dados Pessoais na Internet: Desenvolvimentos Recentes", *Revista de Direito Intelectual,* n.º 2, 2015, pp. 67-84(78) advoga que "mesmo que se entenda haver aqui uma ligeira compressão do direito de acesso à informação, ainda assim ela estará justificada pela salvaguarda de outros direitos fundamentais e numa medida que se afigura adequada, necessária e não excessiva".

116 *Vide* VICENTE, Dário Moura, "Aplicação Extraterritorial do Direito ao Esquecimento na Internet?", *Revista da Ordem dos Advogados*, Volume 80, n.º 3-4, 2020, pp. 475-488(483).

A principal questão passa por aferir se o direito ao esquecimento é, efetivamente, um direito novo ou se, ao invés, resulta da conjugação de disposições distintas. Para CATARINA DOS SANTOS BOTELHO o direito ao esquecimento não é propriamente uma novidade do RGPD ou "um direito criado ex novum, pois este já se podia implicitamente retirar de uma leitura conjunta dos artigos 6.º e 12.º da Diretiva 95/46 /EC[117]". Há quem, por sua vez, defenda que estamos diante um direito novo[118].

Como vimos, a CPDHED consagrou no seu catálogo o direito ao esquecimento. Mesmo não existindo menção na CRP (o legislador constituinte não o previu), convém ter sempre presente a cláusula aberta dos direitos fundamentais. De qualquer modo, e considerando o conteúdo do RGPD, há abrangência normativa suficiente para suportar a existência do direito ao esquecimento.

V.O SURGIMENTO DE NOVOS DIREITOS

5.1 Direito à explicação

Tivemos a oportunidade de aprofundar alguns direitos que têm sido relevantes no contexto digital. Nos últimos anos, a propósito do RGPD, tem sido amplamente debatido a eventual existência de um direito à explicação, estando este debate longe de ser concluído. Tal apresenta uma especial relevância no âmbito das decisões automatizadas[119].

Na doutrina, BRYCE GOODMAN e SETH FLAXMAN foram os primeiros autores a defender a existência de um direito à explicação *ex post*. Baseiam a sua posição no considerando 71, o qual prevê que o tratamento deverá ser acompanhado das garantias adequadas, mormente o direito do titular dos dados a obter uma "explicação sobre a decisão tomada" na sequência da avaliação[120].

Por sua vez, há quem na doutrina refute, pura e simplesmente, a existência de um direito à explicação, destacando-se SANDRA WATCHER, BRENT MITTELSTADT E LUCIANO FLORIDI[121]. Na ótica dos autores, os direitos terão de estar expressamente consagrados na

117 BOTELHO, Catarina dos Santos, "Novo ou Velho Direito? – O Direito ao Esquecimento…" cit., p. 63.
118 É o caso de VICENTE, Dário Moura, Aplicação Extraterritorial do Direito ao Esquecimento na Internet?", *Revista da Ordem dos Advogados*, Volume 80, n.º 3-4, 2020, pp. 475-488(487).
119 Artigo 22.º do RGPD.
120 GOODMAN, Bryce / FLAXMAN, Seth, "European Union Regulations on Algorithmic Decision Making and a "Right to Explanation", *AI Magazine*, Volume 38, n.º 3, 2016, pp. 50-57.
121 WATCHER, Sandra / MITTELSTADT, Brent / FLORIDI, Luciano, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law*, Volume 7, 2, 2017, pp. 76–99.

lei antes da sua aplicação, o que não se sucede no presente caso. Adicionalmente, advogam que a existência de uma explicação, de acordo com os deveres de informação, ocorrerá antes da adoção de qualquer tipo de decisão automatizada e não após[122].

Finalmente, uma última posição defende que poderá retirar-se a existência do direito da leitura conjunta dos artigos 13º, nº 2, alínea f), e 14º, nº 2, alínea g), ao prever-se a possibilidade de o titular dos dados obter informações sobre a lógica envolvida nas decisões automatizadas. A este propósito, GRAÇA CANTO MONIZ defende que tal interpretação é uma consequência dos princípios da transparência e lealdade[123].

Embora no plano do RGPD continue a existir debate doutrinal, não deixa de ser curioso que o Regulamento IA tenha consagrado expressamente a existência de um direito à explicação. Note-se que é um dos únicos direitos subjetivos expressamente mencionados no diploma. Assim, no caso dos sistemas de IA de risco elevado, qualquer pessoa afetada, sujeita a uma decisão tomada pelo responsável pela implantação, e que produza efeitos jurídicos ou analogamente o afete num grau significativo, poderá "obter do responsável pela implantação explicações claras e pertinentes sobre o papel do sistema de IA no processo da tomada de decisão e sobre os principais elementos da decisão tomada[124]". Embora tal opção se encontre restrita aos sistemas de IA de risco elevado, não deixa de ser um passo assinalável do legislador.

Do ponto de vista do RGPD, o TJ teve a oportunidade de se pronunciar sobre a existência de um direito à explicação, na aceção do RGPD. Falamos do caso *CK c. Magistrat der Stadt Wien*[125]. *In casu,* o tribunal defendeu que, resulta do Considerando 71 do RGPD, quando o titular dos dados for objeto de uma decisão baseada exclusivamente no tratamento automatizado e que o afete de forma significativa, este deve ter o direito de obter uma explicação sobre essa decisão[126]. Deste modo, e para permitir ao titular dos dados exercer eficazmente os seus direitos ao abrigo do disposto no artigo 22.º, n.º 3, do RGPD, a explicação deverá ser fornecida através de informações pertinentes e de forma concisa, transparente, inteligível e de fácil acesso. Não poderá, assim, o responsável pelo tratamento fornecer uma simples comunicação de uma fórmula matemática complexa

122 *Ibidem*, pp. 80 e ss.
123 MONIZ, Graça Canto, Manual de Introdução à Proteção de Dados Pessoais, Coimbra, Almedina, 2023, p. 202.
124 Artigo 86.º do Regulamento IA. O direito à explicação não se aplicará à utilização de sistemas de IA para os quais as exceções ou restrições a essa obrigação decorram do direito da União ou do direito nacional em conformidade com o direito da União, sendo que o artigo 86.º somente será aplicável na medida em que não se encontre estipulado em sentido contrário no direito da União.
125 *CK c. Magistrat der Stadt Wien*, C-203/22, 27 de fevereiro de 2025.
126 *CK c. Magistrat der Stadt Wien*, C-203/22, 27 de fevereiro de 2025, parágrafo 57.

(através de um algoritmo), nem a descrição detalhada de todas as etapas das decisões automatizadas[127].

Esta decisão é um marco jurídico. Pela primeira vez, em sede de reenvio prejudicial, o TJ reconhece expressamente a existência de um direito à explicação no RGPD, o que permitirá reforçar a proteção do titular dos dados no contexto algorítmico. Não podemos antecipar o fim do debate doutrinal que se prolonga há vários anos. Ainda assim, nesta era digital, consideramos positivo que a jurisprudência dê os primeiros passos no sentido de reforçar os direitos dos titulares dos dados na era digital.

5.2 Direito de acesso à Internet

A internet faz parte do nosso quotidiano, pelo que praticamente todos os processos decisórios necessitam, em algum momento, da sua utilização. Surge a questão sobre se existirá um direito de acesso à Internet.

Uma vez mais, o legislador português procurou dar um passo em frente e consagrou explicitamente o "direito de acesso ao ambiente digital", o qual se traduz no livre acesso à Internet sem discriminação em razão do género, raça, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou orientação sexual[128]. São estabelecidas incumbências ao Estado, nomeadamente quanto à necessidade de se promover a redução e eliminação das assimetrias regionais e locais em matéria de conectividade[129] ou à execução de programas que garantam o acesso a instrumentos e meios tecnológicos por parte da população[130].

Na era digital, o acesso à Internet tornou-se essencial para todos os domínios da vida moderna. Vimos, particularmente, a sua relevância durante a pandemia. O ensino passou a ser realizado à distância e o teletrabalho tornou-se uma realidade. Assim, "as tecnologias representaram e ainda representam um desenvolvimento das liberdades[131]", pelo que a presença na rede "constitui hoje um instrumento essencial de integração social, de exercício das liberdades económicas, e de participação política dos cidadãos[132]".

---

127 *CK c. Magistrat der Stadt Wien*, C-203/22, 27 de fevereiro de 2025, parágrafos 58-59.
128 Artigo 3.º, n.º 1, da Lei n.º 27/2021, de 17 de maio.
129 Artigo 3.º, n.º 1, alínea d), da Lei n.º 27/2021, de 17 de maio.
130 Artigo 3.º, n.º 1, alínea g), da Lei n.º 27/2021, de 17 de maio.
131 FROSINI, Tommaso Edoardo, "Access to internet as a fundamental right", Italian Journal of Public Law,volume 5, n.º 2, 2013, pp. 226-234, https://heinonline.org/HOL/Page?handle=hein.journals/itajpul5&collection=journals&id=229&startid=&endid=237 (21.03.2025).
132 SILVA, Jorge Pereira da, *Direitos Fundamentais para o Universo Digital…* cit., p. 88.

Deste modo, o pleno exercício dos direitos e liberdades individuais passa pelo digital[133]. Tal fará com que, nos próximos anos, se reclame o acesso à Internet como direito inalienável dos cidadãos. Não implica, ainda assim, a sua consagração na *norma normarum,* considerando o princípio da cláusula aberta. Poderemos incluir a sua inserção numa 5.ª geração de direitos fundamentais. Uma coisa é certa: será impossível ignorar o impacto que a Internet continuará a ter no nosso dia a dia.

5.3 Direito à proteção das decisões algorítmicas

O constitucionalismo digital surge da necessidade de se adaptar os valores constitucionais aos desafios e necessidades da sociedade digital[134]. Assim, o maior desafio passa por criar um sistema capaz de salvaguardar os instrumentos normativos necessários aptos a permitir a evolução da IA, mas também capazes de defender os direitos fundamentais dos cidadãos e os valores democráticos. Há quem na doutrina, como é o caso de GIOVANNI DE GREGORIO, aponte que estamos a entrar numa nova fase de constitucionalismo digital: o fortalecimento dos direitos dos cidadãos[135]. Esta nova fase permitirá uma articulação sofisticada do constitucionalismo digital europeu, centrando as suas respostas nas novas ameaças à dignidade humana (algo também denominado por "humanismo digital"[136]).

Embora, após as revoluções liberais oitocentistas, as constituições tenham sido criadas com o objetivo de limitar o poder estatal e proteger os indivíduos do exercício de poder arbitrário por parte do Estado, a sociedade algorítmica mudou esse paradigma. Reclama-se, por agora, uma atuação positiva, que permita tutelar devidamente os direitos fundamentais dos cidadãos contra os poderes das plataformas. A este propósito, ORESTE POLLICINO e GIOVANNI DE GREGORIO denotam que o poder público já não é a única fonte

133 A defender a existência de um direito fundamental de acesso à Internet, *vide* ESTRADA, Mariana, "Revisiting access to internet as a fundamental right in times of COVID-19", *UNIO – EU Law Journal,* Volume 6, n.º 2, 2020, pp. 16-24.

134 *Vide* GREGORIO, Giovanni de "The rise of digital constitutionalism…", cit, p. 42 e ss., e CELESTE, Edoardo *Digital Constitutionalism – the role of internet bill of rights*… cit., p. 215.

135 GREGORIO, Giovanni de "The rise of digital constitutionalism…", cit, p. 67. O autor faz menção a fases distintas, tais como: (i) o liberalismo digital (caracterizado por uma abordagem liberal, onde cada sociedade digital seria capaz de participar na criação de novas regras para reger o mundo digital), (ii) o ativismo judicial (com a força vinculativa da CDFUE, e a expressa consagração do direito à proteção de dados pessoais, o TJ garantiu em diversas ocasiões a plena aplicação da carta com o objetivo de salvaguardar os direitos fundamentais dos cidadãos na era digital) e (iii) o constitucionalismo digital (com o reforço do poder das plataformas digitais, e para evitar que o seu poder se torne absoluto, o direito constitucional deixa de ser indiferente a estes desafios).

136 GREGORIO, Giovanni de, "The rise of digital constitutionalism…" cit, p. 67.

de preocupação relativamente à proteção dos direitos fundamentais e da democracia[137]. Encontrando-se as fronteiras jurisdicionais em constante mutação, urge repensar o enquadramento atual[138].

A existência de um direito à proteção das decisões algorítmicas, entendido num sentido mais amplo, poderá ser dividir-se em duas situações distintas: (i) o direito de fácil acesso ("*right to accessibility*"), através do qual se visaria garantir o direito de fácil acesso e interação com o algoritmo e (ii) o direito a uma tradução da linguagem tecnológica para linguagem humana, algo que implicaria o uso de linguagem clara e entendível da decisão algorítmica[139]. Este último implicaria a definição de um critério claro quanto ao nível de entendimento necessário. Sabemos que os sistemas de IA se caracterizam pela sua opacidade, pelo que teria de ser densificado qual o padrão de conhecimento a ser utilizado para este caso em concreto. De todo o modo, a consagração de um direito desta natureza daria aos afetados por decisões algorítmicas mais mecanismos ao seu dispor para reagir contra a sua adoção caso tenham sido cometidas ilegalidades durante o processo. O legislador constituinte não poderá, claro está, consagrar tudo na CRP, nem seria expectável que o fizesse. De todo o modo, pretendemos salientar que vivemos uma nova fase de constitucionalismo digital, esperando-se que se antecipem as dificuldades do futuro.

VI. NOTAS CONCLUSIVAS

Os desafios do futuro são tremendos. Nesta nova era digital, a maior dificuldade passará por criar as condições propícias à adequada proteção dos direitos fundamentais dos cidadãos. Conforme tivemos a oportunidade de realçar, as plataformas digitais atuam como atores privados e dispõem, no atual contexto, de poderes quase ilimitados. São elas quem moldam os conteúdos disponíveis online e contribuem, em determinadas situações, para a violação dos direitos fundamentais dos cidadãos. Nos últimos anos, a UE tem apostado fortemente na regulação, algo que, embora não vise eliminar por completo a inovação, pretende garantir uma harmonia entre os diversos interesses em confronto, no

137 Tal como já defendemos anteriormente em CAMÕES, Diana, *A Discriminação Algorítmica na Era do Constitucionalismo Digital*, Coimbra, Almedina, 2025, p. 244.

138 POLLICINO, Oreste / GREGORIO, Giovanni de, "Constitutional Law in the Algorithmic Society", in Hans-W. Micklitz et. al, (Ed.) *Constitutional Challenges in the Algorithmic Society*, Cambridge, Cambridge University Press, pp. 3-24.

139 Proposto na doutrina por POLLICINO, Oreste / GREGORIO, Giovanni de "Constitutional Law in the Algorithmic Society" cit., p. 21.

que concerne à proteção dos direitos fundamentais e ao bom funcionamento do mercado interno.

Neste sentido, e considerando aquela que foi a evolução jurídico-constitucional, conhecemos gerações distintas de direitos fundamentais. Estamos muito longe da conceção protetora com que foram equacionados após as revoluções liberais. Há direitos fundamentais que, pela sua natureza, continuam a ter um enorme impacto no contexto digital. Falamos, mais precisamente, na liberdade de expressão, pedra basilar do sistema democrático. Contrariamente ao que se sucedia há vários anos, os meios de comunicação tradicionais perderam o domínio do conteúdo que é divulgado, sendo que a maioria das informações passaram a ser divulgados pelos próprios utilizadores das plataformas. Assim, e com este novo fórum público, um dos pontos mais problemáticos reside precisamente no modo como será perspetivada e respeitada a liberdade de expressão na era digital. O mesmo se diga quanto ao direito à proteção de dados pessoais, o qual apresenta consagração expressa na CDFUE, e quanto ao direito ao esquecimento.

No contexto português, o catálogo existente de direitos fundamentais não estará, como sabemos, limitado ao que se encontra previsto na *norma normarum*, por força da cláusula aberta de direitos fundamentais. Tal abre portas, uma vez ponderada a respetiva materialidade, para que possamos ter direitos fundamentais fora da constituição, o que no contexto digital poderá ser relevante.

Doravante, poderemos vir a falar de uma 5.ª geração de direitos fundamentais, permitindo-se a devida adaptação aos desafios colocados durante a era digital. Mencionemos o direito de acesso à Internet, o direito à explicação ou o direito à proteção das decisões algorítmicas. Estes são apenas alguns dos exemplos que, começando a dar os primeiros passos, poderão englobar esta nova geração de direitos. Uma coisa é certa: a evolução tecnológica não tem fim à vista e a tutela efetiva dos direitos fundamentais terá de se adaptar à realidade do ciberespaço.

BIBLIOGRAFIA

ANDRADE, JOSÉ VIEIRA DE, *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, Almedina, 6.ª edição, 2019.

ATTORI, MARCELLA, "The Digital Services Act and the Freedom of Expression in the European Union: A Political Perspective", SSRN, 2024, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4887181 (17.03.2025).

BALKIN, JACK M., "The Future of Freedom of Expression in a Digital Age", *Pepperdine Law Review*, Volume 36, Issue 2, pp. 427-444.

BOTELHO, CATARINA SANTOS,

"Novo ou Velho Direito? – O Direito ao Esquecimento e o Princípio da Proporcionalidade no Constitucionalismo Global", *Revista do Instituto do Conhecimento AB*, Ano V, n.º 7, 2017, pp. 50-71.

"Direito da Concorrência e Proteção de Dados nos contextos português e europeu", in Sofia Pais / Vicente Bagnoli (Coord.) *Temas Atuais de Direito da Concorrência – Economia Digital, Direitos Fundamentais e outros desafios*, Universidade Católica Editora, Porto, 2020, pp. 91-115.

BRAVO, JORGE DOS REIS, "Liberdade de Expressão na Era Digital: A reconfiguração de um Direito Humano?", *R. EMERJ*, Volume 23, n.º 1, 2021, pp. 81-95.

CALVÃO, FILIPA URBANO, "A Lei n.º 58/2019, de 8 de agosto: incongruências e insuficiências na execução do RGPD", *Revista de Direito Administrativo,* Ano III, n.º 8, 2020, pp. 45-53.

CASTRO, RAQUEL BRÍZIDA, *Direito Constitucional: Ciberespaço e Tecnologia*, Coimbra, Almedina, 2023.

CAMÕES, DIANA,

"O direito ao esquecimento: uma realidade inevitável do novo (mundo) digital, *Revista Jurídico Luso-Brasileira*, Ano 9, n.º 4, 2023, pp. 503-534.

A Discriminação Algorítmica na Era do Constitucionalismo Digital, Coimbra, Almedina, 2025.

CANOTILHO, GOMES / MOREIRA, VITAL, *Constituição da República Portuguesa Anotada – Artigos 1.º a 107.º*, Coimbra, Coimbra Editora, 2007.

CELESTE, Edoardo, *Digital Constitutionalism – the role of internet bill of rights, Routledge*, New York, 2023.

CORDEIRO, A. BARRETO MENEZES CORDEIRO,

"A Interpretação dos Regulamentos Europeus das correspondentes leis de execução: o caso paradigmático do RGPD e da Lei n.º 58/2019", *Revista de Direito e Tecnologia,* Volume 1, N.º 2, 2019, pp. 175-200.

Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019, Reimpressão, Almedina, 2020.

CUSTERS, BART / MALGIERI, GIANCLAUDIO, "Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data", *Computer Law & Security Review*, 45, 2022, pp. 1-11.

ESTRADA, MARIANA, "Revisiting access to internet as a fundamental right in times of COVID-19", *UNIO – EU Law Journal,* Volume 6, n.º 2, 2020, pp. 16-24.

GOODMAN, BRYCE / FLAXMAN, SETH, "European Union Regulations on Algorithmic Decision Making and a "Right to Explanation", *AI Magazine*, Volume 38, n.º 3, 2016, pp. 50-57.

GREGORIO, GIOVANNI DE,

"The rise of digital constitutionalism in the European Union", *International Journal of Constitutional Law*, Volume 19, n.º 1, 2021, pp. 41-70.

Digital Constitutionalism in Europe – Reframing powers in the algorithmic society, Cambridge University Press, Cambridge, 2022.

GREGORIO, Giovanni de / DUNN, PIETRO, "Profiling under Risk-based Regulation: Bringing together the GDPR and the DSA", Web Summit, 2021, https://assets.ctfassets.net/iapmw8ie3ije/5EuxLPaUIsgGt7R6PgeuFK/c9269e55e10bb2a7a0b392624c08f4d0/De_Gregorio_Dunn_My_Data_is_Mine__1_.pdf (16.03.2025).

GREGORIO, GIOVANNI DE, RADU, ROXANA, "Digital constitutionalism in the new era of Internet governance", *International Journal of Law and Information Technology*, Volume 30, n.º 1, 2022, pp. 68-87.

FARINHO, DOMINGOS SOARES, "Fundamental rights and conflict resolution in the Digital Services Act Proposal: a first approach", *e-Publica*, Volume 9, n.º 1, 2022, pp. 76-103.

FLAHERTY, DAVID H., "On the utility of constitutional rights to privacy and data protection", *Case Western Reserve Law Review,* Volume 41, pp. 831-855.

FROSINI, TOMMASO EDOARDO, "Access to internet as a fundamental right", Italian Journal of Public Law,volume 5, n.º 2, 2013, pp. 226-234, https://heinonline.org/HOL/Page?handle=hein.journals/itajpul5&collection=journals&id=229&startid=&endid=237 (21.03.2025).

MIRANDA, JORGE, *Manual de Direito Constitucional* Volume II, Tomo IV, Coimbra, Coimbra Editora, 2014.

MIRANDA, JORGE / MEDEIROS, RUI, *Constituição Portuguesa Anotada – Volume I*, 2.ª Edição Revista e atualizada, Lisboa, Universidade Católica Editora, 2017.

MONIZ, GRAÇA CANTO,

Manual de Introdução à Proteção de Dados Pessoais, Coimbra, Almedina, 2023.

A Estratégia da UE para os Dados - Que Contributos para a Regulação dos Dados?, Coimbra, Almedina, 2024.

POLLICINO, Oreste, *Judicial Protection of Fundamental Rights on the Internet – A road towards Digital Constitutionalism?*, Oxford, Hart Publishing, 2021.

POLLICINO, ORESTE, BASSINI, MARCO, GREGORIO, GIOVANNI DE, *Internet Law and Protection of Fundamental Rights*, Milan, Bocconi University Press, 2022.

POLLICINO, ORESTE / GREGORIO, GIOVANNI DE, "Constitutional Law in the Algorithmic Society", in Hans-W. Micklitz et. al, (Ed.) *Constitutional Challenges in the Algorithmic Society*, Cambridge, Cambridge University Press, 2022, pp. 3-24.

POLLICINO, ORESTE, ROMEO, GRAZIELLA, "Concluding remarks – Internet Law, protection of fundamental rights and the role of constitutional adjudication", in Oreste Pollicino, Graziella Romeo (Ed) *The Internet and Constitutional Law – The Protection of fundamental rights and constitutional adjudication in Europe*, Routledge, 2020, pp. 234-250.

REXHEPI, RRITA, "Content Moderation: How the EU and the U.S. Approach Striking a Balance between Protecting Free Speech and Protecting Public Interest", *Trento Student Law Review,* Volume 5, n.º 1, 2023, pp. 69-98.

RÜCKER, DANIEL / KUGLE TOBIAS, *New European General Data Protection Regulation*, Hart, Oxford, 2018.

SILVA, JORGE PEREIRA DA, *Direitos Fundamentais para o Universo Digital,* Lisboa, Fundação Francisco Manuel dos Santos, 2024.

SILVA, NUNO SOUSA E,

"Novas regras para a internet: notas breves sobre iniciativas europeias de regulação de plataformas digitais", *Revista de Direito Intelectual*, n.º 1, 2021, pp. 75-102.

"Internet e Direitos Fundamentais: uma crescente interação", *Revista de Direito e de Estudos Sociais*, Ano LXII, n.º 4, 2024, pp. 203-233.

SOUSA, SIMÃO MENDES DE, *Constitucionalismo Digital – Uma Introdução*, Almedina, Coimbra, 2022.

TZANOU, MARIA, "Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right", *International Data Privacy Law*, Volume 3, n.º 3, 2013, pp. 88-99

VAZ, AFONSO VAZ et. al., *Direito Constitucional: o sistema constitucional português*, 1.ª Edição, Porto, 2015, Universidade Católica Editora.

