CYBERLAW

BY CIJIC

DIREITO: A PENSAR TECNOLOGICAMENTE

EDIÇÃO N.º 12

FEVEREIRO 2024

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 XII – FEVEREIRO DE 2024

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

CYBERLAW

BY CIJIC

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

INDÍCE

EDUARDO VERA-CRUZ PINTO

Presidente da Direção do Centro de Investigação Jurídica do Ciberespaço – CIJIC

Breves Palavras de Reconhecimento

A Revista *Cyberlaw by CIJIC*, é uma publicação do Centro de Investigação Jurídica do Ciberespaço (CIJIC), criado no âmbito do Interdisciplinar da Faculdade de Direito da Universidade de Lisboa (IURIS), que funciona como uma montra científica da investigação dos seus membros e investigadores convidados.

Em 2012, concretizando uma proposta didática de pós-graduações, a Faculdade de Direito da Universidade de Lisboa avançou para o pedido de acreditação de um mestrado em Segurança de informação e Direito no Ciberespaço, em parceria com a com o Instituto Superior Técnico e a Escola Naval, que permitiu desenvolver a ligação da docência à investigação no âmbito de disciplinas integradas em um Plano de Estudos

inovador que combinava as dimensões teórico-dogmáticas com os aspetos técnico-práticos do exercício de profissões que suscitam tais competências[1].

Foi um momento inaugural nos estudos conferentes de grau sobre Direito da Cibersegurança, numa perspetiva interdisciplinar que parte de Escolas-âncoras de ensino superior universitário português no âmbito das ciências jurídicas e das tecnologias digitais.

A Revista Ciberlaw, iniciou a sua publicação em Janeiro de 2016, com material recolhido para publicação entre especialistas da sua área temática e de textos de alunos, indicados pelos docentes do Curso de 2º ciclo referido, aprovados pelos seus órgãos. A *Ciberlaw by CIJIC* foi fazendo o seu caminho, dirigida pelo Mestre Nuno Teixeira Castro, com o apoio da Direção do Centro, em qualidade crescente e internacionalização progressiva.

Agradecimentos são devidos a todos os que, com o seu trabalho, fizeram publicar estes 12 números da nossa Revista que se afirmou no mercado de revistas da especialidade, em Portugal e além-fronteiras, como uma ponte entre saberes e profissões, vencendo o estranhamento entre os mundos do Direito e das engenharias.

Um reconhecimento pessoal e institucional é devido ao Mestre Nuno Teixeira Castro, à Prof.ª Doutora Raquel Brízida Castro e ao Prof. Doutor Marco António Marques da Silva por tudo o que deram e representam para esta publicação. O mesmo em relação ao Prof. Doutor Nuno Guimarães e ao Dr. Afonso de Freitas Dantas que têm nos últimos anos colaborado no CIJIC e na sua Revista, com uma entrega e entusiasmo que não posso deixar de lembrar.

Num ano em que a Faculdade de Direito da Universidade de Lisboa acaba de comemorar os seus 110 anos e em que se abre um ciclo de governo da Escola marcado pela inovação e transição nas várias frentes do ensino do Direito, da responsabilidade social da sua comunidade académica e de projetos de investigação aplicada e extensão universitária não podemos deixar de olhar com orgulho para os passos percorridos com

1 Despacho nº 9702/2014, Criação de Novo Ciclo de Estudos, Mestrado em Segurança da Informação e Direito do Ciberespaço, in Diário da república, 2ª série, nº 143, de 28 de Julho de 2014, pp. 19259-19261; e Despacho nº 11914/2021, in DR, nº 233, 2ª Série, Parte E, de 2 de Dezembro de 2021, 149~152.

os colegas e amigos nestes últimos 13 anos de instalação de Cursos sobre Tecnologia e Direito, centrados na problemáticas da Cibersegurança.

Só resta desejar uma longa vida e muitos êxitos à Revista *Ciberlaw by CIJIC*.

NUNO M. GUIMARÃES

Presidente da Comissão Científica do Centro de Investigação Jurídica do Ciberespaço – CIJIC

Mensagem

A revista *Cyberlaw by CIJIC*, publicação do Centro de Investigação Jurídica do Ciberespaço, uma área temática do IURIS, centro de investigação da Faculdade de Direito da Universidade de Lisboa, renova-se, reapresenta-se e reitera a sua perspetiva de convergência entre o direito e a tecnologia, esta entendida aqui como a que realiza a sociedade de informação ou digital ou em rede (*M. Castells, a Sociedade em Rede*) ou *info-esfera* (*L.Floridi, The Fourth Revolution*).

As tecnologias de informação, relativamente às quais podemos hoje, e já com alguma distância, fixar momentos históricos significativos – há 75 anos (1947) a invenção do transístor (*AT&T Bell Laboratories*), há 55 (1969) o nascimento da Internet

(*DARPA*), há 35 (1989) a criação da *World Wide Web* (*CERN*) – transformaram as formas de comunicação, produção e disseminação do conhecimento, negócios e cadeias de valor e, genericamente, a realidade social e económica com impacto nas ordens sociais estabelecidas, nomeadamente na ordem jurídica, em âmbito nacional ou internacional.

O progresso tecnológico, interpretado nos últimos dois séculos com um imanente positivismo que assume justificação social *ex-ante* e crítica e controlo apenas *ex post*, constitui uma fonte aparentemente inesgotável de factos sociais (no sentido de J.Habermas, *Between Facts and Norms*) que transformam as relações entre privados e os próprios conteúdos dos direitos fundamentais e do poder do Estado, do que são exemplo o impacto nas relações contratuais e comerciais, nas liberdades fundamentais de expressão ou participação política, ou mesmo dos direitos de personalidade.

A inovação tecnológica criadora de produtos, serviços, meios e capacidades, num tecido social e económico global, geralmente incapaz de desenvolver respostas imunológicas equilibradas, aumenta a entropia, ou desordem, de sociedades e Estados, e estabelece um quadro de normas de facto, frequentemente em contradição com normas sociais estabelecidas. A lei, entre factos e normas é chamada a assumir o contraponto, desejavelmente democrático, à normatividade emergente por via tecnológica (*M. Ketterman, The Normative Order of the Internet*). Esta normatividade emergente das é dialecticamente confrontada com a reação, positiva ou jurisprudencial, do direito, num quadro de regulação de âmbito global também entendido geopoliticamente (*Anu Bradford, Digital Empires*).

Num quadro de intensa, senão mesmo frenética, regulação – só na EU e recentemente e entre outras leis: o Regulamento Geral de Proteção de Dados, Regulamentos dos Serviços Digitais e dos Mercados Digitais, Regulamento da Inteligência Artificial – com consequências jurídicas de largo espectro – desde as leis comuns até quadros constitucional (*Raquel B. Castro, Direito Constitucional: Ciberespaço e Tecnologia)* – a revista *Cyberlaw by CIJIC*, cuja primeira publicação ocorreu em Janeiro de 2016, adquire uma posição reforçada nesta área de interseção científica, académica e intelectual, ajudando a criar um terreno de intercompreensão sólido entre protagonistas da inovação tecnológica – vulgarmente conhecidos como

engenheiros – e atores da lei e do direito – estes conhecidos como juristas. Ambos tendem a trivializar o domínio de conhecimento da outra parte – opinião pessoal.

Cada publicação na *Cyberlaw by CIJIC* é uma manifestação da ligação entre o desenvolvimento tecnológico e o desenvolvimento jurídico. A reflexão estruturada sobre esta ligação deve estimular a inclusão – por conceção (*by design*) – de elementos jurídicos na inovação e a produção de normas jurídicas com consciência da realidade, potencial e limites das tecnologias. A Comissão Científica do CIJIC, criada em 2023, tem também essa dupla orientação em mente e deseja que a revista *Cyberlaw by CIJIC* continue a ser um fator de consolidação desta convergência.

Breves Notas Interlocutórias

Volvidos quase três anos desde a sua última publicação, a revista digital *Cyberlaw by CIJIC* regressa com nova imagem e de espírito reforçado.

Estes últimos anos foram de mudança. Acelerada. Para todos. No plano concreto, também o foram para o Centro de Investigação Jurídica do Ciberespaço (CIJIC). Alterações internas, de funcionamento, revisão dos seus estatutos, entrada em funções de uma nova Direcção, novo *url* e a celebração variada de acordos com entidades fraternas, destacando-se o Brasil.

O que estava bem, assumimos a sua perseverança. O que nos pareceu carecer de estímulo primaveril, suscitamos renovação. Apesar de contarmos com mais de uma década de existência, as renovações são necessárias à caução de qualidade de um centro de investigação, acautelando que nunca ficaremos estagnados no tempo, modo, e acção face a um mundo em ininterrupta mutação.