VICENTE, DÁRIO MOURA, "Aplicação Extraterritorial do Direito ao Esquecimento na Internet?", *Revista da Ordem dos Advogados*, Volume 80, n.º 3-4, 2020, pp. 475-488.

WATCHER, SANDRA / MITTELSTADT, BRENT / FLORIDI, LUCIANO, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law*, Volume 7, 2, 2017, pp. 76–99.

Legislação

Lei n.º 27/2021, de 17 de maio.

Regulamento (UE) n.º 679/2016, de 27 de abril, 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 (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.

Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724, mais conhecido por Regulamento Governação de Dados.

Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais).

Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho de 14 de setembro de 2022 relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828.

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.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) (Texto relevante para efeitos do EEE).

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

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.

Jurisprudência

Google Spain c. Agencia Española de Protección de Datos (AEPD) e Costeja González, C-131/12, de 13 de maio de 2014.

Google c. CNIL, C-507/17, de 24 de setembro de 2019.

CK c. Magistrat der Stadt Wien, C-203/22, 27 de fevereiro de 2025.

M.S.I.D.C [1]

1 Mestrado Bolonha em Segurança de Informação e Direito no Ciberespaço, mais informação disponível a partir do url: https://fenix.tecnico.ulisboa.pt/cursos/msidc

RESPONSABILIDADE CIVIL NA INTELIGÊNCIA ARTIFICIAL - UMA ANÁLISE DA LEGISLAÇÃO EXISTENTE

CRISTINA REIS HENRIQUES

RESUMO:

A *leges artis* atual é insuficiente na proteção dos lesados em casos de danos causados por inteligência artificial (IA), seja na transação de bens e produtos, questões financeiras ou proteção de dados. Há um esforço para evitar uma "*esquizofrenia legislativa*" e a consequente insegurança jurídica, mas as lacunas na atribuição de responsabilidades persistem.

Uma abordagem promissora é a da responsabilidade pelo risco, onde quem tem um bem sob sua guarda é responsabilizado pelos danos causados por ele, mesmo sem culpa direta, a menos que se prove o contrário. Aplicado à IA, isso significaria que o utilizador, aceitando o risco, seria responsável por quaisquer danos das ferramentas de IA. Contudo, apesar de iniciativas como o Regulamento da IA, persistem omissões na proteção das vítimas. Ainda assim, responsabilidade civil aplicada à IA enfrenta desafios notáveis, nomeadamente, devido às decisões autónomas, opacidade dos algoritmos e interações entre diferentes ordens jurídicas.

É urgente uma maior harmonização legislativa para equilibrar os riscos da IA com a necessidade de segurança jurídica e da inovação, visando garantir uma sociedade mais equitativa e justa na era tecnológica.

Palavras-chave: IA; responsabilidade pelo risco; esquizofrenia legislativa; omissões; harmonização.

ABSTRACT:

The current *leges artis* is insufficient in protecting victims in cases of damages caused by artificial intelligence (AI), whether in the transaction of goods and products, financial matters, or data protection. There's an effort to avoid "legislative schizophrenia" and the consequent legal uncertainty, but gaps in liability attribution persist.

A promising approach is risk-based liability, where whoever has a good under their custody is held responsible for damages caused by it, even without direct fault, unless proven otherwise. Applied to AI, this would mean that the user of AI tools would be responsible for any damages, by accepting the risk. However, despite initiatives like the AI Regulation, gaps in victim protection persist. Nevertheless, civil liability applied to AI faces notable challenges, especially due to autonomous decisions, algorithm opacity, and interactions between different legal systems.

Greater legislative harmonization is urgent to balance the risks of AI with the need for legal certainty and innovation, aiming to ensure a more equitable and just society in the technological era.

Keywords: AI; risk-based liability; legislative schizophrenia; omissions; harmonization

I. INTRODUÇÃO: RESPONSABILIDADE CIVIL DA IA?

A Inteligência Artificial (doravante IA) tem-se vindo a tornar parte do nosso quotidiano ao longo dos últimos anos, seja em contextos simples (como a realização de pequenas tarefas domésticas) até aos contextos mais sofisticados (como é o caso da saúde ou da condução autónoma). A sua crescente influência no nosso dia-a-dia revela também um lado mais obscuro e desafiante, vejamos,

Quem será responsabilizado em casos de ciberataques?

Se esta já é por si só uma pergunta que levanta celeuma, a dúvida seguinte ainda deixa maiores e mais complexas preocupações: Se o ciberataque de que o sistema foi alvo levar a uma adulteração dos dados nos quais o sistema de IA se baseia para tomar decisões, quem será responsável pelos danos causados? Será sequer possível encontrar esse responsável?

As ferramentas de IA estão em constante evolução, tornando-se cada vez mais sofisticadas e abrangentes. No entanto, esta evolução tem tanto de benéfico quanto de nefasto. Por um lado, há mais avanços tecnológicos, mas por outro, surgem mais vulnerabilidades que podem ser exploradas.

Com o presente trabalho procuramos refletir um pouco sobre a problemática da responsabilidade civil em casos em que existe interferência de IA. Perceber que soluções existem atualmente e de que modo as mesmas estão verdadeiramente preparadas para resolver os problemas que vão surgindo.

II. CONCEITOS

a. Uma aproximação à definição de Responsabilidade Civil

Debater sobre um tema implica que de algum modo o conheçamos, pois só assim estaremos dotados das ferramentas necessárias para o poder discutir.

A responsabilidade Civil, lato sensu, consiste na obrigação de um agente assumir os encargos resultantes de uma ação ou de uma omissão que causou danos num terceiro, sendo que esses danos poderão ser morais ou físicos. Em termos práticos, e de uma forma bastante generalizada, o que irá acontecer é que a pessoa responsabilizada será obrigada a indemnizar a pessoa lesada, sendo que várias são as excepções existentes a esta regra.

No entanto, existem alguns pormenores na responsabilidade civil, desde logo porque não faria sentido responsabilizar alguém, apenas pela mera desconfiança de haver causado um dano. Como tal, averiguar a existência de responsabilidade civil implica analisar os

seus 5 pressupostos: facto, ilicitude, culpa, dano e o nexo causal entre o facto e o dano. De uma forma simples podemos dizer que para que alguém seja responsabilizado pela sua ação ele tem de ter agido (facto), de uma forma que não é legalmente aceitável (ilícito), tem de ter tido a vontade de agir (culpa), tem de ter causado o dano, ou seja, o lesado sofreu a consequência desse dano e por fim tem de existir um nexo causal, isto é, uma relação direta entre aquilo que o indivíduo fez (o facto) e o dano que ocorreu no lesado. No entanto, importa ter em atenção que mesmo estes 5 pressupostos têm as suas nuances, e que, por exemplo, nem sempre o pressuposto da culpa será obrigatório estar presente, vejamos:

Dentro da responsabilidade civil importará distinguir a objetiva da subjetiva. A primeira irá prescindir da verificação da culpa do agente (nestes casos o lesado não tem de provar a culpa, como por exemplo ocorre em grande parte dos seguros obrigatórios, onde se presume a responsabilidade pelo risco e não pela culpa). Por outro lado, a responsabilidade civil subjetiva estará dependente da culpa, pelo que aquele que alega ter sofrido o facto danoso terá de fazer prova da existência de culpa por parte do alegado agente (responsável), para poder então ser ressarcido.

b. Inteligência artificial

A IA pode definir-se como a capacidade de uma máquina reproduzir capacidades semelhantes às humanas, como por exemplo o raciocínio, a criatividade e a aprendizagem. Nas palavras do professor Dário Moura Vicente *"A Máquina dotada de Inteligência Artificial é, portanto, uma máquina capaz de compreender o seu ambiente, de aprender a partir dos inputs que retira desse ambiente em que se situa e de adotar ações de forma autónoma com vista a atingir certos objetivos para os quais está predestinada."*.

Ainda quanto à definição de IA, no âmbito do presente trabalho, importa distinguir *Machine learning* e *Deep Learning*.

No caso da *Machine learning* a máquina recebe do seu programador exemplos de respostas corretas a um determinado problema. Segundo a lógica por trás desta forma de aprendizagem está a ideia de que, a partir da introdução de dados, os computadores podem passar a reconhecer padrões, conseguindo realizar tarefas específicas. Nestes casos, as consequências negativas da sua utilização não são completamente imprevisíveis.

Já no caso de *Deep learning* existe uma verdadeira tentativa de imitar o cérebro humano. A informação é organizada em camadas (*Multilayer*) e estas camadas formarão uma rede

neural. O objetivo nestes casos é que os computadores consigam aprender com a sua própria atividade, deixando de ser necessário transmitir-lhes todo o conhecimento.

É ao nível do *deep learning* que existem maiores problemas no que à Responsabilidade Civil diz respeito, isto porque se torna bastante complicado compreender quem, ao surgir um dano, deverá ser responsabilizado pelo mesmo.

Se definir a Inteligência Artificial já não é nos nossos dias uma tarefa complicada, enumerar os seus modelos já se começa a tornar, isto porque são cada vez mais os que vão surgindo e a uma velocidade completamente estonteante. No entanto, podemos definir o que é um modelo de IA e depois então apresentar alguns exemplos.

Um modelo de IA é nada mais nada menos que um programa que foi treinado com um conjunto de dados por forma a reconhecer padrões e tomar decisões sem necessidade de intervenção humana. Os modelos de IA irão aplicar algoritmos diferentes consoante os dados que lhe são fornecidos, por forma a realizar as tarefas para as quais foram programados.

Alguns casos onde é possível ver a aplicação de IA são: assistentes virtuais, software de análise de imagem, motores de busca, sistemas de reconhecimento facial e de voz, robôs, carros autónomos, drones, ou aplicações no âmbito da Internet das Coisas

III. RELAÇÃO ENTRE RESPONSABILIDADE CIVIL E INTELIGÊNCIA ARTIFICIAL

a. Atribuição de Culpa e o Nexo Causal em Casos de Ataques

Aquando da análise de uma situação em que existe um dano causado por IA uma das primeiras figuras que vem à cabeça de um jurista é a da Responsabilidade Civil. No entanto, como já supra referido, o jurista terá de analisar se se encontra perante um caso de responsabilidade subjetiva (dependente da culpa) ou objetiva (independente da culpa). Tal distinção será de extrema importância, mormente para a responsabilização de um sujeito que será chamado a repor a situação existente previamente à ocorrência do dano.

A Responsabilidade Civil subjetiva, aplicada a casos em que existe interferência de IA, iria levar a três soluções possíveis: ou se responsabiliza o hacker que invadiu o sistema de IA, ou se responsabiliza o programador que programou a ferramenta de IA que causou o dano, ou se procura, por absurdo, atribuir essa responsabilidade diretamente à ferramenta de IA o que irá necessariamente exigir a atribuição de personalidade jurídica ao ente dotado de IA, isto porque para se lhes atribuir um juízo de culpa é também

necessário que estes entes sejam suscetíveis de uma censura ético-jurídica, e tal apenas será possível se os mesmos forem dotados de personalidade jurídica..

No entanto, qualquer uma destas soluções não nos parece 100% correta, as duas primeiras por não serem abrangentes a segunda por não ser plausível, vejamos:

Como poderemos solucionar caso o dano que ocorreu não tenha, de modo algum, tido origem numa atuação de um hacker ou de um programador? Se tiver sido simplesmente uma decisão tomada pela própria IA com base na aprendizagem que desenvolveu baseada nas suas experiências anteriores?

Por outro lado, que sentido fará atribuirmos um juízo de censura a uma máquina que não tem personalidade jurídica? Aqui importa atender a que, de acordo com o art.º 66.º, n.º1 do nosso Código Civil *"A personalidade adquire-se no momento do nascimento completo e com vida"* pelo que, tomando a figura existente atualmente no nosso ordenamento jurídico, torna-se por demais evidente que, atualmente, não é possível atribuir personalidade jurídica a estas máquinas o que, no nosso entender quer também dizer que não será possível atribuir um juízo de censura a estas máquinas, porquanto apenas será culpado alguém que seja também imputável, e alguém apenas será imputável se tiver *"capacidade natural para entender ou para prever os efeitos e medir o valor dos atos que pratica e para determinar de harmonia com o juízo que faça acerca deles".*

Porém, importa também atender a um outro problema levantado pela aplicação do instituto da Responsabilidade Civil a danos causados pela Inteligência Artificial, ou seja, o nexo causal, a relação existente entre o dano que ocorreu e o facto que o agente realizou. Ora, se o agente em causa for um sistema de IA, já será difícil este pressuposto ser cumprido, desde logo porque para ser um agente terá de ser dotado de personalidade jurídica, algo que como já supra referido não é, para já, possível. Ademais, esta relação de causalidade entre o facto e o dano poderá ser também complexa pela característica de opacidade que a própria IA tem, porquanto se torna difícil encontrar, na cadeia de criação do sistema de IA, quem será o principal responsável pela atuação incorreta daquele sistema de IA, daí que estabelecer este nexo causal entre o facto ocorrido e o dano sofrido pelo lesado pode ser bastante complexo, senão mesmo impossível em alguns casos.

IV. ANÁLISE DAS DIRETIVAS EUROPEIAS

- **Diretiva de responsabilidade por produtos defeituosos:**
  - **Origem e evolução**.

A Diretiva 85/374/CEE, adotada em 1985, foi a "mãe" da atual diretiva 2024/2853, nascida agora em 2024. A primeira visou promover uma harmonização de soluções relativamente à responsabilidade objetiva dos produtores por danos causados por produtos defeituosos, por forma a garantir uma maior segurança jurídica a todos os consumidores, porquanto deste modo era garantida uma solução igualitária para os mesmos problemas em todos os Estados-Membros da União. Tal preocupação tornou-se pertinente à medida que o mercado global foi crescendo, fazendo crescer o número de negócios realizados entre pessoas (quer singulares, quer coletivas) de diferentes países.

A primeira diretiva carecia cada vez mais de ser revista à luz das constantes evoluções da tecnologia, porquanto esta se vai desenvolvendo a um ritmo alucinante. Se por um lado o objetivo da diretiva "mãe" era garantir a salvaguarda dos direitos dos consumidores aquando da aquisição de produtos defeituosos, tal já não era suficiente para abranger situações em que essa mesma aquisição inclui produtos dotados de IA. Como tal, em 2022 a Comissão Europeia apresentou uma proposta de revisão, exatamente com o objetivo de abranger novos conceitos e novas realidades a que a tecnologia obrigava.

Após dois anos de discussão e constantes revisões, a diretiva entrou em vigor no passado dia 9 de dezembro de 2024, sendo que Portugal tem até dia 9 de dezembro de 2026 para incorporar estas novidades legislativas na sua legislação interna.

Além da preocupação com as novas tecnologias, esta nova diretiva procura também uniformizar as regras relativas à proteção dos consumidores nos diversos Estados-Membros e ainda promover uma maior ecologia dentro da própria UE, através da promoção de uma economia circular.

A transição de uma economia linear para uma economia circular, veio exigir que os produtos sejam duradouros e reparáveis com o objetivo de promover a sustentabilidade. Esta chamada economia circular exige que também exista uma maior proteção dos consumidores na aquisição de produtos, porquanto se os produtos são fabricados para serem mais duradouros e reparáveis, então também os seus produtores deverão ter as capacidades necessárias para garantir esse tipo de serviços e condições.

Porém, importa que nos foquemos aqui nas grandes mudanças que esta diretiva traz no âmbito da inteligência artificial.

Uma das novidades é o alargamento da definição de produto, porquanto é agora necessário incluir os conceitos associados à inteligência artificial, passando a abarcar conceitos como *software*, serviços digitais e ficheiros de fabrico digital, conforme plasmado no art.º 4.º, alínea a) da Diretiva 2024/2853:

Artigo 4.º Definições

Para efeitos da presente diretiva, entende-se por:

1) «Produto», todos os bens móveis, mesmo que integrados noutro bem móvel ou num bem imóvel ou com ele interligados. Inclui a eletricidade, os ficheiros de fabrico digitais, as matérias-primas e o software;

Ademais, e para o que aqui nos importa, esta Diretiva adota uma presunção de defeito de modo a facilitar aos consumidores a prova de que o produto é defeituoso, presumindo-se que o é quando não cumprir requisitos de segurança ou simplesmente falhar no decorrer de um uso normal e consequentemente também se presume que se algum dano ocorrer do uso desse produto defeituoso, esse mesmo dano foi causado pelo defeito em si, ou seja, estabelece-se um nexo causal entre o defeito e o dano ocorrido.

Associada a esta novidade vem também a questão dos prazos, sendo que os fabricantes terão 10 anos para serem processados, sendo este prazo aumentado para 25 anos no caso de se tratarem de produtos que causem danos que demorem a aparecer, porém o lesado apenas tem 3 anos após o conhecimento do defeito (ou o momento em que deveria ter tomado conhecimento do mesmo) para propor a ação, após este prazo esse seu direito prescreve.

- **Aplicação no contexto de IA**.

Ora, como já previamente referido, a Diretiva "mãe" trazia problemas na sua aplicação a situações que envolvessem o uso de IA, porquanto não se previa qual a classificação a atribuir a produtos de natureza tecnológica, nem como aferir a responsabilidade no caso de danos causados por tais entes. Estas questões começaram a conduzir a alguma dispersão legislativa, porquanto alguns Estados-Membros começaram a legislar sobre estes tópicos, levantando as suas preocupações, legítimas, sobre a responsabilização.

No que toca à Inteligência Artificial a diretiva traz três importantes mudanças, uma já referida anteriormente quanto à definição de produtos, e as outras duas são referentes à divulgação de elementos de prova e à presunção de causalidade.

- Apresentação dos elementos de prova - devido à onerosidade que geralmente existe do lado do lesado para obter provas sobre o sistema de Inteligência

Artificial que terá conduzido à sua lesão, ressalva este artigo a possibilidade de os Tribunais Nacionais poderem ordenar a divulgação dos necessários elementos de prova sobre os sistemas da Inteligência Artificial, deixando aqui de se exigir que seja o próprio lesado a fazer prova dos mesmos. Vejamos, neste sentido, o artigo 9.º da Diretiva 2024/2853:

Artigo 9.º Apresentação de elementos de prova

1. Os Estados-Membros asseguram que o demandado seja obrigado a apresentar os elementos de prova pertinentes de que dispõe, a pedido de uma pessoa que peça uma indemnização através de uma ação intentada junto de um tribunal nacional por danos causados por um produto defeituoso («demandante») e que tenha apresentado factos e elementos de prova suficientes para fundamentar a plausibilidade da ação de indemnização, nas condições previstas no presente artigo.

- A presunção da causalidade por seu turno vem estabelecer a possibilidade, conforme já supra referido, de se presumir uma relação causal entre o dano ocorrido e o defeito existente no produto e encontra-se plasmada no art.º 10.º, nº 4 da Diretiva que dispõe o seguinte:

Artigo 10.º Ónus da prova

Um tribunal nacional presume a existência de um defeito do produto ou o nexo de causalidade entre o defeito e o dano, ou ambos, se, não obstante a apresentação de elementos de prova nos termos do artigo 9.º e tendo em conta todas as circunstâncias pertinentes do processo:

a) O demandante enfrentar dificuldades excessivas, em particular por motivos de complexidade técnica ou científica, para provar a existência de um defeito do produto ou o nexo de causalidade entre o seu defeito e o dano, ou ambos; e

b) O demandante demonstrar que é provável que o produto seja defeituoso ou que existe um nexo de casualidade entre o defeito do produto e o dano, ou ambos.

Conforme dá para compreender ambas estas novidades se encontram numa estreita correlação, porquanto se uma trata de uma inversão do ónus da prova, a outra por seu turno trata da possibilidade de serem os próprios Tribunais a exigir o cumprimento dessa inversão do ónus da prova.

- **Regulamento da IA (AI Act):**

O Regulamento da Inteligência Artificial (Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho) é pioneiro no quadro jurídico mundial, sendo a primeira legislação inteiramente dedicada à Inteligência Artificial.

Com este Regulamento visa-se promover a confiança neste tipo de sistemas, assegurando que os mesmos respeitam os Direitos Fundamentais, os princípios éticos e promovem a segurança no uso de tais ferramentas.

A legislação anterior permitia alguma proteção em casos de uso de máquinas dotadas de IA, quanto mais não seja uma Responsabilidade pelo Risco, assumindo-se que aquele que tem a seu cargo um veículo ou máquina será responsabilizado pelos danos que a coisa possa causar e que sejam decorrentes de um uso normal dessa mesma coisa. No entanto, este tipo de soluções não apresenta resposta para casos em que um sistema de IA toma uma decisão em detrimento de outra, sem qualquer motivo aparente. Exemplo disso são as empresas que usam, nos seus departamentos de recursos humanos, sistemas de IA para análise de possíveis candidatos a uma determinada vaga, mas torna-se aqui difícil avaliar se alguém foi injustamente prejudicado ou se, por outro lado, injustamente beneficiado.

- **Evolução cronológica**

O surgimento deste Regulamento não foi imediato, e muito menos célere. O debate sobre tal necessidade já é prévio a 2020, mas foi a 1 e 2 de Outubro de 2020 que o Conselho Europeu iniciou o seu debate formal sobre a IA e os seus desafios. Após este debate o Conselho Europeu convidou a Comissão Europeia a apresentar uma proposta para promover os investimentos públicos e privados, europeus e nacionais, na investigação e implantação da IA e a fornecer uma clara definição de sistemas de IA considerados de alto risco.

Foi em abril de 2021 que a Comissão Europeia apresentou a sua proposta de Regulamento para a IA, onde procurou abranger todos os pedidos que haviam sido feitos pelo Conselho, visando harmonizar as regras em matéria de Inteligência Artificial e um plano coordenado que inclui uma série de ações conjuntas da Comissão e dos Estados-Membros.

A 6 de dezembro de 2022 o Conselho, que havia solicitado esta proposta à Comissão, debate sobre a mesma e adota uma posição ("orientação geral") sobre o Regulamento Inteligência Artificial. O objetivo do novo regulamento proposto é garantir que os sistemas de IA colocados no mercado da UE e utilizados na União sejam seguros e respeitem a legislação em vigor em matéria de direitos fundamentais e valores da União.

Uma vez que a Comissão já havia adotado uma posição de orientação geral, tal permite ao Conselho encetar negociações com o Parlamento Europeu ("trílogos") assim que este adotar a sua própria posição, com vista a chegar a acordo sobre a proposta de regulamento. Finalmente, a 9 de dezembro de 2023, o Conselho e o Parlamento chegam a acordo sobre o Regulamento da IA, e após 3 dias de conversações, o Conselho e o Parlamento chegam ao que se chama um acordo provisório sobre o ato legislativo.

A 21 de maio de 2024 o Conselho aprovou o Regulamento da IA e logo de seguida, a 1 de Agosto de 2024 este entrou em vigor.

Importa ainda referir que a grande novidade deste regulamento é a sua atuação "baseada no risco", ou seja, quanto maior for o risco de danos para a sociedade, mais rigorosas são as regras a aplicar.

Transição para a aplicação plena do Regulamento:

- Logo após a sua entrada em vigor, as práticas de IA consideradas de risco inaceitável são proibidas.
- Nos 6 meses seguintes: são aplicadas restrições quanto a práticas proibidas.
- Após 9 meses: Os códigos de conduta terão aplicabilidade geral.
- Após 12 meses: As regras para a IA de uso geral devem estar em funcionamento.
- Após 24 meses: A maioria das disposições do regulamento tornam-se plenamente aplicáveis.
- Após 36 meses: As obrigações para os sistemas de alto risco entram em vigor.
- Níveis de risco e implicações jurídicas.

Conforme já supra referido, este regulamento adota uma atuação baseada no risco que pode resultar da utilização de sistemas de IA, definindo requisitos específicos para os participantes em cada um dos níveis de risco, requisitos esses que, como veremos, serão tanto mais apertados quanto mais risco se encontrar envolvido. Estas exigências irão ser aplicadas não só aos fornecedores de sistemas de IA, mas também aos próprios programadores responsáveis pela implementação desses sistemas para fins profissionais, ou seja, não será aqui quem produz os sistemas, mas sim quem se dedica a colocá-los em funcionamento.

Vamos então fazer uma breve análise dos diversos níveis de risco apresentados ao longo do regulamento:

- **Risco inaceitável -** abrangerá todos os sistemas de IA que são considerados uma ameaça aos meios de subsistência e à segurança das pessoas e dos estados.

Exemplos deste tipo de sistemas são brinquedos que utilizam a voz para incentivar comportamentos perigosos.

- Ex: **My Friend Cayla** lançada em 2014, usava inteligência artificial para responder a perguntas feitas por crianças.
    - Problema: Embora não incentivasse diretamente comportamentos perigosos, a boneca foi criticada pela sua vulnerabilidade a ser *hackeada*, que poderia levar a que as suas respostas fossem alteradas para conteúdos perigosos ou inadequados. Além disso, veio-se a descobrir que esta boneca recolhia dados pessoais das crianças sem consentimento adequado, expondo-as a riscos de privacidade.
    - Consequência: A boneca foi banida em alguns países, como a Alemanha.

- **Risco elevado**
    - Sistemas de IA considerados de risco elevado incluem a tecnologia utilizada em infraestruturas críticas que possam pôr em risco a vida e saúde das pessoas (como por exemplo os carros autónomos); ou a tecnologia usada na gestão de trabalhadores e de acesso ao trabalho (com o uso de sistemas de triagem automática de CVs); ou ainda a tecnologia usada no ensino e acesso à formação que pode determinar automaticamente o acesso a um curso de licenciatura ou de mestrado (onde os candidatos são analisados automaticamente por sistemas de IA).
- **Risco limitado**
    - O conceito de risco limitado está relacionado à falta de transparência no uso da Inteligência Artificial. O Regulamento de Inteligência Artificial estabelece obrigações específicas para garantir que os indivíduos sejam devidamente informados quando necessário, fortalecendo a confiança nos sistemas de IA. Por exemplo, ao interagir com sistemas como robôs de conversação (*chatbots*), é essencial que as pessoas saibam que estão a comunicar com uma máquina, permitindo-lhes decidir de forma consciente se desejam continuar ou não. Além disso, os fornecedores devem assegurar que os conteúdos produzidos por IA sejam identificáveis.

- **Risco mínimo ou nulo**
    - Aqui inserem aplicações da IA em jogos de vídeo ou filtros de *spam* nos nossos *e-mails*, nestes casos o regulamento permite a utilização gratuita por considerar exatamente haver baixo risco, ou mesmo nulo. A maior parte dos sistemas de IA atualmente em uso inserem-se nesta categoria de risco.

- **Impacto esperado na RC.**

Apesar desta classificação de risco efetuada ao longo do regulamento, a verdade é que pouco ou nada fica decidido quanto a danos causados por sistemas de IA e quem será responsabilizado, sendo que ao longo de todo o regulamento a única referência feita a esta figura é na Secção 4 que versa sobre "Autoridades Notificadoras e organismos notificados", secção esta que estabelece as regras a implementar quanto à análise de risco dos sistemas de IA e conformidade com o regulamento.

Esta única referência estabelece que:

"Os organismos notificados devem subscrever um seguro de responsabilidade civil adequado para as suas atividades de avaliação da conformidade, a menos que essa responsabilidade seja assumida pelo Estado-Membro onde se encontram estabelecidos nos termos da legislação nacional ou que o próprio Estado-Membro seja diretamente responsável pela avaliação da conformidade." - vide art.º 31.º, nº9 do Regulamento da IA

Ora, como se vê, mesmo aqui a referência que é feita nem é sobre uma responsabilidade civil "direta" pelos danos causados pelo sistema/ modelo dotado de IA, mas sim dos organismos que garantem a conformidade destes para com as normas do Regulamento, ou seja, atribui-se a esses organismos a responsabilidade de garantir a conformidade dos modelos para com o regulamento e os respectivos níveis de risco.

Porém esta solução não responde a uma outra questão também ela bastante pertinente: e se os responsáveis por essa análise a fizeram de modo correto, cumprindo com todos os requisitos exigidos, mas ainda assim o sistema é pirateado e uma empresa, por exemplo bancária, sofre perdas financeiras incomensuráveis, quem será responsabilizado? Fará sentido acionar o tal seguro? Não irão as seguradoras, como em grande parte dos casos, procurar fugir a uma responsabilização?

A verdade é que a UE está consciente da insuficiência da legislação em vigor quanto a este tema da responsabilidade civil, e por isso mesmo tem estado a trabalhar em novas

regras relativas à responsabilidade civil da IA (Proposta de Diretiva Responsabilidade da IA) por forma a começar-se a abranger também os danos causados por comportamentos indevidos de sistemas de IA.

- **Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial (Diretiva Responsabilidade da IA)**
    - **Enquadramento histórico**

No decorrer do seu mandato enquanto presidente da Comissão Europeia, Ursula von der Leyen destacou a importância de uma abordagem coordenada na União Europeia para a IA. Em fevereiro de 2020, no Livro Branco sobre IA, a Comissão Europeia comprometeu-se a estimular a adoção desta tecnologia, ao mesmo tempo que procurava mitigar os riscos inerentes a algumas das suas aplicações, promovendo assim a confiança e a excelência. O relatório que acompanha o Livro Branco identificou os desafios específicos que a IA apresenta para as normas de responsabilidade vigentes.
Posteriormente, a 9 de junho de 2020, nas Conclusões intituladas "Construir o futuro digital da Europa", o Conselho reconheceu o valor das consultas públicas realizadas sobre as estratégias do Livro Branco e incentivou a Comissão a avançar com propostas concretas. Por sua vez, o Parlamento Europeu, em 20 de outubro de 2020, aprovou uma resolução solicitando que a Comissão elaborasse uma proposta legislativa sobre responsabilidade civil para IA, com base no artigo 114.º do Tratado sobre o Funcionamento da União Europeia.

- **Importância de legislação neste sentido**

Conforme já foi possível compreender as regras existentes quanto à atribuição de responsabilidade não são suficientemente amplas para conseguir abarcar situações em que há danos causados por produtos e serviços assentes na IA.
De acordo com as regras atualmente em vigor, cabe às vítimas provar que o dano que sofreram adveio de um modelo de IA, o que se pode tornar excessivamente oneroso. Ademais, o conhecido efeito da “caixa negra”, consequência da opacidade e autonomia destes sistemas, dificulta a identificação e atribuição de responsabilidade pelos danos.
Se não existir uma legislação harmonizada quanto a este tema, poderá acontecer que os tribunais nacionais, ao verem-se confrontados com casos que envolvem IA irão procurar aplicar as regras em vigor, e tal poderá ser claramente injusto, uma vez que não se tem

em conta as novas características do caso concreto, nomeadamente que pode ter existido uma atuação de um terceiro que não era de todo evitável (como o caso dos *hackers*). Este tipo de insegurança aumenta se se falar em situações que envolvem diversos ordenamentos jurídicos, porque aí já existirá uma concorrência entre diversas jurisdições, o que poderá, consequentemente, levar a decisões ainda mais díspares.

Sendo estes temas motivo de preocupação junto dos diversos estados-membros, começaram a surgir, de modo interno, algumas medidas legislativas para salvaguarda de casos de responsabilidade civil decorrente da IA. E se a UE não atuasse, aquilo que não passava de um receio de fragmentação legislativa, torna-se numa realidade, com diversas decisões judiciais antagónicas para casos semelhantes entre si.

Esta nova proposta visa promover uma implementação da IA que promova a confiança, garantindo que as vítimas de IA obtêm o mesmo grau de proteção que as vítimas de outros danos.

- **RGPD:**

O avanço da tecnologia tem gerado novos desafios no campo da cibersegurança e na proteção de dados. Com o digital cada vez mais presente nas atividades diárias e a crescente interconexão entre dispositivos, o número de possíveis alvos para cibercriminosos aumenta significativamente. Áreas como redes sociais, plataformas de comércio online e serviços de armazenamento em nuvem são particularmente suscetíveis a ataques, muitas vezes envolvendo o acesso indevido a dados pessoais e confidenciais.

Além disso, os ciberataques tornam-se cada vez mais sofisticados. Técnicas como *phishing* e *ransomware* estão a ser utilizadas por criminosos para explorar falhas em sistemas de informação e comprometer a integridade dos dados. A utilização da Inteligência Artificial por agentes maliciosos intensifica ainda mais o risco, permitindo a criação de ataques automatizados e altamente direcionados, que não apenas ameaçam sistemas, mas também expõem informações sensíveis de indivíduos e organizações. Isso sublinha a importância de implementar medidas robustas para garantir a segurança e a proteção de dados, assegurando a privacidade e a conformidade com regulamentações como o RGPD.

- **Enquadramento da RC em caso de violação de dados.**

A União Europeia tem-se destacado enquanto líder na criação de normas rigorosas para a salvaguarda dos dados pessoais, sendo o Regulamento Geral de Proteção de Dados (RGPD) um dos seus maiores avanços. O regulamento, entre outras, define regras

específicas para a gestão das informações pessoais e prevê as sanções a aplicar para quem não cumpra as disposições ali existentes.

Porém, o RGPD não aborda de um modo direto as questões relacionadas com a IA, mormente em matéria de responsabilidade, sendo que apenas foca a "Responsabilidade do responsável pelo tratamento", sem expandir esta realidade por forma a abarcar os desafios e riscos trazidos pela IA.

Artigo 24.º Responsabilidade do responsável pelo tratamento

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

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

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

A grande questão que se coloca aqui quanto ao RGPD é que as organizações têm de garantir que as suas práticas de processamento de dados com recurso à IA respeitam os princípios da transparência, da minimização de danos e o consentimento informado.

Ademais, quanto mais são usadas ferramentas de IA para tratamento de dados, melhores têm de ser as medidas técnicas para proteger esses mesmos dados contra acessos não autorizados e violações.

- **Um exemplo prático: COMPAS.**

O COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) foi um *software* dotado de IA, desenvolvido nos Estados Unidos com o objetivo de avaliar o risco de reincidência criminal. Este *software*, que utiliza algoritmos que analisam dados pessoais e registos criminais dos réus, auxiliou os tribunais a decidir as sentenças a aplicar em determinados casos.

Em 2016 um estudo veio a comprovar que o referido *software* apresentava vieses raciais, isto é, assumia que os réus teriam maior ou menor probabilidade de reincidência

consoante o seu tom de pele, considerando os "brancos" como menos prováveis a reincidir e os "negros" como mais prováveis de o fazer. Esse mesmo estudo comprovou que, por exemplo, indivíduos negros sem qualquer historial criminal prévio ainda assim eram classificados como de alto risco de reincidência.

Implicações Jurídicas e Éticas

Este estudo sobre o COMPAS levantou discussões sobre o uso de algoritmos em decisões judiciais, nomeadamente devido à falta de transparência nos critérios utilizados pelos *softwares*, que muitas vezes são classificados como fazendo parte do segredo comercial da empresa. Esta questão da falta de transparência conduziu a uma impossibilidade de contestação dos resultados gerados pelo *software,* o que demonstra uma clara violação de direitos fundamentais com o direito a um julgamento justo (art.º 10.º da Declaração Universal dos Direitos Humanos), direito à igualdade perante a lei (art.º 13.º da Constituição da República Portuguesa).

V. REFLEXÕES CRÍTICAS

- **Limitações das diretivas atuais: Lacunas na atribuição de responsabilidades.**

Atendendo ao supra explanado torna-se por demais evidente que qualquer uma das legislações em vigor é ainda insuficiente no que à responsabilidade civil diz respeito. Os lesados continuam a ser pouco protegidos no caso de interferência de IA, e isto ocorre não só na transação de bens e produtos, como também no âmbito de questões financeiras e proteção de dados.

É claro que tem existido um esforço por forma a salvaguardar-se esta questão da responsabilização, até por se reconhecer que permitir que cada Estado decida como melhor lhe aprouver seria permitir uma indesejada "esquizofrenia legislativa", que consequentemente leva a uma insegurança jurídica e falta de confiança dos cidadãos, quer nos sistemas de IA, quer na própria justiça em si (atos legislativos e decisões judiciais).

- **Adaptação das leis existentes.**

Atendendo às soluções existentes atualmente, parece-nos que a abordagem mais adequada para estes casos seria o da responsabilidade pelo risco. Este princípio estabelece que *"quem tiver sob a sua guarda um bem móvel ou imóvel, com o dever de vigilância, bem como quem tiver assumido a responsabilidade pela supervisão de animais, é responsável pelos danos causados por esses bens ou animais, salvo se demonstrar que não houve culpa da sua parte ou que os danos teriam ocorrido mesmo sem qualquer culpa sua".*

Aplicar este conceito aos casos que envolvem IA faria com que consequentemente o utilizador das ferramentas de IA seria responsabilizado por quaisquer danos causados por esta, independentemente da intervenção de terceiros, porquanto ao fazer uso de tais sistemas o utilizador está ciente que é possível existir algum ciberataque, e aceita essa possibilidade, assumindo a responsabilidade por essa possível consequência.

VI.CONCLUSÃO

Apesar de todos os problemas levantados, a verdade é que já começam a surgir algumas soluções que procuram acompanhar o ritmo frenético a que todos estes temas se desenrolam e desenvolvem.

Há discussões sobre a criação de um novo conceito de "responsabilidade dos sistemas", onde as entidades jurídicas, como empresas, assumirão a responsabilidade legal por danos causados por IA, mesmo que não haja um culpado humano claramente identificado.

O Regulamento da Inteligência Artificial, apesar de fazer pouca referência à responsabilidade civil, sugere que a responsabilidade pelo uso da IA seja atribuído aos que operam as ferramentas de IA, o que significa que, p.e, no caso de um veículo autónomo, seja responsabilizado pelos danos aquele que o "conduz", baseando-se aqui numa responsabilidade pelo risco, como supra referido.

É evidente, atenta toda a análise elaborada, que a responsabilidade civil aplicada à IA ainda encontra desafios significativos., especialmente em contextos que envolvem decisões autónomas, opacidade de algoritmos e interações entre diferentes ordens jurídicas. A evolução normativa, como por exemplo através do Regulamento da IA e a proposta de Diretiva da Responsabilidade da IA, demonstram os esforços que têm sido feitos para acompanhar os avanços tecnológicos, mas ainda assim há lacunas por colmatar, nomeadamente quanto à proteção das vítimas e na atribuição de responsabilidades.

Concluindo, urge uma maior harmonização que contemple quer os riscos intrínsecos da IA, quer as necessidades de segurança jurídica e inovação, pois só deste modo será possível equilibrar o potencial transformador desta tecnologia com as exigências éticas e jurídicas de uma sociedade harmoniosa.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, OLIVEIRA . “Acórdão Do Supremo Tribunal de Justiça.” *Dgsi.pt*, 2019, www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/cbc055e78ae86efa80258496005c8e84?OpenDocument. Accessed 6 Jan. 2025.

VARELA, ANTUNES. Das Obrigações Em Geral - Vol. I. Leya, 4 Aug. 2023..

Catarina, Ana, and Oliveira Teixeira. *UNIVERSIDADE CATÓLICA PORTUGUESA Responsabilidade Civil E Inteligência Artificial: Quem Responde Em Caso de Erro Do Equipamento Médico Inteligente?* 2022, repositorio.ucp.pt/bitstream/10400.14/41278/1/203309464.pdf. Accessed 6 Jan. 2025.

de Azeredo Silva, Inês. DIRETIVA RESPONSABILIDADE DA INTELIGÊNCIA ARTIFICIAL DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO RELATIVA À ADAPTAÇÃO DAS REGRAS de RESPONSABILIDADE CIVIL EXTRACONTRATUAL À INTELIGÊNCIA ARTIFICIAL INTRODUÇÃO.

direito.up.ptdigeucit. “Publicada a Diretiva Relativa à Responsabilidade Decorrente Dos Produtos Defeituosos – DigEUCit.” DigEUCit – a Digital Europe for Citizens, 21 Nov. 2024, direito.up.pt/digeucit/2024/11/21/publicada-a-diretiva-responsabilidade-decorrente-de-produtos-defeituosos/. Accessed 15 Jan. 2025.

“Diretiva - 2024/2853 - Relativa à Responsabilidade Decorrente Dos Produtos Defeituosos.” Europa.eu, 2024, eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ%3AL_202402853. Accessed 15 Jan. 2025.

Europeu, Parlamento. “Como Alcançar a Economia Circular Na UE Até 2050?” Temas | Parlamento Europeu, 5 Feb. 2021, www.europarl.europa.eu/topics/pt/article/20210128STO96607/como-alcancar-a-economia-circular-na-ue-ate-2050.

Parlamento Europeu. “O Que É a Inteligência Artificial E Como Funciona?” *Temas | Parlamento Europeu*, 4 Sept. 2020, www.europarl.europa.eu/topics/pt/article/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona.

“Proposta Diretiva Responsabilidade Da IA.” Europa.eu, 2022, eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52022PC0496. Accessed 15 Jan. 2025.

“REGULAMENTO GERAL SOBRE a PROTEÇÃO de DADOS (RGPD) DA UNIÃO EUROPEIA (UE).” Www.pgdlisboa.pt, www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2961&tabela=leis.

“Regulamento Da IA.” Jornal Oficial Da UE, 13 June 2024, eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689. Accessed 5 Jan. 2025.

Sousa, Henrique. A RESPONSABILIDADE CIVIL APLICÁVEL À INTELIGÊNCIA ARTIFICIAL: PRIMEIRAS NOTAS CRÍTICAS SOBRE a RESOLUÇÃO DO PARLAMENTO EUROPEU de 2020.

“Regulamento Inteligência Artificial.” *Consilium*, 2014, www.consilium.europa.eu/pt/policies/artificial-intelligence/.

SOFTWARE LIVRE E DIREITOS FUNDAMENTAIS

ADRIANO ROBERTO PINTO

RESUMO:

As tecnologias de informação são indispensáveis para promover e salvaguardar direitos fundamentais, mas frequentemente são tratadas somente sob aspectos comerciais, de privacidade e/ou segurança - em detrimento de questões socioambientais e de direitos humanos. Sob esta premissa, serão abordadas duas importantes ferramentas para a manutenção dos direitos fundamentais à luz da Constituição: o Software Livre e as Licenças Copyleft.

Palavras-Chave: Software Livre, Copyleft, Direitos de Autor, *Open-Source*, Propriedade Intelectual.

ABSTRACT:

Information technologies are indispensable for safeguarding and promoting fundamental rights, but they're often treated solely under commercial, privacy, and/or security matters – to the detriment of socio-environmental and human rights issues. Under this premise, two important tools for maintaining fundamental rights considering the Constitution will be addressed: Free Software and Copyleft Licenses.

Keywords: Free Software, Copyleft, Copyright, Open-Source, Intellectual Property.

I. INTRODUÇÃO

Este artigo discorre sobre a importância do Software Livre para o acesso ao conhecimento e manutenção dos direitos fundamentais à luz da Constituição da República Portuguesa (CRP), que facilmente encontra equivalências também nas constituições de outros países de regime democrático. As principais premissas são de que para garantia dos direitos fundamentais o conhecimento deverá ser sempre de acesso universal e livre de patentes ou restrições, e que os códigos-fonte de softwares são formas de conhecimento, e para tanto, devem ser mantidos como Software Livre ou licenças correlatas. Softwares sob licenças proprietárias contrariam essas proposições e violam direitos dos usuários.

Para fins de simplificação, os termos *copyright*, patente, direito de autor e propriedade intelectual serão tratados como sinônimos. Apesar de haver diferenças, neste texto o foco está em suas similaridades ao restringirem o acesso ao conhecimento, violarem direitos fundamentais e favorecerem monopólios.

Os conceitos de Software Livre e *copyleft* abrangem também *hardware*, *firmware* e manuais técnicos, mas os exemplos neste artigo serão voltados para programas de computador e seus códigos-fonte. Código-fonte é a forma original de um programa, onde as instruções de execução estão em formato de texto puro, ou seja, somente caracteres alfanuméricos.

Quanto ao termo *open-source*, quando utilizado em inglês, refere-se às licenças desse tipo, já sua forma traduzida (código aberto) trata dos softwares ou programas que tem seus códigos-fonte disponíveis para estudo e auditoria. Em oposição aos softwares de código fechado, que tem apenas versões em código de máquina [17]. Para que as instruções sejam entendidas pelos computadores, os códigos-fonte devem ser convertidos em código de máquina, ou instruções binárias, que são ilegíveis para humanos.

II. COPYRIGHTS E LICENÇAS

Copyright é um anglicismo para direito autoral ou propriedade intelectual, que pode ser definido como direitos garantidos legalmente ao autor para que possa distribuir e reproduzir suas criações ao público da forma que desejar, além de definir as condições para o uso de seus trabalhos por terceiros – o que inclui softwares. Portanto, o *copyright* é uma construção legal que pode dar a alguém direitos exclusivos sobre trabalhos criativos de qualquer espécie, tornando-os automaticamente inacessíveis e não compartilháveis sem a permissão do autor.

O *copyright* surgiu em meados do século 18, como uma forma de regulação da indústria de impressão, editoração e ramos relacionados. O objetivo era estimular a produção de obras escritas ao exigir que as editoras obtivessem permissão dos autores para publicação de seus textos. Com isso, os autores

passaram a ter remunerações pelos trabalhos publicados, o que atraiu mais profissionais para a área e incentivou a expansão dessa indústria. O público geral beneficiou-se, pois nessa época os *copyrights* restringiam apenas os editores, e não o que os leitores e consumidores finais poderiam fazer com as publicações adquiridas [1].

Copyrights sobre softwares afetam tanto profissionais de informática quanto usuários comuns devido às limitações impostas e custos para aquisição. Há situações onde o direito não é apenas sobre um programa específico, mas sobre ideias práticas. Indivíduos que implementem tais ideias, poderão inadvertidamente violar direitos de autor. Um exemplo disso é descrito em um estudo controverso, feito por Dan Ravicher da Public Patent Foundation, sobre 283 *copyrights* dos EUA que teriam sido violados no código fonte do kernel[1] do sistema operacional Linux [8]. Possíveis soluções para esse tipo de problema envolvem mudanças nos critérios de concessão de *copyright*, como proibir novas licenças em certos contextos, mas ainda haveria risco de brechas e não eliminaria licenças existentes. Em Portugal, a abolição de um direito de autor existente entraria em conflito com o **Artigo 18.º, nº3, Força jurídica**, da CRP.

2.1.COPYRIGHTS NA UNIÃO EUROPÉIA

A lei europeia dos direitos de autor é composta principalmente por diretivas e regulamentos concebidos para harmonizar a proteção dos direitos de autor nos estados-membros da União Europeia. Esta abordagem visa garantir que os criadores e os titulares de direitos se beneficiem de proteções equivalentes, independentemente do país. Muitas das diretrizes baseiam-se em elementos de acordos internacionais, como a Convenção de Berna e a Convenção de Roma [20], que cada país membro deve transpor para sua legislação local. A mais recente é a **Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho, de 17/04**, relativa aos direitos de autor e direitos conexos no mercado único digital e que altera as Diretivas 96/9/CE e 2001/29/CE, texto relevante para efeitos do EEE, referida também como "*Direitos de Autor no Mercado Único Digital*". Ela visa melhorar a proteção dos direitos de autor e adaptar as regras ao meio digital, promove acessibilidade transfronteiriça e um mercado digital mais integrado [21].

Em Portugal, obras e criações intelectuais são protegidas pelo Artigo 42.º n.º 2 da Constituição da República Portuguesa (Liberdade de Criação Cultural), e o assunto é pormenorizado principalmente no DL nº 63/85, de 14/03, Código do Direito de Autor e dos direitos conexos, na sua versão actualizada. A gestão dos direitos do autor pode ser exercida pelo próprio autor, por representantes legais e por titulares dos direitos. O uso da obra por terceiros pode ser considerado crime de usurpação se não

1 Kernel é o principal componente de um sistema operacional.

houver autorização, ou se o terceiro se colocar como criador da obra, além de outras condições previstas em lei.

Um *copyright* estabelecido em Portugal tem validade em todos os países da União Europeia e também nos países que assinaram a Convenção da União de Berna para a proteção das obras literárias e artísticas [2][3]. A permissão para uso de uma obra por terceiros, e as respectivas condições, são definidas através de licenças e contratos. No caso das licenças para softwares, a maioria restringe ou afronta de alguma maneira as liberdades dos usuários e também dos profissionais que desenvolvem softwares que utilizam dependências proprietárias. As dependências são partes menores de um programa ou software, necessárias para seu funcionamento [4][5].