Entrando agora em 2024, tendo a Faculdade de Direito da Universidade de Lisboa acabado de celebrar os seus 110 anos de história, aparentou-nos oportuno conjungir a efeméride com a renovação. Trazer um novo rosto à *Cyberlaw by CIJIC* – cujo labor e existência aspiram a vanguarda dos debates científico-jurídicos da tecnologia e do ciberespaço – afigurou-se-nos como pedra fundacional do rejuvenescimento. Neste sentido, gostaríamos de agradecer à Margarida Ferreira, autora deste rejuvenescimento do rosto da revista.

Discorrida a súmula da renovação, entremos na recensão da XII Edição. Com a ascensão da Inteligência Artificial, somos a notar o avanço, de forma antecipada, nos teatros de guerra. Disruptivo. O recurso a sistemas de defesa e segurança cibernética, evoluindo pela criação de armamentos não tradicionais, manifestadas no recurso exaustivo a *drones* ou no desenvolvimento de armas automatizadas e autónomas - estimuladas por *software* inteligente e passível de operar de forma independente - estão a mudar o histórico conservadorismo de operações militares. A tecnologia suplanta a necessidade de *homens no terreno*.

De feitio cotejável, outras exteriorizações de *software* inteligente viabilizam abundante compressão de liberdades fundamentais humanas. Não só um cerco securitário, como um controlo e/ou atribuição de crédito social à cidadania, por exemplo, na República Popular da China. Mas não só.

Na verdade, a compressão de direitos e liberdades fundamentais da pessoa humana tem conhecido múltiplas e variadas manifestações. Ressonâncias demonstráveis tanto através de um *capitalismo de vigilância*, como também através de um *Estado vigilante*[1], cada vez mais hospedado até em democracias ocidentais, pontuadamente menos liberais mas mais musculadas. Uma evolução da comunidade alicerçada numa miríade informacional: *uma sociedade da informação* espelhada na sociedade em rede[2].

---

1 Sobre o tema abrangente do discurso de ódio na internet, vide, por exemplo, @ https://www.coe.int/en/web/combating-hate-speech/council-of-europe-on-hate-speech#{%22216925596%22:[0],%22226902653%22:[0],%22226902685%22:[0],%22226902971%22:[0]} – último acesso Janeiro 2024.

2 «*We are just entering a new stage in which culture refers to culture, having superseded nature to the point that nature is artificially revived("preserved") as a cultural form: this is in fact the meaning of the environmental movement, to reconstruct nature as an ideal cultural form. Because of the convergence of historical evolution and techno-logical change we have entered a purely cultural pattern of social interaction and social organization*. ***This is why information is the key ingredient of our social***

Vários têm sido os pretextos apresentados para consumar o (este) crescente emascular de direitos e liberdades fundamentais. Em abono da verdade, a complexidade informacional serve múltiplos propósitos. Cumprirá, contudo, ao Direito, e aos seus cultores, a constante flexibilização de raciocínio almejando compreender as implicações de tais pretextos ante as novas tecnologias e os impactos de ambos no quotidiano das pessoas e nas suas mais variadas ficções por onde se organizam na sociedade. A salvaguarda e promoção da dignidade da pessoa humana reclamam tal ininterrupto esforço.

Ademais, *hic et nunc* esta expansão informacional arroja o colóquio. Não fátuo. Não frívolo. Numa sociedade do instantâneo, do momento efémero, superficial e petulante, a razão reclama Tempo. Um tempo natural do raciocínio. Desprendido de amarras castradoras. CASTELS, de forma pungente, sintetiza o *status quo*: «(…) *The social construction of new dominant forms of space and time develops a meta-network that switches off non-essential functions, subordinate social groups, and devalued territories. By so doing, infinite social distance is created between this meta-network and most individuals, activities, and locales around the world. Not that people, locales, or activities disappear. But their structural meaning does, subsumed in the unseen logic of the meta-network where value is produced, cultural codes are created, and power is decided. The new social order, the network society, increasingly appears to most people as a meta-social disorder*[3]*»*.

O jurista, o cultor do Direito, não vive sozinho no mundo. No mundo actual, sobressaído desta *meta-social disorder*, de múltiplos "*pós*", também o Direito reclama uma *pós-disciplinaridade*[4]. Aos seus cultores açula-se um estádio de conhecimento que não deve estar delimitado por fronteiras disciplinares. Um conhecimento de abertura *aduaneira* onde *tudo pode passar desde que obtenha passaporte e tenha visto de entrada*[5]. Um conhecimento cuja propriedade de *vários elementos ou de várias partes*

---

organization and why flows of messages and images between networks constitute the basic thread of our social structure.» (negrito nosso)
- Castells, M. (2009). Conclusion: The Network Society. In The Rise of the Network Society, M. Castells (Ed.). pgs. 507/509.

3 Castells, M. (2009). Conclusion: The Network Society. In The Rise of the Network Society, M. Castells (Ed.)., pgs. 507/509.

4 Cunha, Paulo Ferreira da, Teoria Geral do Direito: Uma Síntese Crítica, A Causa das Regras, 2018 - (*pág.* 44).

5 *Idem*.

(almeja) alcançar um resultado melhor ou maior do que a mera soma das partes individualmente materializadas.

De facto, a *bonomia* com que nos presenteiam, com tanta e tamanha regulação das relações, mascara este emascular de direitos e liberdades fundamentais. Apresentam-nos pretextos vários para consumarem as compressões. De forma paternalista, como se a esmagadora maioria dos seres humanos estivesse desprovida de racionalidade, bombardeiam-nos com copiosas e garbosas motivações. De sustentabilidade social e ambiental[6], benevolentes[7] [8], cândidas[9] [10], e (porque não) puras [11], tal como o sorriso de uma criança[12], enquanto, no plano fáctico, a tentação para nos cercear[13], confinar[14], dominar[15], controlar[16], qual gado de corte, vai recrudescendo.

Cum granu salis, o advento (*hype*) da inteligência artificial – o *software* – consolidado numa crescente capacidade e complexidades computacionais (de novéis

---

6 «*Environmental, social and governance (ESG) ratings provide an opinion on a company or financial instrument's sustainability profile or characteristics, exposure to sustainability risks or impact on society and/or the environment*», @ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13330-Sustainable-finance-environmental-social-and-governance-ratings-and-sustainability-risks-in-credit-ratings_en - ultimo acesso Janeiro 2024.

7 Council of Europe on hate speech. @ https://www.coe.int/en/web/combating-hate-speech/council-of-europe-on-hate-speech#{%22216925596%22:[0],%22226902653%22:[0],%22226902685%22:[0],%22226902971%22:[0]} - último acesso Janeiro 2024.

8 *Private communication is a fundamental human right.* @ https://www.eff.org/deeplinks/2023/12/fighting-european-threats-encryption-2023-year-review - último acesso Janeiro 2024.

9 Vide por exemplo: « *The EU must ensure no gaps in the protection of children against child sexual abuse online* » @ https://www.eurochild.org/news/the-eu-must-ensure-no-gaps-in-the-protection-of-children-against-child-sexual-abuse-online/ - último acesso Janeiro 2024.

10 *Child sexual abuse material: Spanish Presidency floats limiting detection orders' scope.*@ https://www.euractiv.com/section/law-enforcement/news/child-sexual-abuse-material-spanish-presidency-floats-limiting-detection-orders-scope/ - último acesso Janeiro 2024.

11 «*Combating child sexual abuse online*», @ https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf - último acesso Janeiro 2024.

12 «*New legislation to fight child sexual abuse online, In "Promoting our European Way of Life"*» https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-combating-child-sexual-abuse-online - - último acesso Janeiro 2024.

13 *EU: Artificial Intelligence Regulation Should Ban Social Scoring*. @ https://www.hrw.org/news/2023/10/09/eu-artificial-intelligence-regulation-should-ban-social-scoring último acesso Janeiro 2024.

14 *The shadow of social credit looms over Europe*. @ https://incyber.org/en/the-shadow-social-credit-looms-europe/ - - último acesso Janeiro 2024.

15 *Personal Scoring in the EU: Not quite Black Mirror yet, at least if you're rich*. @ https://algorithmwatch.org/en/personal-scoring-in-the-eu-not-quite-black-mirror-yet-at-least-if-youre-rich/ - último acesso Janeiro 2024.

16 *Internet censorship and surveillance in Europe*. @ https://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_in_Europe#Little_or_no_censorship_or_surveillance - último acesso Janeiro 2024.

habilitações)[17] [18], com efeito, alardeiam, *Ipso facto*, um potencial de risco novo, ignoto, surpreendente à *sociedade em rede*. O risco é imanente a esta sociedade, tal como BECK a categorizou[19]. E nesta sociedade de risco, em rede, cujas ameaças, as fontes do perigo, *não são mais a ignorância, mas o conhecimento*, teremos ainda ensejo para suscitar a *dúvida metódica*? Teremos ainda tempo e espaço para nos libertarmos dos preconceitos, para desviarmos o espírito dos sentidos, para assumirmos o *cogito ergo sum* de Descartes?