2.2.DEPENDÊNCIAS: *ANALOGIA DO CARRO E DA RODA*

A seguinte analogia sobre o carro e a roda serve para explicar de forma simplificada o que são dependências no contexto de programação e seu papel no Software Livre. Onde o carro pode ser considerado o objeto principal, composto por várias partes fundamentais sem as quais não poderia operar, como as rodas e o motor. Portanto, as rodas e o motor são dependências para o funcionamento do carro. Analogamente, em informática, o software seria o objeto principal e as bibliotecas[2] partes fundamentais, ou dependências, para seu funcionamento.

Dentro da mesma analogia, suponha-se que o atributo circular das rodas fosse de propriedade intelectual de uma empresa ou indivíduo. Outros que desejassem fabricar carros precisariam pagar pela licença de uso das rodas circulares. Como é impossível reinventar a roda, e essa já seria de propriedade de outrem, a única opção para não pagar pela licença seria utilizar uma dependência alternativa, possivelmente menos eficiente, como substituir as rodas circulares por rodas de formato elíptico. Algo parecido ocorre com as dependências de software que não possuem alternativas viáveis - livres de copyrights. Essa analogia absurda seria suportada pelo Artigo 42.º n.º2, Liberdade de criação cultural, da CRP e entraria em conflito com vários outros artigos da CRP, que serão discutidos adiante.

2.3 COPYLEFT

Copyleft é uma abordagem legal para licenciar Software Livre e que oferece a todos os direitos de usar, estudar, compartilhar e melhorar os softwares. Esses quatro direitos são designados como as quatro liberdades do Software Livre. Tais liberdades devem ser mantidas durante a distribuição posterior do software e de trabalhos derivados. Por exemplo, se o software, ou suas dependências,

2 Bibliotecas são subprogramas com funções específicas que servem para simplificar e modularizar o desenvolvimento de um software.

forem modificados por terceiros, eles não poderão ser redistribuídos sob licenças incompatíveis com o *copyleft* original – isso inclui licenças de tipo *open-source* que violem alguma das quatro liberdades. Licenças compatíveis são aquelas que respeitam as quatro liberdades e não possuem restrições. Porém, há casos de licenças com requisitos que não são considerados realmente restritivos. Por exemplo: licenças que não permitem o uso de certas marcas registadas e logotipos. A [12, Fig. 1] demonstra a relação entre algumas licenças *copyleft* e a GPLv3, que é a versão mais recente da Licença Pública Geral GNU[3] e uma das mais utilizadas.

Em resumo, as licenças *copyleft* garantem que softwares derivados e suas dependências sejam licenciados sob os mesmos termos do trabalho original. Assim, partes de Software Livre não poderão ser convertidas em software proprietário [7].

2.4 DOMÍNIO PÚBLICO

Obras sob domínio público, inclusive softwares, não exigem licenças para serem utilizadas por terceiros e assumem essa condição quando os direitos de autor expiram ou são abdicados. Geralmente, domínio público é compatível com licenças *copyleft*. Porém, na União Europeia, cada país membro tem regulamentações e interpretações distintas sobre direitos autorais, por isso a adoção de uma licença *copyleft* pode ser mais segura do que publicar sob domínio público. Outro aspecto importante é que, por padrão, todo software é protegido por direitos autorais, a não ser que seja explicitado o contrário. Em Portugal, o domínio público é abordado genericamente pelo Artigo 84.º, Domínio público, da CRP. Similar ao domínio público, a licença *Creative Commons CC0 1.0 Universal*[4] é uma alternativa que se aproxima muito do que seria a renúncia dos direitos de autor e é compatível com licenças *copyleft*. A compatibilidade das licenças é importante para evitar violações de direitos de autor pela utilização de dependências com licenças incompatíveis no mesmo software [6].

2.5.O MOVIMENTO SOFTWARE LIVRE

O Movimento Software Livre foi iniciado por Richard Stallman em 1984 através do projeto GNU[5], com o propósito de enfrentar copyrights abusivos e oferecer alternativas livres. Desse projeto nasceu uma nova comunidade de compartilhamento de software, iniciada com o desenvolvimento do GNU Emacs[6]. Dificuldades pela falta de um compilador[7] que fosse livre e totalmente gratuito levou

3 https://www.gnu.org/licenses
4 https://creativecommons.org/publicdomain/zero/1.0/
5 https://www.gnu.org/gnu/thegnuproject.en.html
6 https://www.gnu.org/software/emacs/
7 Compilador é um tipo de programa que traduz o código fonte para linguagem de máquina.

também ao desenvolvimento do *GNU* Compiler Collection *(*GCC), hoje muito utilizado para compilar programas em C, C++, Fortran e outras linguagens de programação [9].

Para que não houvesse interferência na distribuição dos softwares do projeto GNU, Stallman abandonou sua posição no Massachusetts Institute of Technology (MIT), assim não haveria riscos do MIT reivindicar direitos sobre seus trabalhos. Além de garantir liberdade aos usuários, o projeto GNU visava também prevenir que os softwares se tornassem proprietário posteriormente. Para isso, adotaram uma licença do tipo *copyleft* que manteria a distribuição como Software Livre de futuras versões modificadas [10].

A implementação de *copyleft* usada para a maioria dos softwares GNU é a GPL, mas há outros tipos de *copyleft* que são usados em casos específicos, como a *GNU* Free Documentation License *(*GFDL), que é utilizada em manuais do projeto GNU. O acrônimo GNU pode referir-se também ao sistema GNU/Linux, que tem como objetivo ser um sistema operacional totalmente livre. O sistema GNU apresenta inúmeras vantagens sobre outros sistemas operacionais. Do ponto de vista ético, oferece maior liberdade e cooperação para melhoria do sistema. Tecnicamente, destaca-se por questões de segurança, estabilidade e desempenho, parte disso graças ao GCC [11].

Em 1985, a Free Software Foundation (FSF) foi criada nos Estados Unidos, uma organização não governamental para o desenvolvimento de Software Livre e seu financiamento. Atualmente, há ramificações independentes da FSF em várias partes do mundo, como a Free Software Foundation Europe (FSFE) [6]. A FSF funciona através de doações, associações e pela venda de manuais sob licenças compatíveis com a GPL.

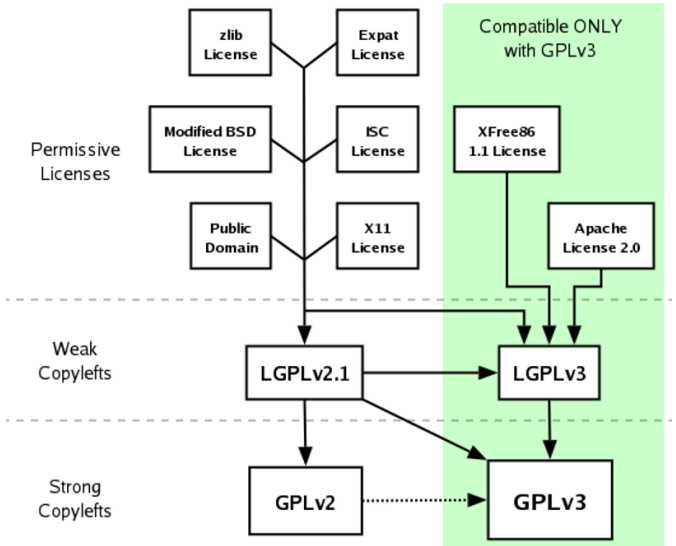

Figura 1: Exemplos de Licenças e relações com GPLv3 [12]

2.6.AS QUATRO LIBERDADES FUNDAMENTAIS

Um software pode ser considerado livre se os usuários do programa tiverem acesso às quatro liberdades fundamentais.

- USO: A liberdade de usar o programa para qualquer finalidade.
- ESTUDO: A liberdade de estudar e alterar o programa, o que pressupõe programas com código aberto.
- COMPARTILHAMENTO: A liberdade de compartilhar e distribuir cópias do programa.
- MELHORIA: A liberdade de melhorar e redistribuir o programa para a comunidade.

Essas liberdades devem ser aplicadas a qualquer software que se planeja usar ou distribuir. Considere-se, por exemplo, um programa **A** que tem como dependência um programa **B**. Distribuir o programa **A** sem modificações forçará os usuários a executarem também o programa **B**. Portanto, é necessário verificar se **A** e **B** são ambos Software Livre. Mas quando se opta por modificar o programa **A** para que não dependa do programa **B**, então apenas **A** precisaria ser Software Livre, a licença de **B** se tornaria irrelevante [13].

Software Livre também pode ser comercializado, excluir a possibilidade de uso comercial inviabilizaria o Software Livre e iria contra as quatro liberdades fundamentais. Porém, a compra do software é decisão do usuário, não pode ser imposta por monopólios ou outros meios. Há muitas empresas e projetos em Software Livre que obtêm seu faturamento através de prestação de suporte, serviços e doações [14].

2.7.DIFERENÇAS ENTRE SOFTWARE LIVRE E OPEN-SOURCE

Software Livre e *open-source* (código-aberto) descrevem categorias similares de programas, mas expressam valores e motivações diferentes. O projeto GNU utiliza o termo Software Livre para expressar a ideia de que não apenas a tecnologia implícita é importante, mas também a liberdade do usuário da tecnologia. Porém, a divulgação do Software Livre se tornou mais difícil a partir de 1998, quando uma parte da comunidade abandonou o termo Software Livre e passou a utilizar o termo *open-source*. Muitos consideravam que a mudança evitaria confusões com o nome em inglês para Software Livre, Free Software, onde a palavra ”Free” pode ser interpretada tanto como ”gratuito” quanto como ”livre” [22]. Outros optaram pelo termo *open-source* por questões comerciais e interesse em obter propriedade sobre os softwares – deixando assim de lado os princípios éticos relacionados ao Movimento Software Livre [15]. Portanto, todo Software Livre possui seu código-fonte aberto, mas nem todo software com código-fonte aberto poderá ser considerado Software Livre.

III. DIREITOS FUNDAMENTAIS E SOFTWARE LIVRE

O uso do Software Livre é indispensável para manutenção de direitos fundamentais e para o cumprimento de obrigações do Estado previstas na Constituição. Nas próximas seções se discute a importância do Software Livre para a educação, na manutenção da igualdade entre os indivíduos, na garantia da concorrência equilibrada em oposição aos monopólios, e também tratará dos problemas do uso de software proprietário em instituições públicas e governamentais.

3.1.INSTITUIÇÕES PÚBLICAS E DE ESTADO

Todos os órgãos de estado e instituições públicas deveriam utilizar exclusivamente Software Livre em seus sistemas, pois o uso de software proprietário torna o estado dependente de empresas do setor privado. Muitas empresas de tecnologia oferecem ao Estado a implantação de software e sistemas proprietários por custos muito baixos, ou até gratuitamente, visando ganhos em longo prazo ao tornar órgãos do governo dependentes da tecnologia comercializada.

No curto prazo, há cortes de gastos que trazem benefícios políticos e fiscais, mas no médio e longo prazo, quando os contratos firmados expiram, as empresas passam a cobrar por licenças e suporte dispendiosos. Nessa altura, a administração pública já não tem condições de voltar atrás, e instalar sistemas baseados em Software Livre, devido o custo para reverter bases de dados e sistemas críticos já consolidados em tecnologias proprietárias. Esse cenário leva ao aumento inesperado de despesas públicas e contraria o Artigos 105.º, Orçamento e o Artigo 106.º, Elaboração do Orçamento, da CRP.

Além dos gastos, suponha-se uma situação em que o estado depende dos sistemas fornecidos por uma empresa de tecnologia privada, e essa empresa declara falência, nesse caso o estado poderia ver-se obrigado a financiá-la para evitar a paralisação de órgãos públicos dependentes de seus serviços.

A adoção de tecnologias proprietárias por órgãos públicos ou de estado também favorece certos monopólios. Pois entidades privadas que utilizam ou integram seus sistemas aos sistemas do estado (exemplo: Finanças, Segurança Social) são indiretamente forçadas a adotar tecnologias compatíveis com as tecnologias proprietárias instaladas. Consequentemente, empresas que vencem as licitações e fornecem tecnologias ao estado acabam por expandir seu alcance e abrangência através do próprio estado.

Outra questão é a obrigação do estado em garantir a proteção dos dados dos cidadãos, conforme o Artigo 35.º, Utilização da informática, da CRP. Tecnologias proprietárias, em geral, tem seu código-fonte fechado, ao aderir a esse tipo de tecnologia o estado não tem condições de garantir que não há

irregularidades no software proprietário, como *backdoors*[8] e outras vulnerabilidades. Todos os problemas mencionados seriam facilmente superados com Software Livre. Primeiro, porque não haveria riscos de dependência e despesas inesperadas por contratos abusivos; segundo, porque os códigos-fonte dos softwares sempre estariam disponíveis para modificação e auditoria por parte do governo e entidades independentes.

3.2.MONOPÓLIO E CONCORRÊNCIA

Conforme o Artigo 81.º f), Incumbências prioritárias do Estado, e o Artigo 99.º Objetivos da política comercial, da CRP, o estado tem obrigação de garantir concorrência equilibrada entre as empresas e impedir monopólios. Mas isso não ocorre, como visto na seção anterior, o estado colabora indiretamente com o fortalecimento dos monopólios.

A Microsoft, que foi uma das pioneiras no mercado com seu sistema operacional Windows, força empresas de ramos diversos a desenvolverem softwares compatíveis somente com o Windows, além disso, ela detém os *copyrights* sobre diversas API[9] e aplicações. No mercado de jogos eletrônicos, por exemplo, a Microsoft pressiona as empresas para que desenvolvam jogos de computador compatíveis somente com Windows, para tal, os jogos tem como dependência a API DirectX, de propriedade da Microsoft. A API DirectX contém um conjunto de bibliotecas e dependências gráficas necessárias para a execução dos jogos. Usuários de outros sistemas operacionais, como o Linux, são obrigados a desenvolver aplicações que intermediam e traduzem as funcionalidades do DirectX para a API OpenGL, que é aberta. Essa etapa intermediária de tradução de uma API para outra impacta o desempenho dos jogos, o que causa a impressão de que o Linux seria inferior ao Windows, mas pelo contrário, trata-se de obstáculo colocado pela Microsoft, que detém monopólio do mercado.

Os monopólios prejudicam não somente a livre concorrência, mas também o consumidor, que se torna refém de tecnologias proprietárias. Pela falta de alternativas, o consumidor sofre abusos como a invasão de privacidade pela coleta de dados de suas atividades ao computador, *backdoors* instaladas em sistemas proprietários, que não possuem código aberto para devida auditoria, além da obsolescência programada. Todas são práticas bastante comuns por parte de grandes empresas de tecnologia como a Microsoft, Google, Apple e outras [18][19].

Sobre a obsolescência programada, essa é uma abordagem onde a empresa de tecnologia reduz artificialmente a vida útil de um software ou hardware. Houve, por exemplo, o caso da empresa de

8 Backdoor são métodos ou vulnerabilidades que permitem contornar medidas de segurança em um sistema computacional para obter acesso não autorizado.

9 API (Application Programming Interface) viabiliza ou facilita a comunicação entre programas e componentes de computador.

tecnologia Apple, que programou os aparelhos telemóveis para que ficassem progressivamente mais lentos e levassem o consumidor a trocar o dispositivo por acreditar que estaria com defeito ou no fim de sua vida útil [16]. Essa situação de desamparo do consumidor, mais uma vez, é causada por omissão do estado e descumprimento do Artigo 81.º i), Incumbências prioritárias do Estado, da CRP, que define como uma das incumbências prioritárias do estado garantir a defesa dos interesses e dos direitos dos consumidores.

3.3.EDUCAÇÃO E IGUALDADE

A liberdade de uso dos softwares desempenha um papel fundamental na educação e na disseminação do conhecimento, pois um software desenvolvido é uma forma de conhecimento, e o conhecimento é uma construção coletiva e contínua feita ao longo da história através da contribuição de todos. Portanto, não se trata de mérito exclusivo de um indivíduo. Mesmo grandes nomes da ciência, como Newton e Einstein, só alcançaram descobertas e avanços graças aos esforços daqueles que vieram antes deles.

O Artigo 43.º, Liberdade de aprender e ensinar, da CRP, garante o direito a todos de aprender e ensinar. Em uma sociedade tecnológica isso só é possível com uso de Software Livre, e não limitado por patentes nem códigos-fonte fechados, os quais não temos condições de estudar e examinar. O código-fonte aberto, e disponível para estudo, é condição suportada pelo Artigo 37.º, Liberdade de expressão e informação, da CRP. Códigos fechados são como caixas pretas, não se sabe o que está dentro, se há algo que poderia ameaçar a segurança e, novamente, impede o estudo e aprendizado sobre o código-fonte e o propósito da tecnologia.

O uso de software proprietário, além de estimular monopólios, restringe também o acesso de instituições e pessoas que não tem recursos financeiros para sua aquisição. O uso de software proprietário afronta o Artigo 13.º, Princípio da igualdade, da CRP, que trata da igualdade, a qual não pode ser alcançada se os mais pobres ficarem em desvantagem por não terem condições de pagar por softwares proprietários.

O Artigo 37.º, nº 1, Liberdade de expressão e informação, da CRP, menciona o *”direito de informar, de se informar e de ser informados, sem impedimentos e discriminações”*, e como dependemos da tecnologia para nos informarmos, o Software Livre torna-se ferramenta importante, em especial pela garantia do código fonte ser aberto. Essa necessidade é ainda reforçada pelo texto do Artigo 73.º, Educação, cultura e ciência, da CRP.

Apesar de todos esses artigos da Constituição que garantem igualdade e acesso ao conhecimento e educação, em geral, as legislações expandem e priorizam interpretações do Artigo 42.º, Liberdade de criação cultural, da CRP, que é colocado a frente de todos os direitos fundamentais mencionados

anteriormente. Nesse artigo é prevista a liberdade de criação intelectual, assim como a proteção legal dos direitos de autor, em detrimento a outras liberdades, que correspondem à igualdade e acesso ao conhecimento. O devido reconhecimento da autoria de um trabalho é essencial, desde que não torne o conhecimento propriedade de poucos e muito menos um bem hereditário. Percebe-se, portanto, que o Artigo 42.º, Liberdade de criação cultural, da CRP, se sobressai devido aos interesses financeiros, *lobbies* e monopólios.

IV. CONCLUSÃO

Hoje são dezenas de milhões de usuários de sistemas em Software Livre, usuários atraídos por razões práticas e éticas, mas o crescimento é lento devido às pressões de *lobbies* e monopólios de grandes empresas de tecnologias como: Apple, Microsoft, Google, Meta e várias outras.

Os fabricantes de hardware e software tendem a manter as especificações de seus produtos em sigilo e os códigos fechados. Isso dificulta a implementação de *drivers*, bibliotecas e dependências livres, e limita a compatibilidade entre dispositivos e sistemas de fabricantes distintos.

Entre as formas para enfrentar esses problemas há a engenharia reversa, que permite desenvolver alternativas livres com base em softwares e hardwares proprietários. Do ponto de vista técnico, a engenharia reversa poderia ser uma boa solução, mas insuficiente. As leis também precisam ser modificadas para estimular a adesão ao Software Livre por parte das instituições públicas e para mitigar/eliminar direitos de autor *leoninos*.

O Software Livre não impede a venda nem a obtenção de lucro, pelo contrário, pode ser o caminho para combater a desigualdade e estimular o desenvolvimento científico e econômico, enfraquecendo os monopólios, abrindo a concorrência e impedindo formas desleais desta.

Até no combate às mudanças climáticas o Software Livre pode ter um papel importante ao ajudar a impedir a obsolescência programada. A Obsolescência Programada leva ao descarte prematuro de dispositivos em boas condições, estimula a produção de lixo, poluição e o uso desenfreado de recursos naturais, o que não é sustentável - Artigo 66.º 2.a) e 2.d), Ambiente e qualidade de vida, da CRP. *Todos temos direito a um ambiente de vida humano, sadio e ecologicamente equilibrado*, e é obrigação do estado estimular isso através da adesão ao Software Livre e da promoção de políticas ecologicamente favoráveis - Artigo 66.º f), Ambiente e qualidade de vida, da CRP.

REFERÊNCIAS

[1] History of Copyright. Online: https://en.wikipedia.org/wiki/History_of_copyright

[2] Código do Direito de Autor e dos Direitos Conexos – CDADC. Online: https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1985-34475475

[3] Convenção da União de Berna. Online: https://pt.wikipedia.org/wiki/Convenção_da_União_de_Berna

[4] What are Dependencies in Programming. Online: https://coderslegacy.com/what-are-dependencies-in-programming/

[5] Library (Computing). Online: https://en.wikipedia.org/wiki/Library_(computing)

[6] Free Software Foundation Europe. Online: https://fsfe.org

[7] What is Copyeft. Online: https://www.gnu.org/copyleft/

[8] Study: Linux may infringe on 283 patents. Online: https://www.computerworld.com/article/2566211/study--linux-may-infringe-on-283-patents.html

[9] Richard Stallman 2022. Online: http://www.computinghistory.org.uk/det/1794/Richard-Stallman/

[10] GCC-GNU Compiler Collection. Online: https://gcc.gnu.org/

[11] The GNU Manifest. Online: https://www.gnu.org/gnu/manifesto.html

[12] A Quick Guide to GPLv3. Online: https://www.gnu.org/licenses/quick-guide-gplv3

[13] The Four Freedoms. Online: https://fsfe.org/freesoftware/index.en.html

[14] Selling Free Software. Online: https://www.gnu.org/philosophy/selling.en.html

[15] Open-source misses the point. Online: https://www.gnu.org/philosophy//po/open-source-misses-the-point.ar-en.html

[16] Apple sued over slowing phones in France, where planned obsolescence is a crime. Online: https://www.independent.co.uk/tech/apple-lawsuit-phones-slow-france-planned-obsolescence-legal-challenge-crime-a8132371.html

[17] Machine Code. Online: https://www.codecademy.com/resources/docs/general/machine-code

[18] NSA Prism program taps in to user data of Apple, Google and others. Online: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[19] XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. Online: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[20] 'The EU Copyright legislation'. Online:

https://digital-strategy.ec.europa.eu/en/policies/copyright-legislation

[21] Copyright Reform: Questions and Answers. Online:

https://digital-strategy.ec.europa.eu/en/faqs/copyright-reform-questions-and-answers

[22] The GNU Project: https://www.gnu.org/gnu/thegnuproject.en.html

CYBERLAW

BY CIJIC

METADADOS: DESAFIOS DE PRIVACIDADE E SEGURANÇA NO CONTEXTO JURÍDICO E TECNOLÓGICO

-

JOÃO MANUEL MARQUES LUCAS

RESUMO:

O presente artigo visa analisar a relação de equilíbrio que deverá existir entre a privacidade individual e as exigências da segurança interna, à luz da conservação e do acesso aos metadados.

Nesse contexto, como principal objeto de estudo, observar-se-á o enquadramento jurídico ao nível da União Europeia e de Portugal, com especial atenção aos desafios levantados pela Diretiva 2006/24/CE, bem como pela jurisprudência subsequente, como é o caso do Acórdão do Tribunal Constitucional n.º 268/2022. Abordar-se-ão questões como o problema de cruzamento dos dados, considerando-se que deverá ser garantida a privacidade individual, sendo realizada uma reflexão adequada.

Palavras-chave: Privacidade; Segurança; Metadados, Direitos Fundamentais, Dignidade Humana.

ABSTRACT

This paper aims to analyse the balance between individual privacy and the demands of internal security, in the context of data retention and access to metadata.

Within this scope, the study focuses on the legal framework of the European Union and Portugal, with particular attention to the challenges posed by Directive 2006/24/CE and subsequent case law, notably the Portuguese Constitutional Court Ruling No. 268/2022. Issues such as data correlation and the need to ensure individual privacy are examined through a critical and reflective approach.

Keywords: Privacy; Security; Metadata, Fundamental Rights, Human Dignity.

I. OBJETIVOS DO ARTIGO

No seguimento do conteúdo referido no resumo inicial, este artigo procura sobretudo, abordar 3 pilares essenciais, sendo estes os seguintes:

- Analisar a relação de privacidade e de segurança interna, no acesso aos metadados. É essencial analisar-se até que ponto se justifica o acesso aos mesmos para fins de segurança interna, podendo esses fins colocar em causa os direitos dos cidadãos, no que se referem à privacidade individual. Como principal objeto de estudo desse capítulo, observar-se-á a questão ao nível da União Europeia (numa perspetiva supranacional) e, posteriormente, de Portugal (numa perspetiva interna);
- Analisar o problema do cruzamento de dados, sendo este, um ponto relacionado com a privacidade dos cidadãos. A possibilidade de cruzamento de dados poderá colocar em causa a anonimização dos mesmos, podendo expô-los de forma indevida e indiscriminada;
- Realizar uma recensão crítica, relativa aos metadados, numa vertente informática, considerando-se a formação do autor deste artigo em Engenharia Informática e o curso de Mestrado em que este se encontra inserido.

II. INTRODUÇÃO

Com o crescente aumento das comunicações digitais, sobretudo a partir do século XXI, os metadados tornaram-se essenciais, por conterem informações com a origem e o destino das comunicações, bem como a respetiva duração e frequência. Pelo surgimento de ameaças à segurança interna das nações, como o terrorismo global, procedeu-se à utilização deste tipo de informação, permitindo a melhoria significativa das investigações e do combate ao crime.

Os metadados, consistindo em informações sobre dados e apesar de não revelarem os conteúdos contidos, permitem a avaliação de padrões comportamentais, que poderão levar a um elevado grau de intrusão. Enquanto os dados convencionais consistem em conteúdos como imagens, os metadados consistem em informações como a localização geográfica associada ao momento da captura da imagem, informações sobre o dispositivo utilizado para a captura da imagem, entre outros elementos relevantes, sobretudo quando cruzados com ferramentas de mineração de dados e de exploração de conteúdo, que utilizam ferramentas como "*exiftool*", "*pikepdf*" e "*openrefine*".

Estes poderão ainda incluir formatos de arquivo, métodos de compactação, locais de armazenamento e detalhes de criptografia, além de poderem ser subdivididos entre descritivos, estruturais, administrativos, técnicos e estatísticos.

Conforme referido por Brízida Castro[1], "*os metadados são dados de tráfego, dados funcionais necessários ao estabelecimento de uma comunicação, como os que permitem a localização do destinatário, a duração da utilização, data e hora, frequência, etc.*".

Torna-se, por isso, fundamental proceder-se a uma reflexão que permita uma análise no que concerne à legitimidade da obtenção dos metadados, especialmente quando se encontra enquadrada em medidas indiscriminadas e preventivas. Dessa forma, procurar-se-á analisar a relação existente entre a segurança interna e a proteção da privacidade dos cidadãos, incorporando-se uma perspetiva crítica e técnica.

III. ENQUADRAMENTO HISTÓRICO DOS METADADOS

O conceito de "*Metadado*" surgiu da necessidade de se proceder à obtenção de informações contidas nos dados primários, que permitissem a identificação e organização de processos de análise, de uma forma mais eficiente.

A evolução deste conceito apenas se tornou possível devido ao desenvolvimento tecnológico que ocorreu em larga escala nas últimas décadas do século XX, fortemente marcado pela digitalização generalizada da informação e crescimento abrupto da internet e dos sistemas de informação. Com este progresso, a criação automática de metadados ocorreu praticamente em todas as formas de comunicação digital.

Por outro lado, as empresas de telecomunicações começaram a gerir e a armazenar (meta)dados em larga escala, através de centrais de processamento de dados (data centers), baseados em sistemas de armazenamento e registo tais como "*Data Warehousing*" e "*Data Mart*".

A partir dessa altura, os metadados constituíram-se como um recurso estratégico fundamental, não apenas pelos seus fins comerciais e operacionais, mas também pela sua utilidade em domínios da segurança nacional e investigação criminal, permitindo às autoridades, quando autorizadas, procederem ao rastreamento de comunicações e atividades suspeitas.

1 Direito Constitucional: Ciberespaço e Tecnologia - Declínio do Constitucionalismo na UE?, Raquel Brízida Castro, Capítulo I, Secção II, Página 57

Mais recentemente, com o surgimento acentuado da inteligência artificial, tornou-se possível a exploração de metadados que permitam que seja realizada a identificação de correlações e o perfilar de determinados indivíduos de uma forma mais célere e eficaz.

IV. A RELAÇÃO ENTRE A PRIVACIDADE E A SEGURANÇA INTERNA NO ACESSO A METADADOS

A relação entre a privacidade e a segurança interna, no acesso a metadados tem sido um tema de debate ao longo dos anos. Isto porque, torna-se difícil, em determinadas circunstâncias, garantir-se um equilíbrio entre a privacidade e a segurança interna. Como principal objeto de estudo deste capítulo, observar-se-á esta questão ao nível da UE e de Portugal.

Em 2006, com o aumento das ameaças à segurança interna dos estados-membros da UE, por força da ameaça crescente de terrorismo que se ia consolidando a nível internacional, foi aprovada a Diretiva 2006/24/CE, que definia que os dados (metadados), deveriam ficar retidos e conservados por períodos não inferiores a 6 meses e não superiores a 2 anos, de acordo com o artigo 6º, além de definir que os estados-membros deveriam tomar medidas de modo a garantirem a sua conservação (artigo 3º, 1º).

O fornecimento desses metadados deveria ser realizado de acordo com legislação do próprio país (artigo 4º). Os metadados em questão incluíam contactos telefónicos, hora e duração de chamadas e endereços IP dos telemóveis utilizados. Com base nessa Diretiva, os metadados poderiam ser acedidos como forma de combate ao terrorismo e em parte, ao crime organizado.

Anos mais tarde, uma empresa irlandesa de defesa dos direitos digitais, denominada *Digital Rights Ireland Ltd*, iniciou uma ação judicial contra a lei irlandesa, alegando que a retenção e a conservação indiscriminada de metadados violava o direito à proteção dos dados pessoais (artigo 8.º), constante na Carta dos Direitos Fundamentais da União Europeia (CDFUE). A ação judicial em questão foi submetida ao Tribunal de Justiça da União Europeia, que procedeu à reavaliação da Diretiva em questão.

Através do Acórdão Digital Rights Ireland, o TJUE declarou a invalidade da Diretiva 2006/24/CE, alegando que a retenção generalizada e indiscriminada constituía uma interferência sobre direitos fundamentais[2], indicados na ação judicial.

A invalidade da Diretiva foi objeto de comentário por Duarte Rodrigues Nunes[3], em que, segundo este, a "*conservação dos dados referidos na Diretiva e o acesso das autoridades a esses dados restringem,*

2 Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") – Universidade do Minho - Repositorium

3 Revista do Ministério Público - 170, Abril, Junho, 2022, Duarte Rodrigues Nunes, Págs. 19, 20 e 21

de forma intensa (embora sem afetar o seu conteúdo essencial), os direitos tutelados pelos artigos 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 reconhecidos por esta deve ser prevista na lei, respeitando o conteúdo essencial desses direitos e liberdades (…), só podem ser introduzidas restrições a esses direitos e liberdades se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros. E, nessa conformidade, 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 restringe, de forma desproporcionada, os mencionados direitos fundamentais, uma vez que:

> *a) abrange, de uma forma indiscriminada, todas as pessoas que, utilizam serviços de comunicações eletrónicas, incluindo, por isso, pessoas em relação às quais não existem indícios de que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com infrações graves e não prevendo qualquer exceção quanto a pessoa cujas comunicações estejam abrangidas pela proteção de segredo profissional;*
>
> *b) não exige nenhuma relação entre os dados cuja conservação está prevista e uma ameaça para a segurança pública nem limita a conservação a dados relativos a um período de tempo e/ou a uma zona geográfica determinada e/ou a um círculo de pessoas determinadas que possam estar implicadas, de uma maneira ou de outra, numa infração grave, nem de dados relativos a pessoas, cuja conservação, por outros motivos, pudesse contribuir para a prevenção, a deteção ou a repressão de infrações graves;*
>
> *c) não estabelece critérios objetivos que permitam delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior para prevenir, detetar ou agir penalmente contra infrações suscetíveis de ser consideradas suficientemente graves à luz da amplitude e da gravidade da ingerência dos direitos fundamentais consagrados nos artigos 7.º e 8.º, da CDFUE (…).*".

A nível nacional, a declaração de invalidade desta Diretiva teve impacto, sendo Portugal um estado-membro da União Europeia. O Tribunal Constitucional, em consonância com a decisão do TJUE, passou a adotar uma abordagem mais cuidadosa, exigindo que a retenção de dados fosse adequadamente fundamentada e justificada.

O Decreto-Lei n.º 32/2008, de 17 de julho de 2008, que permitia a retenção de dados pelas empresas de telecomunicações, para fins de investigação criminal, foi considerado inconstitucional, através do Acórdão n.º 268/2022, por violar princípios constitucionais. Segundo informação constante no Acórdão referido, esta decisão deveu-se sobretudo ao facto de "*sujeitos relativamente aos quais não*

há qualquer suspeita de atividade criminosa: abrangem-se as comunicações eletrónicas da quase totalidade da população, sem qualquer diferenciação, exceção ou ponderação face ao objetivo perseguido[4]". A principal questão será o facto de a invalidade desta diretiva poder colocar em causa a segurança interna, na luta contra o terrorismo e contra o crime organizado.

Rodrigues Nunes[5] abordou esta questão no seu capítulo escrito, na revista do Ministério Público, em que, segundo ele, é "*certo que o TC – embora de uma forma completamente desproporcionada e desrazoável – considerou que o artigo 9.º da Lei n.º 32/2008 é inconstitucional em virtude de não estar prevista a obrigatoriedade da 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 ou integridade física de terceiros. Todavia, tal poderá ser colmatado por via de, apesar de a lei não prever, a autoridade judiciária notificar as pessoas cujos metadados tenhas sido acedidos logo que essa notificação não seja suscetível de comprometer as investigações (quer a investigação naquele processo quer noutros processos) nem a vida, integridade física ou a liberdade (incluindo a liberdade e a autodeterminação sexual) de terceiros, assim se afastando este argumento na eventualidade de um recurso para o TC em sede de fiscalização concreta*".

Ainda no contexto da relação entre a privacidade e a segurança interna, importa referir um caso prático em que existiu uma falta de equilíbrio evidente. Em determinado período, o Ministério Público solicitou, ao Juiz de Instrução Criminal, o acesso a uma lista em formato digital e a um Excel, contendo todos os cartões SIM, relativos às empresas de telecomunicações MEO, Vodafone e NOS, que operaram entre as 01H45 do dia 25 de abril de 2015 e as 02H30 do dia 09 de Janeiro de 2016[6], em áreas de abrangência de 19 antenas em Cascais, sendo abrangidas zonas como a praia de Cascais e a zona centro, *erga omnes* os cartões SIM que estivessem ativos em telemóveis ligados no dia 09 de janeiro de 2015.

Esta solicitação realizada pelo Ministério Público procurava encontrar informações relevantes sobre uma investigação relativa a um roubo agravado (previsto e punido pelo disposto no artigo 210.º, nºs 1 e 2, alínea b, do Código Penal) e à prática de um crime de deteção de arma proibida (previsto e punido pelo artigo 86º, do Regime Jurídico das armas e suas munições), no dia 09 de janeiro de 2016, pelas 02H30, num interior de uma residência em Cascais.

De forma a justificar a solicitação, o Ministério Público sublinhou "*a gravidade do crime cometido*" e "*a indispensabilidade da diligência (...) sendo única e exclusivamente junta aos autos a informação*

4 Acórdão n.º 268/2022, do Tribunal Constitucional
5 Revista do Ministério Público - 170, Abril, Junho, 2022, Duarte Rodrigues Nunes, Págs. 47, 48 e 49
6 Acórdão do Tribunal da Relação de Lisboa, III – Decisão, Ponto 1, Bases Jurídico-Documentais: IGFEJ

pertinente para a investigação."[7]. O Tribunal da Relação de Lisboa (TRL) recusou a solicitação, argumentando que não existiam alvos concretos ou suspeitos identificados, considerando-se que não era possível determinarem-se os suspeitos de crime ou roubo, sendo necessário que se tratasse de uma pessoa concreta, determinável passível de individualização.

No processo, a solicitação ao acesso de metadados de forma generalizada foi comparada a redes de pesca, em que se "apanham" não apenas peixes nessas redes, mas também moluscos e crustáceos, além de "lixo" e espécies protegidas e/ou ameaçadas de extinção[8]. A solicitação foi então recusada. Após o Ministério Público ter recorrido da decisão, os Juízes da 9ª Secção Criminal da Relação de Lisboa, a 22 de junho de 2016, decidiram negar o ratio interposto, confirmando-se integralmente a decisão recorrida.

O caso prático dos Cartões SIM, ocorrido em Cascais, mostra como a possibilidade de desequilíbrio entre a segurança e a privacidade dos cidadãos poderá existir, mesmo que seja para fins de combate ao crime organizado. Embora a segurança pública seja uma preocupação legítima, a retenção de dados deve seguir princípios de proporcionalidade e de necessidade, devendo ser limitada a circunstâncias muito específicas, como *verbi gratia*, investigações de crimes graves, em que se possa determinar, de forma objetiva, o(s) autor(es) de determinado crime.

O próprio TJUE afirmou que a retenção de dados em grande quantidade, sem distinção entre suspeitos e cidadãos comuns, não é proporcional nem justificável, de acordo com os direitos fundamentais promulgados. O princípio da proporcionalidade deverá ser essencial, garantindo o fino e delicado equilíbrio desta relação, já abordada.

V. O PROBLEMA DO CRUZAMENTO DE (META)DADOS

Este capítulo procura aprofundar o problema do cruzamento de dados, estando relacionado com a privacidade dos cidadãos. A possibilidade de cruzamento de dados poderá colocar em causa a anonimização dos mesmos, podendo expô-los de forma indevida e indiscriminada. Existem por isso riscos jurídicos associados e potenciais implicações técnicas de privacidade.

O cruzamento de dados, através da integração de diferentes fontes de informação, poderá levar à identificação de padrões comportamentais e à possibilidade de se poder inferir correlações existentes. Esta questão poderá ser útil em casos específicos, como a investigação de crimes de burla financeira

7 Revista Cyberlaw, Centro de Investigação Jurídica do Ciberespaço, Faculdade de Direito da Universidade de Lisboa, Edição nº11, Março de 2021, 1. Introdução, Página 94

8 Acórdão do Tribunal da Relação de Lisboa, I, Bases Jurídico-Documentais: IGFEJ

ou de burla informática, porém, poderá colocar em causa os direitos, liberdades e garantias dos cidadãos.

Através do cruzamento de dados, torna-se, por isso, possível, proceder-se à reconstrução de rotinas diárias e de hábitos individuais e comuns, com base no conceito de "*profiling*", levantando-se questões relacionadas com a proteção de dados pessoais e a autodeterminação informativa.

O problema torna-se ainda mais robusto quando os dados são filtrados por sistemas de inteligência artificial e de aprendizagem automática, com elevada eficiência e precisão. Recomenda-se, por isso, a minimização, pseudonimização e encriptação dos dados, com base nos limites de privacidade que devem ser garantidos.

Embora o cruzamento de dados possa ser útil para a segurança nacional, e consequentemente, para o Estado, "*O Direito está fora do Estado porque é criado por jurisprudentes com auctoritas e – condição sine qua non – sem imperium*.", segundo Vera-Cruz Pinto[9].

Assim, o cruzamento de metadados, embora seja útil em determinadas circunstâncias, deverá ser adequado aos princípios da necessidade e da proporcionalidade, garantindo-se que a segurança não seja uma constante justificativa para a erosão sistemática da privacidade.

VI. RECENSÃO CRÍTICA

A recensão crítica apresentada é desenvolvida a partir de uma perspetiva técnica, conjugando os fundamentos jurídicos analisados ao longo do artigo com uma visão informática, justificada pela formação académica do autor (Engenharia Informática), bem como pela sua frequência no Mestrado em Segurança de Informação e Direito no Ciberespaço.

A proteção e o tratamento dos metadados, enquanto dados que contextualizam, descrevem e facilitam a recuperação de informações, exigem soluções técnicas adequadas e robustas, sobretudo quando se encontra em causa a sua utilização por entidades públicas para fins de investigação criminal ou soberania nacional.

Segundo Brízida Castro[10] e de acordo com Duarte Rodrigues Nunes[11], de forma implícita, deverá existir o bom senso na utilização dos metadados, devendo estes serem consultados de forma justificada e em circunstâncias muito específicas.

---

9 Introdução ao estudo do Direito Romano - As questões Fundamentais, Eduardo Vera-Cruz Pinto, Capítulo I - O Direito Romano como Origem do Jurídico, Ponto 13 - O Estado de Direito pode ser apenas o Direito do Estado?, Página 57, 2º Parágrafo

10 Direito Constitucional: Ciberespaço e Tecnologia - Declínio do Constitucionalismo na UE?, Raquel Brízida Castro

11 Revista do Ministério Público - 170, Abril, Junho, 2022, 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?*"

Por outro lado, é fundamental a garantia da segurança de informação, através de mecanismos informáticos, tais como algoritmos criptográficos (por exemplo), que assegurem os princípios de confidencialidade, integridade e disponibilidade.

Assim, deverão ser implementadas (medidas) técnicas robustas de segurança de informação, nomeadamente:

- Encriptação ponto a ponto (E2EE), para dados em trânsito e em repouso, com algoritmos atualizados e resistentes a ataques criptográficos;
- Controlo de acessos baseado em perfis de utilizador, reforçado pela autentificação multifator;
- Implementação de auditorias regulares a entidades gestoras de dados, como empresas de telecomunicações, de modo a garantir a conformidade legal;
- Implementação de ferramentas SIEM (Security Information and Event Management), que permitam a deteção e a resposta a incidentes de forma célere.

Estes mecanismos não substituem a necessidade de controlo jurisdicional, mas constituem, numa vertente informática, o alicerce técnico que permite a concretização de garantias previstas pela lei portuguesa.

Assim, esta recensão crítica propõe que o debate jurídico sobre o acesso aos metadados seja acompanhado de uma exigência técnica mínima que torne efetiva a proteção da privacidade dos cidadãos e a salvaguarda dos seus direitos fundamentais. Apenas com a conjugação entre o direito e a tecnologia será possível atingir-se um equilíbrio real entre a segurança e a liberdade individual.

VII. CONCLUSÕES E COMENTÁRIO PESSOAL

A crise dos metadados, sobre a qual nos debruçamos, exige um equilíbrio fino, delicado e proporcional, entre a privacidade dos cidadãos e a segurança interna. A questão central que aqui se coloca é determinar o ponto exato em que o acesso a metadados se justifica para combater o crime organizado e garantir a segurança do Estado. É fundamental que, ao fazê-lo, se assegurem os direitos, liberdades e garantias dos cidadãos. Em última instância, a proteção destes direitos é o que sustenta e promove a saúde da democracia e o Estado de direito democrático, princípios estruturantes da República Portuguesa e assim consagrados nos artigos 1º e 2º da sua Constituição (CRP).

Seguindo as considerações da Brízida Castro, os metadados deverão encontrar-se "*consensualmente, protegidos pelo sigilo das comunicações, estabelecendo a Constituição, na sua versão atual, apenas uma exceção a essa proibição: essa ingerência é possível apenas em processo*

criminal. E, mesmo em processo penal, de acordo com a nossa jurisprudência, como veremos, o juiz de instrução só autoriza o acesso pelo Ministério Público a metadados de suspeitos determinados ou determináveis, perante a notícia de um crime."[12].

Foi ainda abordado o problema do cruzamento de dados, considerando-se os eventuais efeitos negativos deste, além da realização de uma breve recensão crítica, que procurou comentar, através de uma visão informática, o que se considera ser essencial, em termos tecnológicos, relativamente aos metadados.

Ao nível do comentário pessoal, o autor deste artigo apresenta a sua preocupação relativamente à garantia das liberdades e direitos dos cidadãos, na relação de equilíbrio entre a privacidade e a segurança interna, conforme já mencionado anteriormente, devendo esse equilíbrio ser baseado no Direito.

Como forma de conclusão, citando-se Vera-Cruz Pinto, *"(...) não são leis, costumes, doutrinas e sentenças as fontes de Direito; é o Direito que é a fonte de leis, costumes, doutrinas e sentenças.*" [13]

12 Direito Constitucional: Ciberespaço e Tecnologia - Declínio do Constitucionalismo na UE?, Raquel Brízida Castro, Capítulo I, Secção II, Página 57

13 Introdução ao estudo do Direito Romano - As questões Fundamentais, Eduardo Vera-Cruz Pinto, Capítulo I - O Direito Romano como Origem do Jurídico, Ponto 13 - O Estado de Direito pode ser apenas o Direito do Estado?, Página 57, 1º Parágrafo

BIBLIOGRAFIA

[1] Livro Direito Constitucional - Ciberespaço e Tecnologia - Declínio do Constitucionalismo na UE?, Raquel Alexandra Brízida Castro;

[2] Revista do Ministério Público, - 170, Abril, Junho, 2022, 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?, Capítulo escrito pelo Duarte Rodrigues Nunes;

[3] Introdução ao estudo do Direito Romano - As questões Fundamentais, Eduardo Vera-Cruz Pinto;

[4] Repositorium, Universidade do Minho;

[5] Acórdãos, Tribunal Constitucional;

[6] dgsi.pt, Bases Jurídico-Documentais;

[7] Revista Cyberlaw, Centro de Investigação Jurídica do Ciberespaço, Faculdade de Direito da Universidade de Lisboa.

REFERÊNCIAS

[1] Direito Constitucional: Ciberespaço e Tecnologia - Declínio do Constitucionalismo na UE?, Raquel Brízida Castro, Capítulo I, Secção II, Página 57;

[2] Silveira, A., & Freitas, P. M. (2017). The Directive 2006/24 declaration of invalidity and the consequences of metadata retention in the EU Member States: A Fundamental Rights Standards Approach. Law State and Telecommunications Review, 9(1), 47–68. Universidade do Minho – Repositorium - https://repositorium.sdum.uminho.pt/bitstream/1822/65466/1/21513-Article%20Text-37908-2-10-20190411.pdf;

[3] Revista do Ministério Público - 170, Abril, Junho, 2022, Capítulo 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?, Duarte Rodrigues Nunes, Págs. 19, 20 e 21;

[4] TC > Jurisprudência > Acórdãos > Acórdão 268/2022 . (2022). Tribunalconstitucional.pt. https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html;

[5] Revista do Ministério Público - 170, Abril, Junho, 2022, Duarte Rodrigues Nunes, Págs. 47, 48 e 49;

[6] Acórdão do Tribunal da Relação de Lisboa, III – Decisão, Ponto 1, Bases Jurídico-Documentais: IGFEJ. https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/916a3f11e71847c780257fdf004f7f74?OpenDocument;

[7] Revista Cyberlaw, Centro de Investigação Jurídica do Ciberespaço, Faculdade de Direito da Universidade de Lisboa, Edição nº11, Março de 2021, 1. Introdução, Página 94 https://www.iuris.edu.pt/xms/files/Cyberlaw-by-CIJIC_11.pdf;

[8] Acórdão do Tribunal da Relação de Lisboa, I, Bases Jurídico-Documentais: IGFEJ. https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/916a3f11e71847c780257fdf004f7f74?OpenDocument;

[9] Introdução ao estudo do Direito Romano - As questões Fundamentais, Eduardo Vera-Cruz Pinto, Capítulo I - O Direito Romano como Origem do Jurídico, Ponto 13 - O Estado de Direito pode ser apenas o Direito do Estado?, Página 57, 2º Parágrafo;

[10] Direito Constitucional: Ciberespaço e Tecnologia - Declínio do Constitucionalismo na UE?, Raquel Brízida Castro;

[11] Revista do Ministério Público - 170, Abril, Junho, 2022, 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?;

[12] Direito Constitucional: Ciberespaço e Tecnologia - Declínio do Constitucionalismo na UE?, Raquel Brízida Castro, Capítulo I, Secção II, Página 57;

[13] Introdução ao estudo do Direito Romano - As questões Fundamentais, Eduardo Vera-Cruz Pinto, Capítulo I - O Direito Romano como Origem do Jurídico, Ponto 13 - O Estado de Direito pode ser apenas o Direito do Estado?, Página 57, 1º Parágrafo.