É nesta consciência, exortados por um sentido de dúvida constante e insatisfeita, aguçada pelos desafios, riscos, ameaças, mas também oportunidades e quimeras, que se descerram todos os dias, que voltamos aqui para publicar e fomentar discussões fundamentais e imprescindíveis. Nas lições de CUNHA[20]: «*Interessa menos se determinado saber pertence a este ou aquele quintal, desde que se saiba esse saber.*» Como as margens de um rio banhado pela *episteme* do Direito. Com a *Cyberlaw by CIJIC*, e com o Direito: a pensar tecnologicamente.

Faculdade de Direito da Universidade de Lisboa

Instituto de Investigação Interdisciplinar do Direito - IURIS

Centro Investigação Jurídica do Ciberespaço - CIJIC

Fevereiro de 2024

NUNO TEIXEIRA CASTRO & AFONSO DE FREITAS DANTAS

---

17 *Deepfakes being used in 'sextortion' scams, FBI warns*. @ https://www.theregister.com/2023/06/08/ai_deepfakes_sextortion_fbi/- último acesso Janeiro 2024.

18 *X blocks Taylor Swift searches: What to know about the viral AI deepfakes*. @ https://www.aljazeera.com/news/2024/1/29/x-blocks-taylor-swift-searches-what-to-know-about-the-viral-ai-deepfakes - último acesso Janeiro 2024.

19 «*In contrast to all earlier epochs (including industrial society), the risk society is characterized essentially by a Jack: the impossibility of an external attribution of hazards. In other words, risks depend on decisions; they are industrially produced and in this sense politically reflexive. While all earlier cultures and phases of social development confronted threats in various ways, society today is confronted by itself through its dealings with risks.* ***Risks are the reflection of human actions and omissions, the expression of highly developed productive forces. That means that the sources of danger are no longer ignorance but knowledge****; not a deficient but a perfected mastery over nature; not that which eludes the human grasp but the system of norms and objective constraints established with the industrial epoch. Modernity has even taken over the role of its counterpart - the tradition to be overcome, the natural constraint to be mastered.*»(negrito nosso). – Beck, Ulrich. Risk Society: Towards a New Modernity. - (Theory, Culture & Society Series). (pág. 183).

20 Cunha, Paulo Ferreira da, Teoria Geral do Direito: Uma Síntese Crítica, A Causa das Regras, 2018 - (pág. 106).

Os Contratos à Distância

JOSÉ ENGRÁCIA ANTUNES

SUMÁRIO: 1. Aspetos Gerais; 1.1. Noção Preliminar; 1.2. Razão de Ser; 2. Fontes; 2.1. Fontes Nacionais e Europeias; 2.2. Outras Leis; 3. Requisitos; 3.1. Requisitos Subjetivos; 3.2. Requisitos Objetivos; 3.3. Requisitos Operacionais; 4. Modalidades; 4.1. Contratos por Correspondência Postal; 4.2. Contratos por Telefone; 4.3. Contratos por Meios Audiovisuais; 4.4. Contratos Eletrónicos; 5. Negociação; 5.1. Deveres Gerais de Informação; 5.2. Deveres Especiais nos Mercados em Linha; 5.3. Regime; 5.4. Outros; 6. Formação; 6.1. Princípio Geral; 6.2. Regras Especiais; 7. Cumprimento; 7.1. Confirmação do Conteúdo Contratual; 7.3. Transferência da Propriedade e do Risco; 7.4. Outros Aspetos; 8. Extinção; 8.1. O Direito de Desistência; 8.2. Prazo; 8.3. Modalidades; 8.4. Natureza; 8.5. Efeitos; 8.6. Exceções; 9. O Caso Particular dos Serviços Financeiros à Distância; 9.1. Aspetos Gerais; 9.2. Âmbito de Aplicação; 9.3. Regime Aplicável; Abreviaturas e Bibliografia

1. Aspetos Gerais

1.1. Noção Preliminar

I. Designa-se por contrato à distância ("distance contract", "Fernabsatzvertrag", "contratto a distanza", "contrat à distance", "contrato a distancia") o *contrato entre um empresário e um consumidor que, tendo por objeto o fornecimento de bens ou a prestação de serviços, foi celebrado no âmbito de um sistema organizado de negociação de comércio à distância, sem a presença física simultânea dos contraentes*.[1]-[2]

1 Sobre a figura, vide CARVALHO, J. MORAIS, *Prestação de Informações nos Contratos Celebrados à Distância*, in: AA.VV., "Direito Privado e Direito Comunitário", 13-144, Âncora Editora, Lisboa, 2009; CHEN, CHEN, *Contratos à Distância em Geral*, in: Ataíde, R./ Rocha, F./ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. I, 777-801, Lisboa, 2023; CORREIA, M. PUPO, *Contratos à Distância: Uma Fase na Evolução da Defesa do Consumidor na Sociedade de Informação?*, in*:* 4 "Estudos de Direito do Consumidor" (2002), 165-180; DINIS, MARISA, *Contratos Celebrados à Distância e Contratos Celebrados Fora do Estabelecimento Comercial*, in: 77 "Revista Portuguesa de Direito do Consumo" (2014), 11-38; DUARTE, MARIANA, *O Novo Regime dos Contratos Celebrados à Distância e Fora do Estabelecimento Comercial: Reforço da Protecção do Consumidor?*, in: 2 "Ab Instantia - Revista do Instituto do Conhecimento AB" (2014), 115-119; FROTA, MÁRIO, *Contrato à Distância: O Contrato de Seguro,* in: 35 "Revista Portuguesa de Direito do Consumo" (2003), 13-26; MARTINS, A. SOVERAL, *Contratação à Distância e Contrato de Seguro,* in: 10 "Estudos de Direito do Consumidor" (2016), 91-153; MAIA, PEDRO, *Contratação à Distância e Práticas Comerciais Desleais,* in: 9 "Estudos de Direito do Consumidor" (2015), 143-175; MARTINEZ, P. ROMANO, *Celebração de Contratos à Distância e o Novo Regime do Contrato de Seguro*, in: 50 "Revista de Direito e de Estudos Sociais" (2009), 85-116; MOREIRA, TERESA, *Novos Desafios para a Contratação à Distância – A Perspetiva da Defesa do*

1.2. Razão de Ser

I. É sabido que o modelo tradicional da contratação mercantil se caraterizava pela presença física e interação pessoal entre comerciantes e clientes. Inicialmente, o comércio era quase exclusivamente realizado nos estabelecimentos comerciais, traduzindo-se as relações de consumo em contratos entre os comerciantes e os consumidores celebrados nas instalações ou ao balcão do estabelecimento comercial. Mais tarde, fruto de novas técnicas de venda a retalho e de promoção comercial, tais contratos passaram a ser também celebrados fora do próprio estabelecimento comercial, noutros locais públicos ou privados, tais como o domicílio ou local de trabalho do consumidor, em excursões, reuniões e eventos, na via pública, etc.[3]

II. Fruto do desenvolvimento das novas tecnologias (em particular, das tecnologias da computação, informação e comunicação) e da subsequente emergência de uma "economia digital", o mundo vivo da contratação mercantil – e com ela, a contratação de consumo – entrou numa nova etapa no virar do presente século, na qual os contratos entre empresários e consumidores são negociados e concluídos *sem qualquer relação de imediação física e simultânea das partes contratantes*.

III. Hoje, vai sendo cada vez mais raro que a compra de um produto alimentar, de um eletrodoméstico, de uma peça de vestuário, de um livro, de uma viagem turística, de

---

Consumidor, in: 9 "Estudos de Direito do Consumidor" (2015), 19-36; MONTEIRO, A. PINTO, *O Novo Regime da Contratação à Distância,* in: 9 "Estudos de Direito do Consumidor" (2015), 11-18; OLIVEIRA, A. FILIPE, *Dos Contratos Negociados à Distância,* in: 7 "Revista Portuguesa de Direito do Consumo" (1996), 52-96; PINTO, P. MOTA, *O Novo Regime Jurídico dos Contratos à Distância e dos Contratos Celebrados Fora do Estabelecimento Comercial,* in: 9 "Estudos de Direito do Consumidor" (2015), 51-91; PINTO, P. MOTA, *Princípios Relativos aos Deveres de Informação no Comércio à Distância*, in: 5 "Estudos de Direito do Consumidor" (2003), 183-206; PINTO-FERREIRA, J. PEDRO/ CARVALHO, J. MORAIS, *Contratos Celebrados à Distância e Fora do Estabelecimento Comercial,* Almedina, Coimbra, 2014; REBELO, F. NEVES, *O Direito à Informação do Consumidor nos Contratos à Distância,* in: "Liber Amicorum Mário Frota*"*, 103-153, Almedina, Coimbra, 2012; SILVA, D. SOUSA, *Contratos à Distância – O Ciberconsumidor,* in: 5 "Estudos de Direito do Consumidor" (2003), 423-456; SOUSA, A. TEIXEIRA, *O Direito de Arrependimento nos Contratos Celebrados à Distância e Fora do Estabelecimento: Algumas Notas*, in: "Estudos de Direitos do Consumo: Homenagem a M. Ataíde Ferreira, 18-41, Almedina/ Deco, Lisboa, 2016. Para um apanhado jurisprudencial, vide PASSINHAS, SANDRA, *Jurisprudência Relevante em Matéria de Contratação à Distância*, in: 9 "Estudos de Direito do Consumidor" (2015), 251-277.

2 Noutros ordenamentos jurídicos estrangeiros, vide BRUNAUX, GEOFFRAY, *Le Contrat à Distance au XXIème Siècle*, LGDJ, Paris, 2010; COEHEN-ADT, GREGOR, *Der Fernabsatzvertrag: Anwendungsvoraussetzungen und -probleme beim Versandhandel*, Logos, Berlin, 2009; FRATERNALE, ANTONIO, *I Contratti a Distanza*, Giuffrè, Milano, 2002; PÉREZ, N. FERNÁNDEZ, *El Nuevo Régimen de Contratación a Distancia con Consumidores*, La Ley, Madrid, 2009

3 Sobre os contratos fora do estabelecimento comercial, que constituem também um tipo especial dos contratos de consumo, vide ANTUNES, J. ENGRÁCIA, *Os Contratos Fora do Estabelecimento,* in: Ataíde, R./ Rocha, F./ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. I, 767-775, Lisboa, 2023.

ações de uma empresa, e de tantos outros bens ou serviços no mercado, implique a deslocação física do adquirente à empresa produtora, fornecedora, distribuidora, retalhista ou vendedora. De facto, a aplicação criativa das novas tecnologias de comunicação às transações comerciais – desde a primitiva correspondência comercial (v.g., cartas normalizadas e catálogos), passando por meios de comunicação como o telefone ("call centers"), a rádio ("radio sales") e a televisão (v.g., televendas), até aos mais atuais correio eletrónico, páginas "web", redes sociais, plataformas digitais, ou mercados em linha – vem tornando tal hipótese cada vez menos frequente e mais remota.

2. Fontes

2.1. Fontes Nacionais e Europeias

I. Esta novel e primordial modalidade de contratação mercantil trouxe consigo novos desafios e riscos para o âmbito das relações jurídicas de consumo, dada a típica ausência de interação direta do consumidor, quer com a sua contraparte contratual (empresário/profissional), quer com o próprio objeto contratual (produtos ou serviços).

II. Não surpreende assim que os contratos de consumo à distância tenham sido objeto de uma disciplina jurídica própria, através da *Lei dos Contratos Celebrados à Distância e Fora do Estabelecimento Comercial* (doravante abreviadamente LCCD), aprovada pelo Decreto-Lei nº 24/2014, de 14 de fevereiro.[4]

III. A LCCD surgiu sob o direto impulso da legislação comunitária, mais concretamente da Diretiva 2011/83/EU, de 25 de outubro. Tal diretiva veio substituir e revogar a anterior Diretiva 97/7/CE, de 20 de maio, relativa à proteção dos consumidores nos contratos à distância. Esta diretiva houvera sido transposta para o direito português através do Decreto-Lei nº 143/2001, de 26 de abril – onde, pela

4 A LCCD viria a sofrer diversas alterações, introduzidas pela Lei nº 47/2014, de 28 de julho, pelos Decretos-Lei nº 78/2018, de 15 de outubro, nº 9/2021, de 29 de janeiro, e nº 109-G/2021, de 10 de dezembro, e ainda pela Lei nº 10/2023, de 3 de março.

primeira vez, a figura do contrato à distância fora objeto de uma disciplina jurídica própria –, o qual viria a ser revogado pela atual LCCD.[5]

2.2. Outras Leis

I. Sublinhe-se que este tipo especial de contrato de consumo, porque abrange todos as técnicas de comunicação à distância, poderá ainda concitar a aplicação simultânea de regulações legais específicas previstas para determinada *técnica comunicacional em particular*: pense-se, por exemplo, na contratação efetuada através de centros telefónicos de relacionamento ou "call centers" (cf. art. 2.º do Decreto-Lei nº 134/2009, de 2 de junho) ou através de televendas (arts. 2.º, nº 1, v), 40.º a 40.º-B da LTV). Particularmente relevante é a contratação realizada através da "internet", a qual origina um tipo especial e autónomo de contrato de consumo, que se encontra simultaneamente às disposições próprias previstas na LCE e na LDE: os chamados *contratos eletrónicos B2C*.[6]

II. Advirta-se que a disciplina dos contratos à distância prevista na LCCD se pode ainda entrecruzar com *outras leis consumeristas* ou pertinentes ao consumo. Pense-se, a título de exemplo, no regime da informação pré-contratual: para além das disposições centrais previstas na LCCD (arts. 4.º a 4.º-B), poderão ainda ser relevantes para a conformação dos deveres de informação prévios à celebração de um contrato celebrado à distância as disposições especiais previstas na LDC (art. 8.º), na LCCG (art. 5.º e 6.º), na LPCD (art. 9.º), na LComunE (art. 120.º), ou no RGPD (arts. 6.º e 13.º-A), já sem falar até nas próprias normas civis gerais (v.g., em sede da culpa "in contrahendo": cf. art. 227.º, nº 1 do CCivil)[7]. No comum dos casos, tais disposições serão complementares entre si, sendo simultaneamente aplicáveis: todavia, em caso de

5. Sobre o direito pretérito, pode ver-se ANTUNES, J. ENGRÁCIA, *Direito dos Contratos Comerciais*, 142 e ss., 7ª reimp., Almedina, Coimbra, 2021; OLIVEIRA, A. FILIPE, *Dos Contratos Negociados à Distância*, in: 7 "Revista Portuguesa de Direito do Consumo" (1996), 52-96; SILVA, F. SANTOS, *Dos Contratos Negociados à Distância*, in: 5 "Revista Portuguesa de Direito do Consumo" (1996), 45-58.

6 Sobre tais contratos, vide ANTUNES, J. ENGRÁCIA, *Os Contratos Eletrónicos B2C*, em curso de publicação.

7 Para um exemplo da interação entre a LCCD e outras leis, vide o Acórdão do TJUE de 24-II-2022 *(«Tiketa» UAB c. M. Š.*), a respeito da questão de saber se os deveres informativos do empresário/profissional podem ser cumpridos através da sua inclusão nas condições gerais do contrato de adesão celebrados em mercados em linha (in: ECLI:EU:C:2022:112).

conflito, afigura-se que as disposições da LCCD deverão, em princípio, prevalecer sobre as demais disposições setoriais conflituantes.[8]

III. Os contratos à distância possuem ainda outras importantes projeções jurídicas *não consumeristas*. Um exemplo provém do domínio do direito fiscal: com vista a simplificar o cumprimento das obrigações tributárias emergentes de vendas à distância, os legisladores europeu e português criaram o chamado "Balcão Único" ou "OSS – One Stop Shop", no qual se devem registar os empresários e outros sujeitos de IVA que efetuem vendas à distância a consumidores finais (Anexo I da Lei nº 47/2020, de 24 de agosto, Diretivas EU/2017/2455, de 5 de dezembro, e EU/2019/1995, de 21 de novembro).

3. Requisitos

I. O legislador previu a noção legal de contrato celebrado à distância no art. 3.º, h) da LCCD, que o define como "o contrato celebrado entre o consumidor e o fornecedor de bens ou o prestador de serviços sem presença física simultânea de ambos, e integrado num sistema de venda ou prestação de serviços organizado para o comércio à distância mediante a utilização exclusiva de uma ou mais técnicas de comunicação à distância até à celebração do contrato, incluindo a própria celebração" (art. 3.º, h) da LCCD).

II. Tomando por base esta definição legal, dir-se-ia que nos encontramos perante um contrato de consumo que exige a verificação cumulativa de três *requisitos* distintivos, de natureza subjetiva, objetiva e operacional.

3.1. Requisitos Subjetivos

I. "Primus", os contratos à distância têm como sujeitos ou partes o *empresário* – ou seja, a pessoa singular ou coletiva titular de empresa que, no âmbito da sua atividade profissional, diretamente ou através de terceiro, fornece os bens ou presta os serviços

8 Cf. também o art. 3.º, nº 2 da Diretiva 2011/83/UE: "Sempre que as disposições da presente directiva forem incompatíveis com as de outro instrumento da União que regule sectores específicos, as disposições deste outro instrumento da União prevalecem e aplicam-se a esses sectores específicos".