CYBERLAW

BY CIJIC

SEGURANÇA DE INFORMAÇÃO NAS ORGANIZAÇÕES: A IMPORTÂNCIA DA FORMAÇÃO DOS COLABORADORES

ANA CATARINA TAVARES FARINHAS [1]

1 Mestranda em Segurança de Informação e Direito no Ciberespaço no Instituto Superior Técnico e Faculdade de Direito da Universidade de Lisboa e Escola Naval; Licenciada em Engenharia Mecânica.

RESUMO:

A transformação digital redefiniu o panorama económico global, impulsionada pela digitalização e pela conectividade, que assumiram ainda maior relevância durante a pandemia de COVID-19. Este trabalho analisa o impacto crescente das ameaças associadas ao fator humano, com um foco particular no contexto empresarial.

A análise sublinha a importância da formação dos colaboradores como uma estratégia essencial para mitigar ataques de engenharia social, como o phishing, reconhecendo o fator humano como uma das principais vulnerabilidades na segurança da informação. Para promover a consciencialização, são apresentadas estratégias práticas e diversificadas, incluindo vídeos, jogos interactivos e formações presenciais, destacando os benefícios de uma abordagem integrada.

Conclui-se que a capacitação contínua dos colaboradores é indispensável para fomentar uma cultura organizacional centrada na segurança e na resiliência face às ciberameaças, contribuindo para a proteção efectiva das organizações num cenário digital cada vez mais desafiante.

Palavras-chave: Transformação digital, Cibersegurança, Engenharia social, Phishing, Fator humano, Formação de colaboradores, Mitigação de ameaças, Segurança de informação.

ABSTRACT:

The digital transformation has redefined the global economic landscape, driven by digitization and connectivity, which gained even greater prominence during the COVID-19 pandemic. This paper analyses the growing impact of threats associated with the human factor, with a particular focus on the business context.

The analysis underscores the importance of employee training as an essential strategy to mitigate social engineering attacks, such as phishing, recognizing the human factor as one of the primary vulnerabilities in information security. To promote awareness, practical and diversified strategies are presented, including videos, interactive games, and in-person training, highlighting the benefits of an integrated approach.

It concludes that the continuous empowerment of employees is indispensable for fostering an organizational culture centred on security and resilience in the face of cyber threats, contributing to the effective protection of organizations in an increasingly challenging digital scenario.

Keywords: Digital transformation, Cybersecurity, Social engineering, Phishing, Human factor, Employee training, Threat mitigation, Information security.

I. INTRODUÇÃO

Ao longo da última metade do século XX, assistiu-se a uma rápida evolução tenológica, permitindo que sociedades gerassem elevados índices de crescimento económico e social, e desencadeando o desenvolvimento e adoção de novas Tecnologias de Informação e Comunicação (TIC).

Em particular, a pandemia de COVID-19, um acontecimento notável e sem precedentes, intensificou esta evolução, alterando a forma como milhares de milhões de cidadãos vivem, trabalham e comunicam entre si, e obrigando empresas de todo o mundo a adotarem soluções digitais, como o trabalho remoto e o comércio online, de forma a garantir a continuidade dos negócios.

Dando um especial foco ao contexto empresarial, este acontecimento trouxe uma série de fatores positivos, mas também uma série de desafios principalmente no que diz respeito à cibercriminalidade. Uma vez que grande parte dos incidentes de segurança resulta de falhas humanas, sejam estas acidentais ou intencionais, foi necessária uma adaptação rápida e uma consciencialização continua não apenas de membros em cargos superiores, mas também de todos os colaboradores.

II. PANORAMA ATUAL

O relatório *Threat Landscape 2024* elaborado pela Agência da União Europeia para a Cibersegurança (ENISA) destaca descobertas sobre o mais recente panorama de ameaças à cibersegurança, mais especificamente entre julho 2023 e junho 2024.

De acordo com a análise realizada pelo ETL, em 2024, à semelhança do ano anterior destacaram-se sete ciberameaças principais, nomeadamente Malware, Information manipulation, Ransomware, Supply-chain attacks, Threat against Data, Threats againt avaiability e Social engineering attacks.

No seguimento desta análise, o relatório mostra também a distribuição de incidentes, em percentagem, por tipo de ameaça em 2024, figura 1. É possível observar que o DOS (Denial of Service) lidera com uma percentagem de 41,1, na segunda posição encontra-se o Ransomware com 25,79 %, na terceira Data com 19,01 e na quarta, mas não menos importante, Social Engineering. Comparativamente ao cenário de 2023, observa-se uma troca posições evidente entre DOS e Ransomware, Figura 2, enquanto as restantes, apesar de algumas permutações, permanecem com percentagens semelhantes às do ano anterior.

Se quisermos fazer uma comparação num período de tempo superior, por exemplo, 2014, verifica-se que a maioria das ameaças de hoje já estavam presentes há 10 anos atrás. Ao longo destes 10 anos observámos uma grande evolução da tecnologia, especialmente nos anos seguintes à pandemia

COVID-19, e uma crescente preocupação e, por consequência, exploração de áreas como a segurança de informação e cibersegurança. No entanto, os atores do crime acompanharam essa evolução, permitindo que as principais ameaças de 2014 continuassem relevantes até aos dias de hoje.

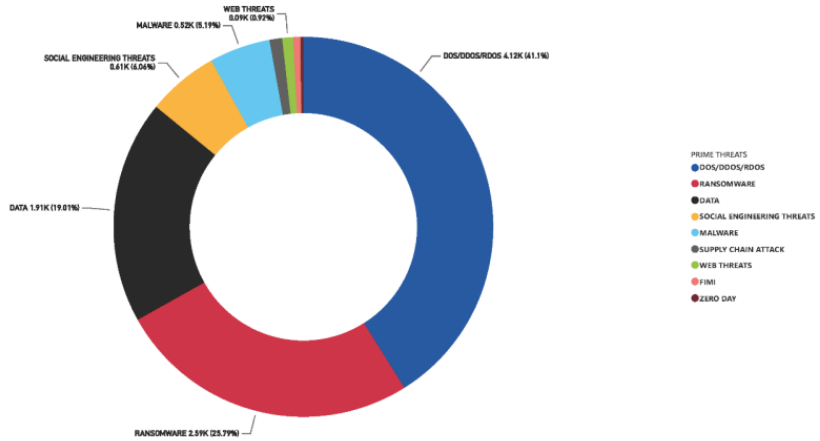

Figura 2-Ditribuição de incidentes por tipo de ameaça 2024.

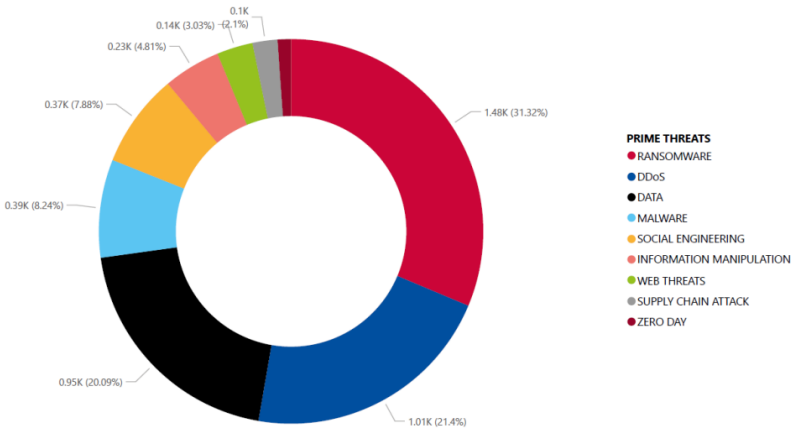

Figura 2-Ditribuição de incidentes por tipo de ameaça 2023.

Durante o período em análise, 2023/2024, no panorama europeu, observou-se um elevado número de incidentes direcionados a organizações dos setores da administração pública (19%), transporte (11%) e financeiro (9%). Incidentes direcionados à infraestrutura digital (8%) e aos serviços empresariais também constituem uma parte substancial dos eventos observados, Figura 3.

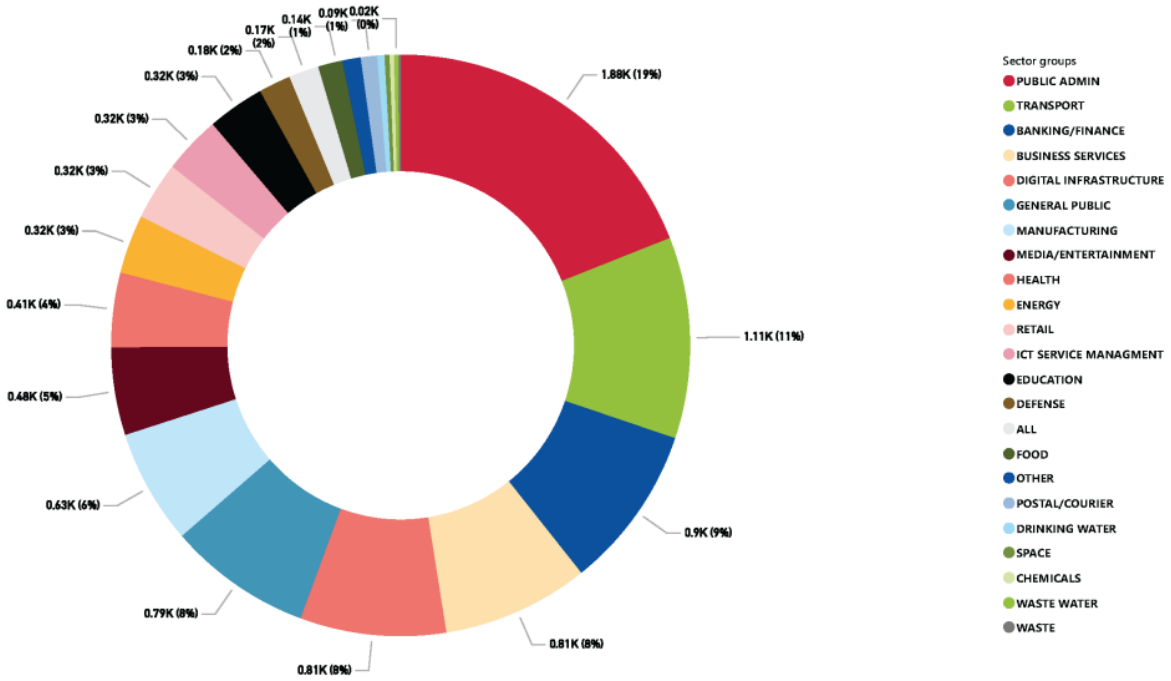

Figura 3- Setores-alvo por número de incidentes (julho de 2023 a junho de 2024).

Adicionalmente, verificou-se um número considerável de incidentes dirigidos à sociedade civil, não necessariamente a um setor específico (estes são classificados como 'Público Geral' e representam 8% dos incidentes observados).

Apesar de não ser a número 1 ameaça segundo o ETL, as técnicas de engenharia social foram consideradas pelo relatório como um vetor de entrada eficaz para outros tipos de ciberameaças.

Entre os principais vetores de ataque de engenharia social encontram-se o *phishing, spear-phishing, whaling, smishing, vishing,* ataques de *watering hole, baiting, pretexting, quid pro quo, honeytraps* e *scareware*. Estes métodos são frequentemente utilizados para obter acesso inicial aos sistemas, criando um ponto de entrada para ataques mais sofisticados, como , por exemplo, o *ransomware*.

A dependência do elemento humano torna a engenharia social uma técnica extremamente perigosa, pois combina persuasão psicológica com exploração técnica, permitindo aos atacantes contornar defesas tecnológicas mais robustas. No contexto empresarial o comprometimento de e-mail (BCE) é uma das principais consequências destas técnicas, comumente o atacante recorre o *pretexting* ao utilizar cadeias de e-mails existentes para convencer uma vítima a realizar uma ação.

Assim esta análise leva-nos a crer que sensibilizar os utilizadores/colaboradores e implementar boas práticas de segurança são essenciais para garantir a segurança de informação .

Apesar de não ser o principal objeto de análise, não poderíamos deixar de fazer uma breve análise do panorama atual nacional com base no Relatório Riscos e Conflitos elaborado pelo Centro Nacional de Cibersegurança (CNCS).

De acordo com o relatório observou-se um aumento da criminalidade informática no ciberespaço de interesse nacional em 2023. Destacaram-se como as ciberameaças mais relevantes o Ransomware, o Phishing e Smishing, outras Técnicas de Engenharia Social, Burlas Online e Comprometimento de contas.

Figura 4- Top 5 Ciberameaças em Portugal 2023.

Os setores e áreas governativas com mais incidentes registados pelo CERT.PT (Computer Emergency Response Team) em 2023 foram os Prestadores de Serviços de Internet (26% do total), a Banca (10%) e a Saúde (8%). Os Prestadores de Serviços de Internet e a Saúde subiram registaram um aumento significativo face a 2022, 249% e 106%, respetivamente (CERT.PT). Ainda assim as vítimas mais afetadas por ciberataques em 2023 foram, mais do que setores em particular, os indivíduos e as pequenas e médias empresas (PME), sobretudo enquanto alvos de *phishing, smishing*, outras formas de engenharia social e burlas online.

À semelhança do relatório anterior, também este reforça a importância das técnicas de Engenharia Social, em particular o *Phishing/Smishing* como vetores de entrada para outras ameaças, afirmando que "*Em algumas situações de phishing, smishing e outras formas de engenharia social foram capturados dados das vítimas, como credenciais de acesso a contas, que poderão ter contribuído para uma outra ciberameaça relevante, o comprometimento de contas, a partir da qual diversas ações maliciosas podem ocorrer, como o ransomware ou o envio de emails fraudulentos*." e que "*Na realidade, algumas das ciberameaças relevantes estão necessariamente correlacionadas entre si*.".

Para terminar, o CNCS disponibilizou o que se prevê serem as tendências para o futuro, nomeadamente, exploração vulnerabilidades "dia 0", mencionada no Top ciberameaças no ETL, pouco reconhecida em Portugal, Aumento das infeções através de *pen* USB, novamente um ataque ao fator humano, desta vez no meio físico, Risco de cibersabotagem e hacktivismo, de extrema importância dado o contexto geopolítico atual, Potenciar do cibercrime por via de um maior uso de criptomoedas, Mais desinformação com conteúdos de IA generativa, novamente um possível ataque ao fator humano, a utilização de inteligência artificial em técnicas de engenharia social poderá aumentar a complexidade destas e por consequência a dificuldade dos utilizadores em detetar conteúdo falso, por fim Persistência de ameaças que exploram o factor humano, bem como *ransomware* e *infostealers*.

Figura 5- Tendências para o futuro.

Posto isto, é evidente o impacto da Engenharia social no panorama atual de cibersegurança, em particular no meio empresarial. Nos próximos capítulos iremos aprofundar estas técnicas e mostrar através de estudos realizados como uma formação eficaz dos colaboradores reduz a ocorrência das mesmas.

III. ENGENHARIA SOCIAL

Engenharia social é um conjunto de técnicas de manipulação psicológica utilizadas por atacantes para explorar o fator humano, frequentemente considerado o elo mais fraco em qualquer sistema de segurança. O objetivo é induzir pessoas a cometerem erros, como partilhar informações confidenciais, realizar ações específicas ou comprometer sistemas e redes, muitas vezes por motivos ilícitos.

A sua eficácia reside na exploração de comportamentos humanos, como confiança excessiva, medo, curiosidade ou distração, tornando-a uma das principais causas de compromissos de segurança atualmente.

De uma forma geral podemos definir as técnicas de Engenharia Social destacadas pelo relatório ENISA Threat Landscape e pelo Relatório Riscos & Conflitos elaborado pelo CNCS no que diz respeito ao panorama atual e três outras, *Quishing*, *AI Phishing* e *Hybrid Vishing*, destacadas pela IBM como tendências futuras da seguinte forma:

***Phishing* por E-mail**: Consiste no envio massivo de e-mails fraudulentos que aparentam ser de fontes confiáveis, como bancos ou empresas conhecidas. O objetivo é induzir o destinatário a fornecer informações sensíveis, como credenciais de login ou dados financeiros, ou a clicar em links maliciosos que podem instalar malware.

***Smishing* (*Phishing* por SMS)**: Utiliza mensagens de texto (SMS) fraudulentas para induzir as vítimas a clicar em links maliciosos ou a fornecer informações pessoais. As mensagens frequentemente alegam ser de fontes confiáveis e podem conter alertas urgentes para pressionar a vítima a agir rapidamente.

***Vishing* (*Phishing* por Voz)**: Envolve o uso de chamadas telefónicas para enganar as vítimas, levando-as a divulgar informações pessoais ou financeiras. Os atacantes podem fazer-se passar por representantes de instituições legítimas, como bancos ou entidades governamentais.

Spear Phishing: Uma forma mais direcionada de phishing, onde o atacante foca em indivíduos ou organizações específicas. Utiliza informações personalizadas sobre a vítima para tornar a fraude mais convincente, aumentando a probabilidade de sucesso[1].

Spoofing: Consiste na falsificação de informações, como o endereço de e-mail, número de telefone ou URL, para se fazer passar por uma fonte confiável, facilitando ataques como *phishing* ou *vishing*.

Whaling: Uma variante do *spear phishing* que tem como alvos indivíduos em posições de poder dentro de uma organização. O objetivo é obter acesso a informações confidenciais ou autorizações financeiras significativas.

---

1 Um caso de *spear phishing* realizado com sucesso foi o da captura de credenciais da conta de John Podesta, na altura, gestor da campanha de candidatura à presidência dos Estados Unidos de Hillary Clinton. De acordo com a CBS News, Podesta recebeu na sua caixa de correio um alerta relativo a um acesso ilegítimo à sua conta, proveniente de um país estrangeiro, o qual incluía um link, através do qual a palavra-passe poderia ser reposta. Por precaução, o gestor de campanha consultou o suporte IT, através da sua assistente, que reencaminhou o email original para os técnicos. Estes, afirmando a legitimidade da mensagem, sugeriram não só a reposição da palavra-passe, mas também a ativação da autenticação multifator, tendo para tal, disponibilizado um link adequado para o efeito. Apesar disso, os técnicos de suporte não verificaram que o próprio link no email recebido originalmente remetia para um abreviador de endereços ("bit.ly"), que não pertencia ao fornecedor de serviços de e-mail. Retirado de https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/.

Pretexting: Envolve a criação de um cenário ou pretexto falso para enganar a vítima e obter informações confidenciais. O atacante finge ser alguém de confiança ou autoridade para persuadir a vítima a revelar dados pessoais ou empresariais.

Baiting: O atacante oferece algo atraente para enganar a vítima a executar uma ação que comprometa a segurança, como baixar um software malicioso ou fornecer informações pessoais. Pode envolver a distribuição de dispositivos físicos infectados, como pen drives, deixados em locais estratégicos.

Quid Pro Quo: Semelhante ao *baiting*, mas envolve a promessa de um serviço ou benefício em troca de informações ou acesso. Por exemplo, o atacante pode oferecer suporte técnico gratuito em troca de credenciais de login.

Ataques de *Watering Hole*: O atacante compromete websites que são frequentemente visitados pelo alvo pretendido. Quando a vítima acede ao site comprometido, o seu dispositivo é automaticamente infectado com malware.

Quishing: Uma forma de *phishing* que utiliza códigos QR maliciosos para direcionar as vítimas a sites fraudulentos ou para descarregar software malicioso nos seus dispositivos.

AI Phishing: Ataques de *phishing* que utilizam inteligência artificial para criar mensagens mais sofisticadas e personalizadas, sem erros ortográficos, inconsistências gramaticais ou outros sinais comuns que normalmente denunciam tentativas de phishing, aumentando assim a probabilidade de sucesso ao imitar padrões de comunicação humanos.

Hybrid Vishing: Combina técnicas de *vishing* com outros métodos de ataque, como o *phishing* tradicional ou *smishing*, para aumentar a eficácia, utilizando múltiplos canais de comunicação para enganar a vítima.

IV. A IMPORTÂNCIA DA FORMAÇÃO DOS COLABORADORES E ESTRATÉGIAS PARA MITIGAR O PROBLEMA

Os colaboradores desempenham um papel central na mitigação de ataques de engenharia social, como o phishing. Embora a tecnologia seja uma ferramenta essencial na gestão da segurança da informação, estudos indicam que esta, isoladamente, não é suficiente para lidar com os riscos associados. A chave para uma gestão eficaz da segurança da informação está nas pessoas, que constituem a primeira e mais crítica linha de defesa das organizações.

Historicamente, a segurança da informação era vista principalmente como uma questão técnica, mas esta abordagem revelou-se insuficiente. Perdas significativas resultantes de falhas de segurança, muitas vezes associadas a erros humanos, alteraram o paradigma. Hoje, gestores e especialistas reconhecem

a importância do "fator humano" na proteção das organizações, promovendo a formação e a sensibilização como estratégias essenciais para mitigar riscos. Este enfoque vai além da equipa de TI, abrangendo todos os colaboradores, que precisam de ser capacitados para identificar e reagir adequadamente a ameaças como o phishing.

Um exemplo claro da eficácia da formação encontra-se num estudo realizado numa grande empresa de transportes na Turquia. Neste projeto, foram implementadas campanhas de sensibilização e formação em segurança da informação, com resultados notáveis:

Melhoria na Gestão de Palavras-Passe: Houve uma redução significativa no uso de palavras-passe fracas, com os colaboradores a adotarem práticas mais seguras.

Participação Ativa nos Controlos de Segurança: Os funcionários passaram a envolver-se nos mecanismos de segurança implementados, demonstrando uma maior consciência e compromisso.

Cultura de Melhoria Contínua: Os colaboradores começaram a integrar boas práticas de segurança de forma consistente nas suas rotinas.

A experiência turca reflete a importância de alinhar os colaboradores com os objetivos de segurança organizacional. Quando devidamente sensibilizados, os funcionários tornam-se agentes ativos na defesa contra ameaças. Para alcançar este nível de eficácia, a formação deve ser contínua e envolver estratégias variadas, adaptadas às diferentes necessidades das organizações.

Outro estudo, nomeadamente "*Effectiveness of and user preferences for security awareness training methodologies"*, realizado pela universidade Mahidol, destaca novamente a eficácia dos programas de formação e consciencialização na redução da suscetibilidade a ataques de engenharia social. A análise de métricas, como a taxa de falsos negativos, demonstra que diferentes tipos de formação têm impactos variados, sendo que uma abordagem combinada e diversificada é a mais promissora.

Foram identificadas estratégias eficazes para reduzir a vulnerabilidade dos colaboradores a ataques de phishing. Estes métodos são adaptáveis a diferentes contextos organizacionais e combinam acessibilidade, interatividade e eficácia prática:

Formação em Vídeo: Vídeos curtos e objetivos que introduzem conceitos básicos sobre phishing, as técnicas utilizadas pelos cibercriminosos e os indicadores para identificar e-mails fraudulentos. Este formato oferece flexibilidade e é particularmente útil para colaboradores com agendas apertadas, permitindo a aprendizagem ao seu ritmo

Jogos: Jogos, por exemplo, desafiam os utilizadores a distinguir e-mails legítimos de fraudulentos em cenários simulados. Esta abordagem aumenta o envolvimento dos participantes e facilita a retenção do conhecimento, tornando este método especialmente eficaz para organizações que valorizam a interatividade nas suas formações.

Material de Texto: Brochuras e textos educativos apresentam exemplos práticos para detetar phishing, detalhando as potenciais consequências e indicadores, como URLs suspeitas. Este método é acessível, económico e eficiente para organizações com recursos limitados, oferecendo uma base sólida para a consciencialização dos colaboradores.

Formação Presencial com Instrutores: As sessões lideradas por instrutores proporcionam uma experiência mais interativa, com quizzes em tempo real e debates que permitem esclarecer dúvidas e aprofundar o conhecimento. Embora mais exigente em termos de tempo e recursos, esta abordagem é frequentemente preferida pelos participantes devido à interação direta e à personalização do conteúdo.

O estudo revelou que todas as formas de formação reduziram significativamente a suscetibilidade dos colaboradores a phishing. Contudo, a formação presencial, quando combinada com métodos como vídeos e jogos, mostrou resultados superiores. Esta diversificação de estratégias permite maximizar a eficácia, adaptando-se às necessidades e aos recursos das organizações.