("fornecedor de bens" ou "prestador de serviços": cf. art. 3.º, h) da LCCD)[9] – e o *consumidor* – ou seja, qualquer pessoa singular atuando com fins que não se integrem no âmbito de uma atividade comercial, industrial, artesanal ou profissional (art. 3.º, e) da LCCD). Aspeto importante é o de que estão aqui também abrangidos, não apenas os contratos celebrados pelo empresário em nome próprio, mas também através de terceiros "que atuem em seu nome ou por sua conta" (art. 3.º, h), "in fine", da LCCD). Esta extensão do âmbito subjetivo pode ser particularmente relevante no domínio dos mercados em linha, incluindo no caso de plataformas digitais que intermedeiam o relacionamento entre empresários e consumidores.[10]

II. Decisivo – e nota distintiva desta figura contratual – é que o contrato tenha sido celebrado *sem a presença física* simultânea de ambas as partes contratantes, mediante a utilização exclusiva de uma ou mais técnicas de comunicação à distância, v.g., carta normalizada, catálogos, videotexto, telefone fixo, telemóvel, mensagens gravadas, SMS, "fax", correio eletrónico, rádio, televisão, redes sociais, "internet", etc. (art. 3.º, e), h) e w) da LCCD). Este requisito distingue justamente os contratos à distância dos contratos fora do estabelecimento, distinção esta que, todavia, não pode ser reconduzida à tradicional divisão entre contratos entre presentes e entre ausentes: com efeito, esta última não se baseia no critério da imediaticidade física dos contratantes, mas antes na imediaticidade temporal das respetivas declarações negociais (v.g., um contrato celebrado por telefone, videoconferência ou "internet" entre dois indivíduos será um contrato "inter presentes", enquanto um outro concluído presencialmente entre dois

9 Apesar da terminologia utilizada pelo legislador, mostra a experiência que, na esmagadora maioria dos casos, os fornecedores ou prestadores constituirão empresários individuais ou coletivos – circunstância esta que, de resto, transparece inequivocamente da própria disciplina legal, que se refere amiúde às "*empresas* fornecedoras" (arts. 20.º, nos 1 e 3, 21.º, nº 1, a), 23.º, nº 2, a) e b) da LCCD). Sobre esta prominência da figura do empresário como contraparte ou sujeito passivo das relações de consumo, vide ANTUNES, J. ENGRÁCIA, *Direito do Consumo*, 56 e ss., Almedina, Coimbra, 2019.

10 Sublinhe-se que, de acordo com a jurisprudência europeia, para efeitos do cumprimento dos deveres de informação pré-contratual, devem considerar-se também aqui abrangidos os prestadores de serviços em linha e os intermediários de plataformas digitais que atuam em nome do empresário/profissional (Acórdão do TJUE 24-II-2022 *(«Tiketa» UAB c. M. Š.*), in: ECLI:EU:C:2022:112. Para outras projeções da intermediação em linha, vide DODSWORTH, TIMOTHY, *Intermediaries as Sellers – A Commentary on «Wathelet»*, in: 5 "Journal of European Consumer and Market Law" (2017), 213-215; na jurisprudência, vide os Acórdãos do TJUE de 9-XI-2016 (*Sabrina Wathelet c. Garage Bietheres & Fils SPRL*), in: ECLI:EU:C:2016:840, e de 30-III-2017 (*Verband Sozialer Wettbewerb*), in: ECLI:EU:C:2017:243.

indivíduos que emitiram as suas declarações em momentos diferentes será um contrato "inter absentes").[11]

3.2. Requisitos Objetivos

I. "Secundus", os contratos à distância poderão ter por objeto, em princípio, quaisquer *bens ou serviços* negociados por aquele empresário (arts. 2.º e 3.º, h) da LCCD).

II. Em abstrato, estará aqui abrangida a *generalidade dos bens móveis corpóreos e dos serviços*, incluindo os bens em segunda mão, a água, gás e eletricidade quando colocados em venda num volume limitado ou em quantidade determinada, e os bens com elementos digitais (isto é, que incorporem ou estejam interligados com um conteúdo ou serviço digital) (art. 3.º, a) e k) da LCCD).

III. Do mesmo modo estará aqui abrangida a generalidade dos contratos, típicos ou atípicos, que tenham por objeto o fornecimento de bens ou a prestação de serviços (v.g., compra e venda, fornecimento, empreitada, locação) (art. 3.º, j), n) e k) da LCCD), incluindo os contratos sobre *bens e serviços de natureza digital* sem suporte material cuja contraprestação consiste em dados pessoais (arts. 2.º, nº 2, 3.º, f), l) e u) da LCCD): são assim relevantes os contratos que tenham por objeto conteúdos digitais (v.g., programas informáticos, aplicações informáticas, ficheiros de vídeo ou áudio, livros eletrónicos)[12] ou serviços digitais (v.g., partilha de "software", alojamento de ficheiros, serviços de armazenagem em nuvem).[13]

IV. Enfim, estarão aqui também abrangidos os *contratos mistos* – que tenham por objeto simultaneamente bens e serviços (v.g., aquisição de telemóvel inteligente com

11 Sobre tal distinção, vide FERNANDES, L. CARVALHO, *Teoria Geral do Direito Civil*, vol. II, 92 e ss., 5ª edição, UC Editora, Lisboa, 2010.

12 Ao passo que para efeitos da LCCD apenas são relevantes os conteúdos digitais fornecidos em linha ("online"), a LVBC já conferiu relevância aos conteúdos digitais fornecidos com suporte material ou "off line", v.g., DVD, CD, chaves USB, cartões memória (cf. arts. 3.º, nº 3, d) e 37.º, nº 2).

13 Sobre a noção de conteúdos digitais e serviços digitais, vide ANTUNES, J. ENGRÁCIA, *A Compra e Venda de Consumo*, em curso de publicação; CARVALHO, J. MORAIS, *Compra e Venda e Fornecimento de Conteúdos e Serviços Digitais – Anotação ao Decreto-Lei nº 84/2021, de 18 de Outubro*, 22 e s., Almedina, Coimbra, 2022. A distinção entre conteúdos digitais e serviços digitais é relevante, mormente para efeitos do direito de desistência do consumidor, que inexiste no caso de contratos de fornecimento de conteúdos digitais em linha (art. 17.º, nº 1, l) da LCCD): sustentando uma interpretação restritiva desta exceção, vide o Acórdão do TJUE de 8-X-2020 (*EU c. PE Digital GmbH*), in: ECLI:EU:C:2020:808 [§§ 41 a 46].

serviço de comunicações eletrónicas)[14] – e os contratos *onerosos ou "gratuitos"*, "rectius", os contratos em que a contraprestação do consumidor consista no pagamento de um preço ou na disponibilização dos seus dados pessoais (arts. 2.º, nº 2, arts. 6.º, nº 1, a) e 7.º do RGPD).[15]

V. É mister sublinhar, por outro lado, que a lei previu um importante conjunto de *exclusões* que importa ter presente: com efeito, não se encontram sujeitos a esta disciplina legal os contratos que tenham por objeto (i) serviços financeiros, (ii) máquinas automáticas, (iii) determinados serviços de telecomunicações (iv), bens imóveis, (v) serviços sociais, (vi) serviços de saúde, (viii) jogos de fortuna ou azar, (viii) viagens organizadas, (ix) direitos reais de habitação periódica, (x) direitos de habitação turística, (xi) fornecimento de géneros alimentícios e outros fornecidos regularmente ao consumidor, e (xii) determinados serviços de transporte de passageiros (art. 2.º, nºs 3 e 4 da LCCD)[16]. Sublinhe-se que uma boa parte destes contratos é objeto

14 A qualificação de tais contratos como de compra e venda ou de prestação de serviços (relevante para certos efeitos do regime aplicável, v.g., transferência do risco, prazos de desistência) deverá realizada tomando em consideração o seu objeto principal: assim, por exemplo, será de qualificar de compra e venda o contrato de aquisição de mobiliário de cozinha que inclui um serviço de instalação, mas de prestação de serviços a realização de um curso de formação que inclui a entrega de materiais de apoio aos participantes. A este respeito, vide os Acórdãos do TJUE de 26-V-2005 (*Marcel Burmanjer e o.*), in: ECLI:EU:C:2005:30 [§§ 24 a 35], de 2-XII-2010 (*Ker-Optika c. ÀNTSZ*), in: ECLI:EU:C:2010:725 [§ 43] e de 14-V-2020 (*NK c. MS e AS*), in: ECLI:EU:C:2020:382 [§§ 58-59].