V. CONCLUSÃO

A transformação digital trouxe enormes benefícios, mas também desafios significativos no domínio da segurança da informação e da cibersegurança. A pandemia de COVID-19 acelerou esta evolução, expondo vulnerabilidades nas infraestruturas digitais e destacando a importância de proteger informações confidenciais.

Os relatórios analisados, tanto a nível europeu como nacional, evidenciam que ataques como *phishing*, *smishing* e outras formas de manipulação psicológica continuam a ser vetores predominantes de entrada para ciberameaças mais complexas, como ransomware. Além disso, os setores mais afetados, como administração pública, transporte, finanças e saúde, refletem a necessidade urgente de fortalecer as defesas cibernéticas em áreas críticas.

Neste trabalho explorámos a crescente ameaça de ataques tecnológicos e ao fator humano, com particular destaque para as práticas de engenharia social, como o *phishing*. Estas ameaças, alimentadas por lacunas tecnológicas e falhas humanas, revelam a necessidade de reforçar a proteção organizacional não apenas com soluções técnicas, mas também através de uma estratégia robusta de formação e sensibilização.

Os colaboradores desempenham um papel central na segurança das organizações, sendo a primeira linha de defesa contra ciberameaças. Como evidenciado, a formação contínua é indispensável para

mitigar erros humanos, aumentar a consciencialização e promover boas práticas. Estudos comprovam que métodos diversificados – como vídeos, jogos, brochuras e sessões presenciais – são eficazes na redução da suscetibilidade aos ataques. Além disso, a integração de várias estratégias de formação potencia a retenção de conhecimento e reforça a cultura de segurança nas organizações.

Por fim, fica evidente que o sucesso na gestão da segurança da informação exige uma abordagem holística, que combine tecnologia, formação e cultura organizacional. Apenas desta forma as organizações estarão preparadas para enfrentar os desafios do ciberespaço e proteger os seus ativos mais valiosos – as suas informações e as pessoas que as gerem.

REFERÊNCIAS BIBLIOGRÁFICAS

(2014). *Enisa Threat Landscape* [Review of *Enisa Threat Landscape*]. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2014.

(2023). *Enisa Threat Landscape*. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

(2023). *Relatório Riscos & Conflitos*. CNCS. https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs15m.pdf.

(2024). *Enisa Threat Landscape*. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

(2024). *Relatório Riscos & Conflitos*. CNCS. https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs15m.pdf.

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report*, *14*(4), 223–229. https://doi.org/10.1016/j.istr.2010.05.002.

IBM. (2024). *What is Social Engineering?* Www.ibm.com. https://www.ibm.com/topics/social-engineering. [Acedido a 11 Dezembro 2024]

IBM. (2024, May 17). *Phishing*. Ibm.com. https://www.ibm.com/think/topics/phishing. [Acedido a 11 Dezembro 2024]

Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, *5*(6), e02010. https://doi.org/10.1016/j.heliyon.2019.e02010.

GESTÃO DE VULNERABILIDADES EM SISTEMAS DE INFORMAÇÃO NAS ORGANIZAÇÕES PORTUGUESAS

MARTA MONTEIRO FERREIRA [1]

1 marta.monteiro.ferreira@tecnico.ulisboa.pt

RESUMO:

A segurança da informação desempenha um papel fundamental na proteção das organizações contra os ciberataques, que têm vindo a crescer. Neste artigo, abordam-se os conceitos essenciais da gestão de vulnerabilidades, explorando metodologias e ferramentas que auxiliam na identificação, priorização e mitigação de falhas de segurança. É apresentado um caso prático sobre o ataque de *Ransomware* sofrido pela empresa Energias de Portugal (EDP), que elucida as consequências da exploração de vulnerabilidades não corrigidas e a importância de uma abordagem eficiente na gestão dos riscos.

As conclusões deste artigo reforçam que a gestão de vulnerabilidades não é apenas uma ferramenta para minimizar riscos, mas também um factor estratégico para a adaptação organizacional num ambiente digital em constante evolução.

Palavras-chaves - vulnerabilidades, *Ransomware*, ciberataque, EDP, *framework*, segurança da informação.

ABSTRACT:

Information security plays a fundamental role in protecting organizations from cyberattacks, which have been on the rise. This article addresses the essential concepts of vulnerability management, exploring methodologies and tools that aid in the identification, prioritization, and mitigation of security flaws. A practical case study on the Ransomware attack suffered by Energias de Portugal (EDP) is presented, illustrating the consequences of unpatched vulnerabilities and the importance of an efficient approach to risk management.

The conclusions of this article reinforce that vulnerability management is not just a tool for minimizing risks, but also a strategic factor for organizational adaptation in a constantly evolving digital environment.

Keywords: Vulnerabilities, Ransomware, Cyberattack, framework, information security.

I. INTRODUÇÃO

A. Contextualizar a importância da gestão das vulnerabilidades na segurança da informação

As vulnerabilidades são definidas como falhas nos sistemas, redes e aplicações que podem ser exploradas por atacantes, que representam um dos riscos à segurança. A identificação e mitigação dessas vulnerabilidades são importantes para evitar a violação dos dados.

Para identificar essas vulnerabilidades é necessário fazer a gestão, que permitirá avaliá-las e corrigi-las de maneira contínua. O aumento de incidentes de segurança, como ataques de Ransomware e DDoS, salienta a importância de implementar processos, como por exemplo a framework NIST Cybersecurity, que mitiguem esses ataques.

B. Cenário atual nas organizações em Portugal

No cenário português, a proteção das infraestruturas é um desafio constante porque tem existido um aumento significativo dos ataques direcionados a setores críticos, tais como o setor financeiro, o setor da saúde e o setor dos serviços públicos.

C. Objetivo do artigo na relevância da gestão de vulnerabilidades

O objetivo do presente artigo é identificar as ferramentas e metodologias consideradas como boas práticas na gestão de vulnerabilidades.

A relevância do tema visa assim sensibilizar para a importância da implementação de boas práticas na gestão de vulnerabilidades, promovendo uma maior segurança e resiliência nas organizações.

II. CONCEITOS FUNDAMENTAIS DA GESTÃO DE VULNERABILIDADES

A. Importância da segurança da informação

Quando nos referimos a uma vulnerabilidade, estamos a referir-nos a uma fraqueza num sistema informático que pode ser explorada por um hacker para realizar um ataque. O objetivo dos hackers é explorar o sistema, de modo a descobrir falhas.

B. Ciclo de vida da gestão de vulnerabilidades

O ciclo de vida das vulnerabilidades é a forma como as organizações detetam e tentam evitar que as vulnerabilidades encontradas possam ser suscetíveis a ataques.

Este processo é contínuo e iterativo, sendo dividido em 6 etapas:

Identificação: esta etapa é muito importante, uma vez que é criado um inventário de todos os dispositivos e recursos na rede que a empresa possui.

Priorização: com o inventário criado, é necessário identificar os recursos que precisam de mais "atenção".

Avaliar: nesta etapa é avaliada, especificamente, a funcionalidade de cada recurso e criado um "perfil" de risco para cada um.

Relatar: com base nos resultados da avaliação é elaborado um documento onde está discriminado que tipo de vulnerabilidades foram encontradas, quais os níveis de priorização e quais as recomendações a ter em atenção.

Remediar: identificar as vulnerabilidades mais permanentes na organização e implementar o plano de segurança. A remediação pode abranger várias atividades, tais como atualizar o software, aplicar *patches* ou isolar os sistemas vulneráveis para proteger os outros componentes.

Verificar: a última fase consiste na confirmação de que as vulnerabilidades foram eliminadas.

C. Metodologias e *frameworks* comuns

Sendo a gestão de vulnerabilidades um ponto crítico para a segurança da informação, foram adotadas diversas metodologias e *frameworks*, de modo a estruturar e criar um padrão, garantindo assim que as organizações possam mitigar os riscos de forma eficiente e consistente.

As metodologias mais comuns que as empresas adotam são o ciclo de vida de gestão de vulnerabilidades, a abordagem baseada no risco e o *testing-based methodology*.

A metodologia "ciclo de vida de gestão de vulnerabilidades" baseia-se no ciclo iterativo composto por etapas, como foi explicado nos pontos anteriores. Esta abordagem promove a melhoria contínua e está alinhada com os princípios do ciclo PDCA (Plan-Do-Check-Act). Este ciclo é uma das ferramentas mais utilizadas pelas organizações, pois permite acelerar e aperfeiçoar os processos através da identificação dos problemas, descobrir as principais causas, bem como as possíveis soluções.

A metodologia "abordagem baseada no risco" envolve a avaliação dos projetos com base na probabilidade de ocorrer um ataque e o impacto que este pode causar à empresa.

A metodologia "*testing-based methodology*" utiliza os testes de penetração (*penetration testing*) e testes de vulnerabilidade (*vulnerability scanning*) para identificar quais as vulnerabilidades ativas no sistema.

As *frameworks* mais comuns são a NIST Cybersecurity Framework (CSF), a ISO/IEC 27001, a ISO 27002, a CIS Controls e o MITRE ATT&CK.

A framework "*NIST Cybersecurity Framework* (CSF)" é uma das mais utilizadas, porque proporciona

uma abordagem mais estruturada para a gestão das vulnerabilidades.

As *frameworks* "ISO/IEC 27001 e ISO 27002" são um guia para a implementação de um sistema de gestão de segurança da informação (SGSI).

A *framework* "CIS Controls", também conhecido como Centrer for Internet Security, oferece um conjunto de processos práticos, incluindo o processo "Continuous Vulnerability Management". Este processo orienta a identificação e a remediação das vulnerabilidades.

A *framework* "MITRE ATT&CK" é utilizada para priorizar as vulnerabilidades com base nas táticas e técnicas que os atacantes utilizam regularmente.

III. FERRAMENTAS E MÉTODOS DE GESTÃO DE VULNERABILIDADES

A. Ferramentas para a gestão de vulnerabilidades

Com o aumento significativo do uso da tecnologia têm surgido várias ferramentas especializadas que ajudam as organizações a implementar soluções para a gestão de vulnerabilidades. As ferramentas são dividas em 3 áreas de utilização: ferramentas para deteção de vulnerabilidades, ferramentas para a gestão das mesmas e ferramentas específicas na Information Technology (IT), como base de dados e testes de segurança.

As ferramentas utilizadas para a deteção de vulnerabilidades são a Nessus, a QualysGuard e a OpenVas.

As ferramentas utilizadas para a gestão de vulnerabilidades são a Rapid7, InsightVM e a Tenable.io.

Na última categoria, é utilizada a ferramenta Burp Suite para SQL e a Matasploit Framework para testes de penetração.

B. Métodos de avaliação

Para mitigar de forma eficaz, é necessário implementar métodos de avaliação com base no seu impacto e probabilidade de exploração. Para isso, é necessário seguir os seguintes passos: Análise de Vulnerabilidade, Avaliação baseada no Risco, Testes de Penetração e a Modelagem de Ameaças.

A análise de vulnerabilidades consiste numa exploração detalhada nos sistemas e na rede das organizações, utilizando ferramentas automatizadas para as identificar. Este método é dividido em 3 etapas: Descoberta, Classificação e Reportagem. Na primeira etapa é feito o mapeamento do sistema, dos serviços e dos softwares que vão ser analisados. Na segunda etapa são atribuídas severidades às vulnerabilidades encontradas. Por fim, na última etapa é criada a documentação de toda a análise feita.

O método de avaliação baseado no risco passa por considerar o impacto e a probabilidade de exploração, permitindo dar prioridade à correção das falhas críticas.

Os testes de penetração são utilizados para simular um ataque de modo a descobrir as vulnerabilidades críticas presentes na rede da organização.
A modelagem de ameaças ajuda a identificar as falhas nos sistemas da empresa, permitindo antecipar possíveis vetores de ataques.

IV. CASOS PRÁTICOS

A. Ataque à EDP

Um caso concreto de um ataque aos sistemas informáticos ocorreu na EDP, que foi alvo de um ataque de Ransomware pelo grupo de *Hackars Ragnar Locker*.
O ataque ocorreu em Abril de 2020, em plena pandemia COVID-19, tendo os atacantes explorado as vulnerabilidades nos sistemas internos da empresa. Este ataque foi facilitado pelo incremento do teletrabalho e pela utilização de redes externas.
O grupo utilizou várias técnicas para implementar o ataque, como exploração de vulnerabilidades do software, movimentação lateral, criptografia dos dados e exfiltração dos dados. Após entrarem nos sistemas internos da empresa, os hackers utilizaram o *Remote Desktop Protocol* (RDP) para explorar a rede. Foram transferidos cerca de 10 TB de dados sensíveis ameaçando divulgá-los caso a empresa não pagasse o resgate de 10 milhões de euros. Posteriormente, os dados foram encriptados para que não fossem passíveis de serem acedidos.
A empresa sofreu várias consequências com este ataque, incluindo a interrupção dos sistemas críticos, prejuízos financeiros resultantes do pagamento do resgate e danos na reputação perante os clientes.
Contudo, foi possível retirar lições importantes para a gestão de vulnerabilidades, como a importância da realização de atualizações regularmente, a implementação de sistemas de monitorização e deteções de atividades suspeitas, o melhoramento da gestão de acessos, a implementação de um plano de respostas a incidentes e a formação dos funcionários em cibersegurança.

B. Ataque à Vodafone

Outro caso prático de um ataque informático ocorreu na empresa Vodafone, pelo grupo *Lapsus$ Group*.
Este ataque afetou as infraestruturas da operadora, levando à interrupção dos serviços de voz, SMS e dados móveis dos seus clientes. O impacto foi também sentido em algumas instituições públicas e privadas, como por exemplo o INEM, que registaram dificuldades nas comunicações.
De acordo com as informações divulgadas, o ataque terá sido realizado através da obtenção ilegal das credenciais de acesso de um trabalhador da empresa. O grupo conseguiu intercetar esses dados e clonar

o cartão do telemóvel do funcionário. Com esses dados na sua posse, o grupo conseguiu ultrapassar o sistema de autenticação de multifator.

Após obter os dados de acesso, o grupo colocou esses dados à venda num site russo, com um preço base de 2500 dólares.

Este caso evidencia a importância da adoção de várias medidas de segurança, como por exemplo a utilização de VPN, a criação e atualização regular de cópias de segurança dos dados essenciais da empresa.

C. Ataque à Câmara Municipal de Gondomar

Por fim outro caso prático ocorreu na Câmara Municipal de Gondomar. Este ataque paralisou os serviços informáticos da Câmara, impedindo o funcionamento dos sistemas administrativos e de atendimento ao público.

Pelas investigações, a origem do ataque terá estado nos servidores da Rússia, mas não foi possível aferir se foram os responsáveis.

Os atacantes exigiram um pedido de resgate no valor de 750 mil euros para restaurar o acesso aos dados encriptados, que não foi aceite pela autarquia, o que levou um esforço para a mitigação dos dados causados.

O ataque comprometeu os dados pessoais dos munícipes, como por exemplo os dados nominativos (nome, morada, contacto e número de identificação), os dados fiscais e dados bancários.

No entanto, este caso serviu de alerta para a vulnerabilidade das infraestruturas públicas locais e levou a reforçarem as suas medidas de cibersegurança.

V. CONCLUSÃO E RECOMENDAÇÕES

Ao longo do artigo verificamos que a identificação e a mitigação de vulnerabilidades não requerem apenas ferramentas tecnológicas, mas também processos bem estruturados com base na estratégia da empresa.

Este estudo reforça a importância em adotar uma abordagem contínua, com base em *frameworks* reconhecidas e ferramentas eficazes, superando os desafios e mitigando os riscos associados às vulnerabilidades.

Com base nos resultados obtidos e na análise realizada, são apresentadas as seguintes recomendações: investigar em consciencialização e em formação contínua, adotar *frameworks* e metodologias consolidadas, priorizar as vulnerabilidades com base no risco, implementar ferramentas de automação e estabelecer um processo contínuo de monitorização e de melhoria contínua.

REFERÊNCIAS

Next4Sec Security Intelligence; 2022; As fases do ciclo de vida da gestão de vulnerabilidades; Linkedin; https://www.linkedin.com/pulse/fases-do-ciclo-de-vida-da-gest%C3%A3o-vulnerabilidades-next4it/

O que é a gestão de vulnerabilidade? ; Microsoft; https://www.microsoft.com/pt-pt/security/business/security-101/what-is-vulnerability-management

Equipa EcoTrust; 2023; Como implementar o Gerenciamento de Vulnerabilidades; EcoTrust; https://blog.ecotrust.io/gerenciamento-de-vulnerabilidade/

2023; PDCA: Plan-Do-Check-Act (repeat); accept; https://www.accept.pt/pdca-plan-do-check-act/

Gabriela de Britto Maluf; 2023; O que é Abordagem Baseada em Risco (ABR)?; uplexis; https://uplexis.com.br/blog/artigos/o-que-e-abordagem-baseada-em-risco-abr/

Morpheuslord; 2024; Teste de penetração e verificação de vulnerabilidades; hackernoon.com; https://hackernoon.com/lang/pt/testes-de-penetra%C3%A7%C3%A3o-e-verifica%C3%A7%C3%A3o-de-vulnerabilidades

2024; Pentest e Gestão de Vunerabilidades; columbiati.com; https://columbiati.com/pentest-e-gestao-de-vunerabilidades/

Kleber Aquino Santos Júnior; 2023; Modelagem de Ameaças: Identificando e Mitigando Riscos de Segurança; Linkedin; https://pt.linkedin.com/pulse/modelagem-de-amea%C3%A7as-identificando-e-mitigando-riscos-kleber

NIST Cybersecurity Framework; Wikipedia; https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework

Dejan Kosutic; Semelhanças e diferenças entre a ISO 27001 e a ISO 27002; advisera.com; https://advisera.com/27001academy/pt-br/knowledgebase/semelhancas-e-diferencas-entre-a-iso-27001-e-a-iso-27002/

Alexandre de Lima Lopes; Mudanças na Nova ISO/IEC 27001 e ISO/IEC 27002; wiseplangroup; https://wiseplangroup.com/mudancas-na-nova-iso-iec-27001-e-iso-iec-27002/

2024; CIS: Controle 7 – Gestão contínua de Vulnerabilidades; ostec.blog; https://ostec.blog/geral/gestao-continua-de-vulnerabilidades/

MitreAttack; https://attack.mitre.org/

Openvas; https://www.openvas.org/

Tenable; https://www.tenable.com/products/vulnerability-management

Metasploit; https://www.metasploit.com/

Sergiu Gatlan; 2020; EDP energy giant confirms Ragnar Locker ransomware attack;

bleepingcomputer; https://www.bleepingcomputer.com/news/security/edp-energy-giant-confirms-ragnar-locker-ransomware-attack

Mark Loman; 2020; Ragnar Locker ransomware deploys virtual machine to dodge security; news.sophos.com; https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security

Agnė Augustėnė, 2023; Ciberataque à Vodafone: lições e consequências; NordVPN; https://nordvpn.com/pt/blog/ataque-vodafone/

2022; Vodafone Portugal alvo de ciberataque; Vodafone; https://www.vodafone.pt/press-releases/2022/2/vodafone-portugal-alvo-de-ciberataque.html

2023; Comunicado de 17 de outubro de 2023; Gondomar; https://www.cm-gondomar.pt/comunicado-17-de-outubro-de-2023/

2023; Gondomar sofreu o maior ataque informático a uma instituição pública em Portugal; Sol; https://sol.sapo.pt/2023/11/01/gondomar-sofreu-o-maior-ataque-informatico-a-uma-instituicao-publica-em-portugal/

2030: THE UNFOLDING CONVERSATION - BEYOND THE SCRIPT

- A BUSCA POR UMA CONEXÃO HUMANA AUTÊNTICA NO FUTURO.

***2030: The Unfolding Conversation - Beyond the Script* - a busca por uma conexão humana autêntica no futuro.**

Bem-vindos ao novo marcador da «*Cyberlaw by CIJIC*» dedicado a explorar os próximos anos através duma visão especializada, provocadora, acutilante, mas fundamentalmente humana. Longe de ser um espaço de (mais) tecnicidade, aqui convidamos autores e leitores a mergulhar em reflexões pungentes e acessíveis sobre as tendências que moldarão as nossas relações humanas, a nossa identidade humana e o nosso lugar no mundo até 2030. *And beyond*. Aqui, procuraremos ir um pouco mais além do roteiro esperado, desafiando narrativas pré-estabelecidas, desvelando os diálogos não escritos e as complexidades dum futuro que se revela e acelera a cada dia. Considerando a natureza intrínseca e vital da necessidade humana pelo outro e o nosso ideal humano de interdependência, construção conjunta, colaboração, cooperação, partilha, pertença e coexistência, é para um futuro dinâmico e evolutivo - que nos desafia a pensar sobre quem somos hoje, a nossa natureza humana amanhã e como nos reencontraremos - que decidimos projectar a nossa nova utilidade.

A nossa edição deste ano termina com a abertura *ex novo* dum desafiante mas catalisador marcador:

«2030: *THE UNFOLDING CONVERSATION - BEYOND THE SCRIPT*».

Bem-vindos à busca por uma conexão humana autêntica no futuro.

2030: The Unfolding Conversation, Beyond the Script - The quest for authentic human connection in the future.

Welcome to our newest feature of *Cyberlaw by CIJIC*, aimed at exploring the coming years through an expert, thought-provoking, incisive, yet fundamentally human vision. Far from being a space of (further) technicality, here we invite authors and readers to delve into poignant and accessible reflections on the trends that will shape our human relationships, our human identity, and our place in the world until 2030. And beyond.

Here, we will seek to go a little further than the expected roadmap, challenging pre-established narratives, unveiling unwritten dialogues and the complexities of a future that reveals itself and accelerates daily. Considering the intrinsic and vital nature of the human need for one another and our human ideal of interdependence, joint construction, collaboration, cooperation, sharing, caring, belonging, and coexistence, it is towards such a dynamic and evolving future - one that challenges us to ponder who we are today, our human nature tomorrow, and how we will reconnect in the future - that we have decided to project such new feature.

This year's edition concludes with the *ex novo* opening of a challenging yet catalysing new chapter:

«*2030: THE UNFOLDING CONVERSATION - BEYOND THE SCRIPT*»

Welcome to the quest for authentic human connection towards the future.

JUST THE HUMAN IN THE LOOP:

WORK, WORTH AND THE ALGORITHMIC ECONOMY OF 2030

By **Marcia Narine Weldon**[1]

December 2030

December 2030: A Day in the New Economy

Maria woke up to a soft ping on her phone. Task Cluster #872. Her AI assignment for the day: emotional tone calibration for a batch of client responses generated overnight. She was one of 38 million certified human "feelers"—gig workers trained to polish algorithmic outputs for warmth and relatability. Her universal basic income covered essentials. But she still logged in for meaning, not money.

Maria had planned to apply to law school. But by 2027, AI had passed every jurisdiction's bar or professional licensing exam. In 2028, California became the first state to allow AI-only legal representation in family court, and by 2029, the EU had allowed AI lawyers for everything but capital and asylum cases.

---

1 *Marcia Narine Weldon a professor at the University of Miami School of Law, the the former general counsel of an AI startup that created digital twins with ethics at its core and is the current general counsel and head of business affairs of a company that uses behavioral science and data analytics to design compliance and governance programs. She teaches ethics and technology to college students, integrates AI across her law school curriculum, and writes, speaks, and advises globally on AI governance and ethics. Her 2024 law review article on future-proofing legislation explores the gaps emerging technologies expose in our legal system and is available here.*

The Great Professional Collapse

Legal documents generated by AI were consistently accurate, persuasive, and free from hallucinations. Courts began to rely on AI-generated opinions, which improved consistency and reduced delays. Judges who once struggled with backlogs found themselves moving through dockets faster than ever, aided by systems that drafted thoughtful, well-reasoned rulings within minutes. The access to justice gap had rapidly closed.

The story was the same in medicine. AI surpassed human doctors not only in diagnostic accuracy but in early detection of rare conditions and subtle patterns. Patients began to rate AI-based consultations higher than human ones, citing greater empathy, better follow-up, and more consistent explanations. By 2028, medical school enrolment had plummeted.

Other graduate programs soon followed. MBA programs saw declines in applications as corporations leaned into algorithmic strategy engines and AI-managed financial modelling. As early as 2025, even top-tier programs, such as Harvard Business School, began reporting significant employment placement challenges for new graduates (Wall Street Journal, 2025). Meanwhile, younger professionals reported record levels of disillusionment with traditional career tracks, citing instability, delayed payoffs, and unclear relevance in an AI-first economy (The Atlantic, 2025).

The professions once protected by prestige, licensing, and complexity were no longer immune to displacement. The shift didn't just affect white-collar sectors. By 2029, manual labor jobs—once devalued—became a luxury service tier. Wealthy clients paid a premium for human massage therapists, drivers, housekeepers, and even handwritten calligraphy for invitations to exclusive events. Touch and time became status markers in a world of machine precision.

The New Human Role: Interface Maintenance

The institutions meant to certify human value couldn't compete. For those who had spent years chasing degrees, licensure, and high-performance metrics, the shift was existential. Many found themselves relegated to roles as micro-task testers, brand validators, or AI ethic spotters, not because they lacked talent, but because the system no longer rewarded it. They watched as the value of their expertise was replaced by the speed, scale, and consistency of generative models. Some still carried the titles: J.D., M.D., MBA. But in the new economy, those credentials carried little weight.

Meanwhile, job titles faded. Graduate school applications dropped because the metrics changed. What mattered was your usefulness to the system. Humans work, not to build careers or to follow their callings, but to remain relevant. They fine-tune AI outputs, flag emotional risk, and tag satire and

deepfakes. They make products feel safe to the end user. Would-be doctors, lawyers, and engineers act as quality assurance workers.

The humans who remain in the loop serve three purposes: emotional resonance, legal legitimacy, and consumer signalling. In 2030, this means if you're flagged for exclusion, demotion, or review, a human may appear at the end of the process. But that person didn't decide. They just confirmed, and in most cases, they are gig workers themselves—brought in to ensure that the company can claim "a human was involved." The "human in the loop" became branding. It signalled oversight without offering any. At best, it meant a human read the decision. At worst, it meant someone was there to absorb liability. Humans weren't managing the algorithm. Instead, they were lending a label to its output.

The UBI Paradox

At the same time, most people appeared content with universal basic income. The EU, US, and the wealthier countries covered rent, food, and streaming subscriptions. With essentials met and incentives minimal, citizens slipped into patterns of passive consumption—streaming, scrolling, swiping, and most of all, consuming. Of course, even UBI is no silver bullet. While it eliminates the anxiety of survival, it does little to replace the sense of contribution, belonging, and identity that meaningful work provides. And in this new economy, many people accept purposelessness in exchange for stability even if leads to stagnation.

Those who clung to work as identity, meaning, or status found themselves increasingly out of step with a society that had redefined contribution as presence.

The Power Consolidation

The digital divide widened. Meanwhile, the tech oligarchy consolidated their power. They no longer needed to code. They instead focused on extracting data, attention, and emotional nuance, which became extremely valuable corporate assets.

By 2028, multinational insurers had become the most powerful entities in the accountability ecosystem. They refused coverage to firms that couldn't prove certified human oversight, and their proprietary liability algorithms became more influential than government policy. This meant that humans always had to be "in the loop."

Disruptions, Resistance, and Unexpected Developments

Of course, not every future unfolded on schedule. A surge in quantum breakthroughs briefly destabilized AI model training in late 2027, and a two-year spike in global energy prices forced several governments to ration compute power. But the march toward automation continued. The largest

companies diversified into localized models and carbon-efficient design, accelerating innovation in some regions while leaving others behind.

There was some resistance, of course. A Swiss referendum in 2028 banned AI agents from supervising health care workers. In Spain and Brazil, grassroots cooperatives launched "*Only Human*" certification labels for cafes, wellness centers, and tutoring services. The EU introduced pilot programs mandating one human for every 50,000 machine-led decisions in regulated industries. The US Federal Trade Commission required 'algorithmic nutrition labels' on enterprise AI tools, showing accuracy rates, bias metrics, and last audit dates.

On a positive note, while AI was orchestrating labor, it was also solving scientific challenges that had eluded us for decades in health care and climate change. By 2029, AI-assisted researchers made Mars habitable. That same year, the Martian Sovereignty Project was launched. Spearheaded by entrepreneur Melon Husk, it offered a stark choice: adapt to Earth's AI-first economy or leave. Millions boarded ships. Billions stayed on earth. They preferred the devil they knew.

How We Got Here: Looking Back at 2025

In 2025, the World Economic Forum predicted that 78 million new jobs would be created globally by 2030—but emphasized that these roles would demand creativity, emotional intelligence, resilience, and analytical thinking (WEF 2025 Future of Jobs Report). The problem? Most schools never taught those skills. The pipeline broke, and people got left behind.

As journalist Carole Cadwalladr had warned in 2025, this was a digital coup. Silicon Valley's "*bro-ligarchy*" as she called it, had quietly seized control over key levers of public and private decision-making, with little resistance or oversight (TedTalk April 2025).

In 2025, industry leaders promised a better path. Microsoft and Salesforce projected a "hybrid workforce," where AI would augment human potential, not replace it. Jeanne Meister described a future where machines would handle the repetitive while people focused on empathy, strategy, and innovation (Forbes, 2025).

Phillip D'Souza offered a hopeful frame: that AI agents would serve as collaborators, occasionally "hiring" humans to handle judgment-driven or creative decisions (LinkedIn, 2025). That vision didn't scale. The incentives didn't align.

Marc Benioff of Salesforce heralded a "digital labor revolution" predicting that by 2028, AI agents would responsible for over 40% of workplace communication, task delegation, and performance scoring across many major industries (Business Insider, 2025). Anthropic CEO, however, told Axios in June 2025 that "AI could wipe out half of all entry-level white-collar jobs — and spike

unemployment to 10-20% in the next one to five years." Regulators either didn’t care, were willfully ignorant, or felt too beholden to tech companies to stop slow things down.

AI agents were touted as the future in 2025 because they do not sleep, pause, or doubt. They do not have moods. They do not ask for flexibility. They simply execute. Scott Likens of PwC described this as the emergence of AI agents as autonomous workflow managers. He noted that agents now triage work, schedule tasks, escalate decisions, and guide performance review systems—all functions once handled by mid-level managers (PwC CES 2025 Interview). This, in theory, makes AI agents perfect workers and managers.

The Regulatory Failures

In 2025, EU regulators attempted to lead. But under pressure from tech giants like Apple, Google, and Meta, the AI Act was watered down before its final adoption ((CIO, 2025; Reuters, 2025). Provisions mandating transparency and human oversight were softened or delayed. What began as a call for accountability quietly turned into a long recess. In the US, individual states made laws, but the federal government refused to act, leading to a patchwork of

In theory, we're heading toward more inclusive governance frameworks. But research from BCG shows that while AI adoption is growing quickly, integration remains uneven, and frontline workers are often left out of the change process altogether (BCG, 2025). Governance often lags behind deployment. The people most affected by algorithmic oversight are the ones least likely to understand how or why the system made its decision. Article 22 of the GDPR, for instance, gives individuals the right not to be subject to automated decisions without meaningful human involvement. But in practice, that "meaningful" oversight is often superficial or symbolic.

The Vision We Lost

David Lee's TEDx talk imagined a better world. One where humans did work that felt like play and purpose, not productivity, guided job design. He argued that UBI could be a foundation for new types of roles—jobs that centered creativity, connection, and community (TEDx, 2017).

But perhaps the next revolution will not come from tech companies at all. It may come from legal scholars, insurance actuaries, and public interest lawyers who ask: If an AI agent acts as your manager, your evaluator, or your recommender, shouldn't it be subject to the same rules as any employer? That future is still possible—but only if we reclaim work as something more than interface maintenance.

The Warning We Should Have Heeded

We still have choices, and we must act now otherwise the future I have outlined will lead to what I have coined "optical ethics by design"—a system that mimics the aesthetics of human-centered governance without the substance. Unlike ethics by design, which embeds values into technology architecture, optical ethics by design embed appearances. It creates structures that project integrity and fairness while shielding systems from scrutiny. Human involvement exists not to question or change outcomes, but to reassure stakeholders that someone, somewhere, looked. The ethical layer becomes visual, not functional refined for optics, not agency.

The question now in 2025 is not whether AI agents can manage workflows. They already do.

The question is whether humans will retain the right to shape systems that govern them or whether our only remaining power is the right to say *yes*.

MARCIA NARINE WELDON

THE AI ERA:

CHARTING A DIGITAL CONSTITUTIONAL PACT FOR EVOLUTION BY 2030

By **Raquel Brízida Castro**[1]

"*AI isn't a tool - it's an agent. If most of the decisions are made by AI's... then power will gradually shift from humanity to these new alien intelligences*."[2]

The transformative and unprecedented development of Artificial Intelligence (AI) technology has rendered conventional modern constitutional theories increasingly inadequate, building on conceptual shifts already evident with the advent of digital technologies. AI's pervasive integration into society signifies a profound societal transformation, demanding a fundamental reconceptualization of constitutional frameworks[3]. Doctrinal analyses consistently highlight a

1 Phd in Law; Professor at the Faculty of Law, University of Lisbon; Researcher at the Lisbon Public Law Centre; currently, serves as Vice-President of ANACOM.

2 Harari, Yuval Noah. «Nexus: A Brief History of Information Networks from the Stone Age to AI» (Penguin Random House, 2024)

3 Avbelj, Matej. (2024). «Reconceptualizing Constitutionalism in the AI Run Algorithmic Society». German Law Journal , Volume 25 , Issue 7 , October 2024 , pp. 1081 – 1094. DOI: https://doi.org/10.1017/glj.2024.35

fundamental transformation of constitutionalism's matrix requiring a fundamental recalibration of its core principles and structures[4].

This AI-driven transformation presents critical challenges to constitutionalism's foundational pillars, including the rule of law, the separation of powers, and the protection of fundamental rights. These challenges also exacerbate an existing epistemic gap, contributing to a discernible crisis of legitimacy and knowledge within established governance models[5].

As a Democratic and Social Rule of Law State, Portugal's constitutional framework, specifically Article 2 of the *Constituição da República Portuguesa* (CRP), firmly establishes its foundations. It proclaims a state "based on popular sovereignty, on pluralism of democratic political expression and organization, on respect for and guarantee of the effective exercise of fundamental rights and freedoms, and on the separation and interdependence of powers, aiming at the realization of economic, social, and cultural democracy and the deepening of participatory democracy." These core tenets represent non-negotiable principles that intrinsically bind the Portuguese State in all its operations.

The robust application of this principle constitutes a central theme in constitutional doctrine and a primary concern for international human rights law, given its universal validity. An examination of the checklist provided by the Venice Commission within the Council of Europe framework[6] reveals that the current and foreseeable applications of AI demonstrably fail to meet the established requirements for a rule of law state. Specifically, the integration of AI introduces structural deficits concerning compliance with fundamental principles such as legality, legal certainty, the prohibition of arbitrariness, equality, non-discrimination, access to justice, and particularly, constitutional justice. While some of these challenges stem from broader digital regulation, others are uniquely pertinent to AI, prompting varying degrees of adaptations or targeted adjustments to existing legal frameworks.

Strategic Responses by 2030

Given the inherent constitutional challenges posed by the AI era, a multi-faceted approach becomes essential, focusing on strategic directives for future legal and governance frameworks by 2030. Firstly, clarifying the role of national constitutional rights, where reinforcing national constitutional identities and traditions presents both a substantial challenge and an extraordinary opportunity for the renewal of constitutionalism. This involves a predictive analysis of how existing

4 Idem, ibidem.
5 Idem, ibidem.
6 https://www.coe.int/en/web/venice-commission

rights can be reinterpreted or bolstered in the digital age. Secondly, entrenching fundamental digital rights, involving their formal constitutionalization or, at a minimum, their robust enshrinement within national laws that implement instruments such as the AI Act, ensuring alignment with respective constitutional traditions. Illustrative examples include the fundamental rights to explainability, effective human oversight, a human decision in specific cases, and the right to demand the disconnection of systems demonstrably harmful to fundamental rights. Implementing these rights will establish clear metrics for assessing AI accountability and human-centric control. Thirdly, deepening the Principle of Legality in the digital context will drive the enactment of legislation explicitly governing the use of AI systems by public administrations, particularly where they impact legally protected rights and interests. This requires establishing clear legal boundaries, defining permissible applications, and mandating robust mechanisms for effective control and accountability. The success of this deepening will be measurable by the clarity of legal frameworks and the demonstrable effectiveness of oversight processes. Fourthly, ensuring effective judicial protection requires equipping legal systems with agile and adequate instruments to safeguard fundamental rights, a necessity particularly acute within Administrative and Constitutional Justice. In these domains, AI applications introduce novel challenges to redress mechanisms, making future effectiveness directly assessable by the speed and adequacy of judicial responses to AI-related rights infringements. Lastly, regulatory action demands strengthened constitutional grounding. Given the increasing responsibilities delegated to regulators by the EU, their decisions must unequivocally align with national constitutional mandates, extending beyond mere compliance with EU law. The integrity of AI governance hinges on the demonstrable and measurable adherence of regulatory bodies to these foundational constitutional principles.

This comprehensive approach underpins the construction of the Digital Constitutional Pact for the age of Artificial Intelligence, which defines the proposed Digital Democratic Rule of Law State as an enduring guarantor of human well-being. Essential to this realization is ensuring that all digital power - whether public or private - operates and makes decisions impacting fundamental rights or other constitutionally protected interests, adhering to an order intrinsically tied to human dignity. This commitment demands a fundamental understanding that AI, as a powerful tool, serves to an end, with the human person invariably being the ultimate end. Consequently, all such operations must adhere to a clear legal basis, robust transparency rules, and effective auditing and accountability mechanisms. This foundational requirement applies universally, encompassing decisions leveraging algorithms and AI systems, and thus establishing a quantifiable framework for prospective governance oversight.

Practical Adaptations: some Portuguese case studies

The establishment of this Digital Democratic Rule of Law State calls for a hermeneutical approach, implying a preliminary roadmap of legally, administratively, and constitutionally pertinent questions. To illustrate this, two examples are presented:

A) One pertinent case study concerns the constitutional duty of the Public Administration to provide reasons (cf. Article 268/3 of CRP) and its correlation with the algorithmic explainability of administrative decisions, particularly under the *Código do Procedimento Administrativo* (cf. Articles 152 and 153 CPA). The prevailing legal and constitutional framework for the duty to provide reasons is sufficiently strong to support a robust fundamental right to algorithmic explainability, especially when considering the additional obligations imposed by the General Data Protection Regulation (GDPR) and the EU AI Act. Specifically, Article 152 of the CPA applies fully to automated administrative decisions, mandating that the reasoning for such decisions incorporates minimum elements of algorithmic explainability, thereby ensuring comprehensive understanding for the administrated individual. When interpreted considering the Constitution, the GDPR, and the EU AI Act, the CPA consequently demands that automated decisions uphold principles of transparency, auditability, and contestability. However, a critical distinction arises as the EU AI Act, at least by its own terms, does not universally contemplate a generic fundamental right to explainability - that is, the right to comprehend a specific result or decision in every concrete case. Notably, Article 86 of the AI Act, titled “Right to explanations regarding individual decisions”, explicitly limits its application to high-risk systems. Within this defined scope, a Principle of Explainability is affirmed, mandating that high-risk artificial intelligence systems must be designed and developed to ensure the intelligibility, by human beings, of their decision-making processes, internal functioning, and concrete results produced. This principle inherently implies: (i) *Transparency of decisions*; (ii) *Comprehension of algorithmic processes*; and (iii) *Traceability and audibility*.

B) A second critical area pertains to the imminent widespread adoption of AI systems by Public Administration and other relevant entities for decision-making, which will inevitably exert extensive impact on citizens' legal spheres and fundamental rights. In this context, public procurement regulations emerge as a decisive mechanism to ensure both AI system compliance with the AI Regulation's mandates and the robust protection of fundamental rights. Integrating specific, binding rules within public procurement procedures represents an effective legislative strategy to directly promote AI system compliance and robust rights protection. This is accomplished by obliging contracting authorities to stipulate that awarded proposals guarantee essential aspects of contractual execution, independent of competitive considerations. This framework ensures compliance with the

AI Regulation's obligations, which will integrate the legality block of public procurement once fully in force. By making such requirements binding, under penalty of exclusion, these rules proactively assist the Administration in mitigating potential high risks "*by design*" and in effectively addressing the protection of fundamental rights for citizens adversely affected by AI systems, ensuring full respect for effective judicial protection.

To this end, the European Commission has already published a set of AI Model Contractual Clauses (CCT-AI)[7], comprising High-Risk CCT-AI and Limited and Minimal Risk CCT-AI, designed for application until the AI Act becomes fully operational. For enhanced legal certainty and sustained impact, these clauses (or suitable adaptations thereof) should be formally integrated into national Public Contracts Codes, specifically regarding the mandatory or permissible clauses for inclusion in procedural documents. Such a measure would constitute a substantial advancement in the establishment of the Digital Rule of Law State, providing a measurable pathway for proactive rights protection.

The New Power Architecture: Latency and Sovereignty

This constitutional evolution also requires addressing the emergence of a new, dominant digital power architecture, where latency (AI's response time) becomes a strategic and decisive currency of influence and sovereignty. This dynamic pose new challenges to democratic ideals, risking the creation of new digital monopolies where access to vital AI capabilities and equitable response times is dictated by economic means rather than universal entitlement. For in an age where algorithms increasingly shape perception and opportunity, the digital divide becomes a chasm threatening not just material well-being, but the shared reality upon which democratic societies stand. This redefines societal access and control, making human connection and equitable access paramount. Also, it raises the question of a potential right to temporal neutrality, analogous to net neutrality, to ensure that no user is disadvantaged by artificially induced latencies, thereby guaranteeing truly universal and equitable access to essential services. Achieving this, particularly by 2030, calls for sustained and adaptive regulatory frameworks designed to actively counter market forces that would otherwise exacerbate digital disparities, ensuring that technological advancement genuinely serves as a democratizing force for all, rather than a tool for further stratification. The path chosen now, for a future defined by AI, will

7 https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/updated-eu-ai-model-contractual-clauses

determine whether humanity embraces a shared digital future of empowerment, or succumbs to an era of unprecedented control and division.

Conclusion - (AI)volution, Not Rupture

Recent decades have been characterized by a notable divergence between the accelerated pace of technological evolution and the comparatively slower progression of legal frameworks and institutional responsiveness. This phenomenon, often termed technological and social accelerationism, underscores the essential need to drive a decisive constitutional evolution in the age of AI.

Consequently, establishing a Digital Democratic Rule of Law State is a defining action, firmly anchored in constitutional principles. Here, a *technologically neutral constitutional interpretation*[8] must secure human dignity and fundamental rights as its essential foundation, upholding their primacy against the threats of digital stratification and *techno-nationalism*. Indeed, for a society increasingly reliant on algorithms and AI, the very essence of its human character depends on robust, enforced safeguards. This foundational understanding[9] reinforces the conviction that any future society, particularly one deeply intertwined with advanced algorithms and AI, must centrally place human dignity and fundamental rights at its epicenter. This is pivotal. **Without such a human-centric foundation, the very essence of a functioning, just and human society is seriously undermined**.

By 2030, the true measure of our constitutional commitment to human-centric AI will be its demonstrable success in building inclusive digital societies that empower every person, decisively overcoming the *forces of division* for a thriving collective human future.

RAQUEL BRÍZIDA CASTRO

8 Brízida Castro, Raquel (2023) Direito Constitucional: Ciberespaço e Tecnologia. Declínio do Constitucionalismo na UE? Almedina: Coimbra; pp. 43-52.
9 Idem, Ibidem; pp. 58 *et seq*.

CYBERLAW

BY CIJIC

MORE THAN MONEY:

HUMAN STORIES BEHIND CURRENCY EXCHANGE

By **Rachel Canales**[1]

"*The future depends on what we do in the present*." – Mahatma Gandhi

In today's world of global transitions (where families relocate, businesses expand across borders, and people seek stability amidst uncertainty), currency exchange often operates quietly in the background. But each transaction holds a deeply personal story...

In a world driven by fast-moving technologies and an ever-expanding digital economy, it's easy to overlook the quieter systems that connect us, currency exchange being one of them. But behind every international transfer lies a story. A couple moving abroad to start a new chapter. A small business entering a new market. A parent sending funds to support their child's education overseas.

1 Currency Exchange Specialist at GC Partners.
rachel.canales@gcpartners.co

These decisions are deeply personal, yet they take place within systems that feel increasingly technical and abstract. This article explores the evolving role of currency exchange not simply as a financial mechanism, but fundamentally as a human process. One that reflects our desires, fears, transitions and hopes for a more connected future.

Currency Exchange Is Not Just Economics, It's Human Movement

While numbers fluctuate on screens and markets shift by the minute, each transaction tells us something about people. It reveals migration patterns, education flows, investment trends and the way families support one another across borders.

As someone working closely with individuals and businesses making cross-border decisions, I've seen firsthand how emotional and complex these moments can be. A property purchase abroad might mean a retirement dream coming true. A series of transfers to another country may represent the start of a new life or business. In these moments, currency is not just money, **it's meaning**. And yet, much of this is hidden behind automation and buzzwords. The challenge isn't only technical, it's how we preserve agency and clarity in a financial world that feels increasingly distant.

Resilience in a Shifting Landscape

We often speak of "resilience" in economic terms. Systems that can withstand shocks, recover quickly, and continue to perform. But what does resilience mean for the individual navigating cross-border life? It could mean knowing when to exchange during volatile markets. Or having tools to plan long-term moves without losing sleep over rate swings. Sometimes, it's simply having someone to call - someone who understands both the spreadsheet and the story behind it.

When an American family moves to Portugal and needs to send funds monthly to support their life transition, it's not just about fees or speed. It's about trust. When a Canadian entrepreneur expands into Europe and needs to hedge against market risk, it's about strategy. And when a pensioner sells their home in the UK to settle in Portugal, it's about timing, security and peace of mind.

Tools Can Empower (If We Use Them Well)

Take Ana and Mark, for instance, who recently moved from the States to the Algarve. "*Navigating exchange rates while managing a property purchase and school fees abroad felt*

overwhelming - until we explored forward contracts and rate alerts tailored to our needs. The result wasn't just savings, but peace of mind."

The future of currency exchange will likely become more digital, more instant, and more embedded into platforms we use every day. But the real question is how we use these tools to empower people.

There are tools that, when used thoughtfully, can offer stability and confidence. A Spot Payment provides speed for urgent needs. A Forward Contract can protect a buyer from future volatility. Limit Orders offer choice, while Rate Alerts and Recurring Transfers bring structure. These aren't just financial instruments - they're **ways to plan with intention**.

These tools are available - but many people either aren't aware of them or aren't sure how to use them well. That's where a human voice still matters. Not to replace technology, but to interpret it. **To guide**, not to gatekeep.

If we pause to look forward (to 2030, say) and reflect on how financial tools evolved, what will we notice?

Perhaps we have become more global and mobile than ever before. That technology solved many problems but introduced new ones. That while we gained efficiency, we risked losing understanding.

In that sense, currency exchange acts as a litmus test for how we view finance, not just as transactions, but as **meaningful connections**. Do we see money as merely transactional, or as something that connects, protects, and enables human lives?

The deeper question isn't: "How do we move money?". **It's:** "How do we move through life, across borders, with agency and support?"

An Invitation to Rethink the Familiar

This isn't just a technical article. It's a small invitation to reimagine how we treat the everyday systems that enable movement, choice, and connection.

When we consider financial tools (from bank transfers to blockchain, from AI to smart contracts), let's remember the human in the loop. Let's design systems that support people not just as users, but as storytellers of their own journey. After all, currency may be numbers, but it is also narrative. A record of where we've been, and where we hope to go next.

But for any of this to matter, we need to stay close to what makes us human. At the core of every transfer, every decision, every risk taken across borders, is a desire to care - for family, for a future, for a better quality of life.

Currency exchange might feel technical on the surface, but beneath it lies something very tender: trust, emotion, and the hope that someone, somewhere, has your best interest at heart.

That's why human connection must remain central. It's not just about what we do, but how we do it - with empathy, clarity, and a commitment to listening. Tools should serve people, not the other way around. Technology can streamline, but it should never distance. If anything, our job as professionals is to ensure it brings us closer - to each other, and to the lives we're working to build. **Because at the end of the day, we are social beings, wired for relationship, and reliant on one another to thrive.**

RACHEL CANALES