15 É sabido que um número crescente de contratos de conteúdos e serviços digitais, sendo aparentemente gratuitos (no sentido em que não envolvem o pagamento de qualquer quantia pecuniária), têm na verdade como contrapartida a aceitação por parte do consumidor da disponibilização ao empresário prestador do acesso aos seus dados pessoais (v.g., identidade, idade, profissão, contactos, preferências, localização): tais contratos encontram-se também abrangidos pela LCCD. Inversamente, já são irrelevantes estes efeitos aqueles contratos em que os dados pessoais facultados pelo consumidor sejam destinados exclusivamente a assegurar o fornecimento conforme dos conteúdos ou serviços digitais ou o cumprimento dos próprios requisitos legais a que está sujeito ao prestador do serviço, não sendo utilizados para quaisquer outros fins (art. 2.º, nº 2, "in fine", da LCCD, art. 6.º, nº 1, b) e c) do RGPD). Tal não significa, naturalmente, que não continuem a ser aplicáveis nestes casos as disposições gerais do RGPD: na prática, vale por dizer, designadamente, que sempre inexista consentimento do consumidor, as operações de tratamento dos seus dados pessoais terão sempre de assentar num dos outros fundamentos jurídicos previstos na lei (art. 6.º). Sobre os dados pessoais como contraprestação dos contratos de consumo, vide BETTENCOURT, M. ORTINS, *A Proteção do Consumidor em Contratos Digitais: Análise dos Contratos Celebrados com Dados Pessoais como Contraprestação*, in: 3 "Anuário do Nova Consumer Lab" (2021), 387-476; FARINHA, MARTIM, *Os Limites da Proteção dos Consumidores no Regime de Tratamento de Dados Pessoais Contraprestação na Diretiva (EU)2019//770*, in: AA.VV., "Diretivas 2019/770 e 2019/771 e Decreto-Lei n.º 84/2021", 143-185, Almedina, Coimbra, 2022.

16 Esta exclusões ou exceções devem ser objeto de uma interpretação estrita: cf. Acórdão de 15-IV-2010 (*E. Friz GmbH c. Carsten von der Heyden*), in: ECLI:EU:C:2010:186 [§32]. Para algumas ilustrações jurisprudenciais, vide, a respeito dos contratos sobre bens imóveis, o Acórdão do TJUE de 14-V-2020 (*NK c. MS e AS*), in: ECLI:EU:C:2020:382 [§§ 43], e, de contratos de transporte de passageiros, o Acórdão do TJUE de 12-III-2020 (*Verbraucherzentrale Berlin c. DB Vertrieb GmbH*), in: ECLI:EU:C:2020:199 [§ 35].

de disciplina consumerista própria[17]: é o caso dos contratos de *serviços financeiros à distância* (Decreto-Lei nº 95/2006, de 29 de maio)[18], *viagem organizada* (art. 2.º, nºs 2, h) e 4 da LCCD, Decreto-Lei nº 17/2018, de 8 de março)[19], dos contratos de *habitação periódica* (Decreto-Lei nº 275/93, de 5 de agosto)[20] ou dos contratos *automáticos* (arts. 2.º, nº 2, b), 22.º a 24.º da LCCD).[21]

3.3. Requisitos Operacionais

I. "Tertius", no que concerne aos requisitos operacionais, é necessário que o contrato "seja integrado num sistema de venda ou prestação de serviços organizado para o comércio à distância mediante a utilização exclusiva de uma ou mais técnicas de comunicação à distância até à celebração do contrato, incluindo a própria celebração" (art. 3.º, h) da LCCD).

II. Para que exista um contrato à distância, é assim necessário, desde logo, que as partes tenham recorrido à *utilização exclusiva de uma ou mais técnicas de comunicação à distância*, entendendo-se por tal "qualquer meio que, sem a presença física e simultânea do fornecedor de bens ou prestador do serviço e do consumidor, possa ser utilizado tendo em vista a celebração do contrato entre as referidas partes" (art. 3.º, w) da LCCD): estão aqui abrangidas, designadamente, a correspondência postal (v.g., cartas normalizadas, catálogos, brochuras), o telefone fixo ou móvel (v.g., mensagens de texto ou voz), os meios de comunicação audiovisuais (v.g., radio ou televisão), o correio eletrónico, ou a "internet" (v.g., sítios eletrónicos, redes sociais, mercados em linha)[22]. Sublinhe-se que esta exclusividade abrange a negociação e a celebração

17 Ou seja, esta exclusão legal não significa que as relações contratuais sobre tais produtos ou serviços não se encontrem sujeitas as demais regras jusconsumeristas gerais ou setoriais pertinentes: para um exemplo, SCHAFFER, FERNANDA, *Procedimentos Médicos – Realizados à Distância e o Código de Defesa do Consumidor*, Juruá Editora, Curitiba, 2006.

18 Sobre este contrato em especial, vide *infra* 9.

19 Sobre este contrato em especial, vide SANTO, L. ESPÍRITO, *O Contrato de Viagem Organizada*, Almedina, Coimbra, 2016.

20 Sobre este contrato em especial, vide MENDES, I. PEREIRA, *Direito Real de Habitação Periódica*, Almedina, Coimbra, 1993.

21 Sobre a contratação mercantil automática, vide ANTUNES, J. ENGRÁCIA, *Direito dos Contratos Comerciais*, 148 e ss., 7ª reimp., Almedina, Coimbra, 2021; sobre a contratação de consumo automática, ANTUNES, J. ENGRÁCIA, *O Regime Geral da Contratação de Consumo*, 133, in: 2 "Anuário do Nova Consumer Lab – Yearbook of the Nova Consumer Lab" (2020), 123-163.

22 Sublinhe-se que o envio de comunicações não solicitadas através da utilização de técnicas de comunicação à distância depende do consentimento prévio expresso do consumidor (art. 8.º da LCCD),

contratual: tal implica que não serão de qualificar como contratos à distância aqueles que hajam sido negociados no estabelecimento comercial do empresário e posteriormente celebrados através de um meio de comunicação à distância (v.g., um consumidor escolhe o modelo de eletrodoméstico em loja, confirmando a compra posteriormente por telefone) ou que, tendo sido concluídos ou negociados através de um meio de comunicação à distância, sejam celebrados presencialmente no estabelecimento comercial do empresário (v.g., solicitação telefónica de reserva de determinado serviço, tal como uma mesa em restaurante ou uma marcação em cabeleireiro).[23]

III. Para além disso, necessário se torna ainda o contrato se integre *num sistema organizado de vendas ou serviços* especialmente predisposto pelo empresário para o comércio à distância e para a celebração de negócios à distância (v.g., "22en 22entres", televendas, páginas "web", plataformas digitais), não bastando a mera utilização de técnicas de comunicação à distância desinseridas de um tal sistema. Assim, por exemplo, será havida como contrato à distância a encomenda e aquisição de um produto efetuada através de um centro de atendimento telefónico ou um programa de televendas explorado pelo empresário, mas já não aquela que é feita na sequência de mera publicidade televisiva a tal produto ou de um contacto telefónico pontual para o número geral do estabelecimento comercial.[24]

---

mormente para fins de "marketing" direto, designadamente através da utilização de sistemas automatizados de chamada e comunicação que não dependam da intervenção humana (aparelhos de chamada automática), de aparelhos de telecópia ou de correio eletrónico, incluindo SMS (serviços de mensagens curtas), EMS (serviços de mensagens melhoradas), MMS (serviços de mensagem multimédia) e outros tipos de aplicações similares (art. 13.º-A do RGPD).

23 Inversamente, já serão de qualificar como contratos à distância aqueles em que o consumidor, após uma visitar um estabelecimento comercial onde recolheu informações sobre os produtos expostos, negoceia e celebra o respetivo contrato de aquisição através de um "call center" ou uma página "web" do empresário titular do estabelecimento.

24 Sublinhe-se que o requisito legal da exclusividade diz respeito unicamente à técnica de comunicação utilizada na celebração do contrato, e já não ao sistema de contratação do empresário: com efeito, nada impede – e é até frequente – que o empresário disponha simultaneamente de diferentes sistemas de vendas à distância (v.g., centros de relacionamento telefónico, televendas, páginas "web"). Além disso, no caso de utilizações avulsas ou desgarradas de técnicas de comunicação, será ao empresário que em princípio caberá o ónus da prova da inexistência de um sistema organizado de comércio à distância (PINTO, P. MOTA, *Princípios Relativos aos Deveres de Informação no Comércio à Distância*, 185, in: 5 "Estudos de Direito do Consumidor" (2003), 183-206).

4. Modalidades

I. Apesar de o legislador não haver consagrado modalidades legais ou típicas dos contratos à distância (como o fez para os contratos fora do estabelecimento comercial: cf. art. 3.º, i) da LCCD), a "praxis" comercial encarregou-se de desenvolver algumas espécies ou categorias mais frequentes, as quais se distinguem, fundamentalmente, pela particular técnica de comunicação que está na base da respetiva celebração: tais modalidades impróprias são os contratos celebrados por correspondência postal, por telefone, por meios audiovisuais, e por meios eletrónicos.

4.1. Contratos por Correspondência Postal

I. Os contratos por *correspondência postal* são a mais antiga e primogénita modalidade da contratação à distância, que se carateriza pelo recurso a serviços de comunicação que envolvem o envio de documentos e encomendas entre um remetente e um destinatário (serviços postais públicos ou privados, v.g., "CTT", "FedExpress"): tal o caso de cartas normalizadas, formulários, catálogos, brochuras ou outros documentos enviados por correio para o consumidor, que representem propostas contratuais ou convites a contratar por parte do empresário fornecedor dos bens ou prestador dos serviços.

II. Esta modalidade está sujeita ao cumprimento das exigências informativas da LCCD (art. 4.º, e 5.º, nº 1), sendo igualmente relevantes as regras em matéria da publicidade domiciliária (art. 23.º do CPub).[25]

4.2. Contratos por Telefone

I. Os contratos por *telefone* são uma modalidade de contratação à distância tradicional e frequente que se caracteriza pelo recurso a comunicações realizadas entre

25 Particularmente relevante é a tutela dos destinatários através de um sistema de "opt out", sendo por isso absolutamente vedada a publicidade indesejada, seja esta endereçada ou não endereçada, sempre que o destinatário tenha expressamente manifestado o desejo de não receber correspondência publicitária (arts. 3.º e 4.º da Lei nº 6/99, de 27 de janeiro). Sobre o ponto, COELHO, J. GALHARDO, *Publicidade Domiciliária – O Marketing Direto,* Almedina, Coimbra, 1999; PINTO, P. MOTA, *Notas Sobre a Lei nº 6/99, de 27 de janeiro – Publicidade Domiciliária, por Telefone e por Telecópia,* in: 1 "Estudos de Direito do Consumidor" (1999), 117-176.

telefones fixos ou móveis de empresários e consumidores, mormente através de "24en 24entres".

II. Esta modalidade está sujeita a determinadas exigências específicas previstas na LCCD, que impõem ao empresário fornecedor do bem ou prestador do serviço, no início de qualquer contacto telefónico, comunicar explicitamente ao consumidor a respetiva identidade e o objetivo comercial da chamada (art. 5.º, nº 7), além da exigência de forma escrita especial para o contrato (art. 5.º, nº 8). São ainda relevantes as regras relativas aos centros telefónicos de relacionamento ("call centers"): cf. Decreto-Lei nº 134/2009, de 2 de junho)[26], à disponibilização e divulgação de linhas telefónicas de contacto ao consumidor (Decreto-Lei nº 59/2021, de 14 de julho)[27] e à publicidade telefónica (art. 5.º da Lei nº 6/99, de 27 de janeiro).[28]

4.3. Contratos por Meios Audiovisuais

I. Os contratos por *meios audiovisuais* são uma modalidade de contratação à distância bastante divulgada que se carateriza pelo recurso a comunicações comerciais realizadas através "mass media" como a rádio ou a televisão: um exemplo com mais de meio século, que continua a proliferar, são os programas televisivos dedicados à comercialização de bens ou serviços (televendas ou "teleshopping").

II. Esta modalidade está sujeita às exigências específicas previstas na LCCD, designadamente no seu art. 5.º, nº 5, o qual determina que, mesmo nos casos de utilização de um meio de comunicação à distância com espaço ou tempo limitados para

---

26 MELO, MANUEL, *Regime Jurídico dos Centros Telefónicos de Relacionamento ("Call-Centers"),* Dissertação, Lisboa, 2016.

27 Sublinhe-se que, no caso de o empresário utilizar uma linha telefónica para ser contactado em relação ao contrato celebrado, o consumidor, ao contactar aquele, não fica vinculado a pagar mais do que a tarifa de base (art. 21.º da Diretiva 2011/83/UE, de 25 de outubro, art. 4.º, nº 1, q) da LCCD, art. 4.º do Decreto-Lei nº 59/2021, de 14 de julho), isto é, o custo de uma comunicação telefónica que o consumidor espera suportar de acordo com o respetivo tarifário de telecomunicações. Sobre o ponto, vide ROCHA, F. RODRIGUES/ FIDALGO, V. PALMELA/ RODRIGUES, A. BARROSO, *Comunicações Eletrónicas*, 92 e ss., in: Ataíde, R./ Rocha, F./ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. II, 67-139, Almedina, Coimbra, 2023; na jurisprudência europeia, os Acórdãos do TJUE de 2-III-2027 (*Zentrale zur Bekämpfung unlauteren Wettbewerbs Frankfurt am Main c. Comtech GmbH*), in: ECLI:EU:C:2017:154, e de 13-IX-2018 (*Starman AS c. Tarbijakaitseamet*), in: ECLI:EU:C:2018:721.

28 Esta publicidade – realizada mediante sistemas automáticos com mensagens pré-gravadas, incluindo SMS (serviço de mensagens curtas), EMS (serviço de mensagens melhoradas) ou MMS (serviço de mensagens multimédia) – é, em princípio, proibida, dado a lei ter consagrado um sistema de "opt in": a publicidade telefónica com recurso a mensagens pré-gravadas depende sempre da autorização prévia dos destinatários ou da sua não integração nas listas para efeitos de comunicações não solicitadas.

divulgar a informação, o empresário fornecedor do bem ou prestador do serviço está obrigado a dispensar ao consumidor através desse meio um conjunto mínimo de informações pré-contratuais (art. 4.º, nº 1, a), d), e), g), h), i), m) e r) da LCCD)[29]. Igualmente relevantes são ainda as disposições em matéria da publicidade televisiva, prevista na Lei da Televisão ou LTV (Lei nº 27/2007, de 20 de julho), "maxime", identificação, separação, inserção e interatividade da publicidade televisiva (arts. 40.º-A, 40.º-C e 40.º-D) e televenda (art. 40.º-B, todos da LTV).

4.4. Contratos Eletrónicos

I. Os contratos por *meios eletrónicos* – a mais recente mas também, crescentemente, uma das mais relevantes modalidades da contratação à distância graças à proliferação do comércio eletrónico ("e-commerce") – são contratos que se caraterizam pelo facto de as declarações de vontade dos contraentes serem produzidas e transmitidas por via telemática mediante o recurso a equipamentos de processamento e transmissão eletrónica de dados (computadores, "tablets", "smarthphones"), designadamente através de correio eletrónico ("e-mail"), páginas ou sítios "web" ("internet"), redes sociais ou outros análogos. Dado que estes contratos constituem, em si mesmos, um tipo autónomo de contrato de consumo – os *contratos eletrónicos com consumidores* ou B2C –, deixaremos o seu estudo para essa oportunidade.[30]

II. O *regime legal* dos contratos à distância encontra-se previsto nos arts. 4.º e segs. da LCCD: tais regras dizem respeito a todas as fases da vida contratual, incluindo a *negociação*, a *formação*, a *execução* e a *extinção* de tais contratos. A elas dedicaremos agora uma atenção autónoma.

---

29 Entre estes elementos informativos mínimos inclui-se o direito de desistência do consumidor, com exceção do modelo de formulário de retratação previsto no anexo I, parte B da LCCD (art. 5.º, nº 5, "in fine"). A este respeito, veja-se o Acórdão do TJUE de 23-I-2019 (*Walbusch Walter Busch c. Zentrale zur Bekämpfung unlauteren Wettbewerbs)*, onde se determina que "se o contrato for celebrado através de uma técnica de comunicação à distância que impõe limitações de espaço ou de tempo para divulgar a informação e sempre que exista o direito de retratação, o profissional tem o dever de fornecer ao consumidor, na tecnologia em questão e antes da celebração do contrato, a informação sobre as condições, o prazo e o procedimento de exercício desse direito. Em tal caso, este profissional deve fornecer ao consumidor o modelo de formulário de retratação previsto no anexo I, parte B, da referida diretiva, por outra fonte, em linguagem clara e compreensível" (in: ECLI:EU:C:2019:47 [§ 47]).

30 ANTUNES, J. ENGRÁCIA, *Os Contratos Eletrónicos B2C,* em curso de publicação. Dada esta natureza bifronte, os contratos eletrónicos encontram-se assim sujeitos simultaneamente, em princípio, às regras gerais em sede da contratação à distância (LCCD) e às suas regras próprias em sede de contratação eletrónica (mormente, a LCE).

5. Negociação

I. Relativamente à fase da negociação dos contratos à distância, avultam indubitavelmente os *deveres pré-contratuais de informação* do empresário perante o consumidor. Tais informações podem ser divididas em informações gerais (art. 4.º da LCCD) e informações adicionais (arts. 4.º A e 4.º-B da LCCD).

5.1. Deveres Gerais de Informação

I. O art. 4.º da LCCD contém um extenso elenco de *informações gerais* que devem ser prestadas pelo empresário antes da celebração de um contrato à distância.

II. Tais informações incluem, designadamente (i) a sua identidade, endereço e contactos[31], (ii) a identidade e endereço dos terceiros que atuem em seu nome e por sua conta[32], (iii) as caraterísticas essenciais do bem ou do serviço[33], (iv) o preço total do bem ou do serviço[34], (v), o preço personalizado[35] (vi) o modo de cálculo do preço[36],

31 Tenha-se presente que os empresários em geral se encontram sujeitos a um mero dever de *divulgação* de linhas telefónicas dedicadas nas relações com os consumidores, apenas estando sujeitos a um dever de *disponibilização* efetiva no âmbito dos contratos de prestação de serviços essenciais (arts. 3.º e 5.º da Lei nº 59/2021, de 14 de julho). Num sentido semelhante, o Acórdão do TJUE de 10-VII-2019 veio considerar que o profissional deve informar o consumidor dos seus contactos telefónico e eletrónico (cf. art. 4.º, nº 1, a) da LCCD), não sendo, todavia, obrigado a ativar uma nova linha telefónica, de "fax", ou endereço eletrónico para permitir aos consumidores contactar com ele (in: ECLI: EU:C:2019:576).

32 Sobre a identificação dos terceiros intermediários, vide os Acórdãos do TJUE de 9-XI-2016 (*Sabrina Wathelet c. Garage Bietheres & Fils SPRL*), in: ECLI:EU:C:2016:840, e de 4-II-2022 *(«Tiketa» UAB c. M. Š.*), in: ECLI:EU:C:2022:112: nos termos deste último acórdão, os deveres de informação pré-contratual são também extensíveis e aplicáveis aos intermediários de plataformas digitais que atuam em nome do empresário/profissional [§§ 24 e ss.].

33 Sempre que os bens ou serviços incluírem outros bens ou serviços acessórios, de aquisição facultativa, o consumidor deverá ser também informado dessas opções adicionais: por exemplo, aplicações informáticas que incluam compras integradas ("in-app") (v.g., videojogos com níveis suplementares) ou assinaturas de serviços que incluam conteúdos opcionais (v.g., serviço audiovisual com visualização de canais ou conteúdos "premium"). Cf. também art. 9.º-A da LDC.

34 Incluindo taxas, impostos e outros encargos, v.g., IVA, direito aduaneiros, etc. No caso de contratos de duração indeterminada ou que incluam uma assinatura de periodicidade, o preço total indicado deverá incluir os custos totais, por período de faturação e, tratando-se de contratos com uma tarifa fixa, deverá incluir todos os custos periódicos: assim, por exemplo, num serviço de televisão ou "internet", o consumidor deve ser previamente informado da taxa mensal, bimensal, trimestral ou outra que vai pagar independentemente da utilização.

35 Sobre os preços personalizados com base em decisões automatizadas no âmbito dos contratos de consumo em linha, vide COSTA, I. SILVA, A *Proteção da Pessoa na Era dos Big Data: A Opacidade do Algoritmo e as Decisões Automatizadas*, 56 e ss., in: 24 "Revista Electrónica de Direito" (2021), 33-82; OLIVEIRA, M. PERESTRELO, *Definição de Perfis e Decisões Individuais Automatizadas no Regulamento Geral sobre a Proteção de Dados*, in: Cordeiro, A./ Oliveira, A./ Duarte, D. (coord.), "Fintech – Novos Estudos sobre Tecnologia Financeira", 61-88, Almedina, Coimbra, 2019.

(vii) as modalidades de pagamento, entrega ou execução, bem como a data-limite de entrega do bem ou serviço[37], (viii) a existência de um direito de livre resolução do contrato, seu modo de exercício, termos e efeitos[38], (ix) o custo de utilização da técnica de comunicação à distância[39], (x) a duração do contrato ou as condições da sua denúncia[40], (xi) a existência de prazo da garantia de conformidade dos bens[41], (xii) a assistência e serviços pós-venda, bem com as garantias comerciais[42], (xiii) as funcionalidades, compatibilidade e interoperabilidade dos bens com elementos digitais, conteúdos e serviços digitais[43], (xiv) a existência de códigos de conduta relevantes[44], (xv) a existência de depósitos ou outras garantias financeiras[45] e (xvi) a possibilidade de acesso a um mecanismo extrajudicial de reclamação a que o empresário esteja vinculado.[46]

---

36 Incluindo quaisquer encargos suplementares de transporte, de entrega e postais, e quaisquer outros custos, quando a natureza do bem ou serviço não permita o cálculo em momento anterior à celebração do contrato.

37 Sobre os prazos de entrega dos bens e serviços (art. 19.º da LCCD), vide *infra* 7 (III).

38 Tenha-se presente que estes deveres informativos sobre o direito de livre resolução podem ser cumpridos mediante a entrega do modelo legal constante da Parte A do Anexo ao Decreto-Lei 24/2014 (art. 4.º, nº 2 da LCCD). Sobre o direito de livre resolução (arts. 10.º a 17.º da LCCD), vide *infra* 8.

39 Nos casos em que tal custo seja calculado numa base diferente da tarifa base: por exemplo, no caso de contratos celebrados através de contacto telefónico, um número de telefone com serviço de tarifa majorada (STM).

40 Nos casos de contratos de duração indeterminada ou de renovação automática, o consumidor deve ser informado dos requisitos da denúncia contratual (v.g., termos e prazos de exercício, encargos aplicáveis) e, no caso de contratos sujeitos a períodos contratuais mínimos, os encargos com a cessação antecipada (v.g., para os serviços de comunicações eletrónicas, vide arts. 122.º, nº 1, b), 128.º, nº 12, e 136.º, nº 4 da LComunE).

41 Sobre a garantia legal de conformidade contratual na atual LVBC, vide ANTUNES, J. ENGRÁCIA, *A Compra e Venda de Consumo*, em curso de publicação; FALCÃO, DAVID, *Análise à Nova Lei das Garantias: DL 84/2021, de 18 de Outubro*, 521 e ss., in: 81 "Revista da Ordem dos Advogados" (2021), 493-541; LEITÃO, L. MENEZES, *Desconformidade e Meios de Tutela do Adquirente na Venda de Bens de Consumo*, 173 e ss., in: Ataíde, R./ Rocha, F./ Fidalgo, V. (cor.), "Estudos de Direito do Consumo", vol. II, 161-185, Almedina, Coimbra, 2023.

42 Sobre as garantias comerciais, vide ANTUNES, J. ENGRÁCIA, *A Compra e Venda de Consumo*, em curso de publicação. Sobre a existência e extensão dos deveres de informação dos empresários vendedores relativamente às garantias comerciais de terceiros (produtores ou fabricantes), vide o Acórdão do TJUE de 5-V-2022 *(Absoluts-bikes GmbH & Co. KG c. The-trading-company GmbH)*, in: ECLI*:* EU:C:2022:353.

43 Sobre tais conceitos, vide os arts. 2.º, j), 6.º, a), 28.º, a) e 29.º, b) da LVBC (ANTUNES, J. Engrácia, *A Compra e Venda de Consumo*, em curso de publicação).

44 Sobre os códigos de conduta como fonte de Direito do Consumo, vide ANTUNES, J. ENGRÁCIA, *Direito do Consumo*, 20 e s., Almedina, Coimbra, 2019. Sobre a sua vinculatividade jurídica, vide o Acórdão do TJUE de 19-IX-2018 (*Bankia SA c. Juan Carlos Marí e Outros*), in: ECLI: EU:C:2018:73.

45 Especialmente frequente nos contratos de locação, tal como o aluguer automóvel.

46 Sobre tais mecanismos de resolução extrajudicial de conflitos, vide ANTUNES, J. ENGRÁCIA, *Os Conflitos de Consumo*, em curso de publicação; CARVALHO, J. MORAIS/ PINTO-FERREIRA, J. PEDRO/ CARVALHO, J. CAMPOS, *Manual de Resolução Alternativa de Litígios de Consumo*, Almedina, Coimbra, 2017.

5.2. Deveres Especiais nos Mercados em Linha

I. Paralelamente, existe ainda um conjunto de *informações e diligências adicionais* no caso particular dos contratos celebrados em mercados em linha (arts. 4.º-A e 4.º-B da LCCD).

II. É sabido que, com o advento do comércio eletrónico, uma parte sempre crescente dos contratos de consumo são negócios formados, celebrados e até cumpridos através de *plataformas digitais* ("digital platforms"), que estão na origem de mercados eletrónicos ("emarket places") ou em linha ("online markets"). Tais plataformas são muito diversas, podendo a sua titularidade e exploração ser detida pelas próprias empresas fornecedoras dos bens ou prestadoras dos serviços, funcionando com um canal de contratação "on line" daqueles bens e serviços alternativo à tradicional contratação "off line" (plataformas próprias ou internas) ou ser detida por terceiras empresas especializadas cuja função é criar um autónomo "mercado em linha", ou seja, providenciar um espaço digital de encontro entre a oferta e a procura, desenvolvendo assim uma atividade de intermediação entre as empresas fornecedoras de bens e serviços, por um lado, e os respetivos consumidores e clientes, por outro (plataformas externas ou de intermediação).[47]

III. Ciente do relevo crescente destas plataformas e mercados, o legislador veio determinar que o prestador de mercado em linha (art. 3.º, t da LCCD) deve facultar ao consumidor informações (i) sobre os principais parâmetros que determinam a classificação das propostas apresentadas ao consumidor em resultado da pesquisa; (ii) de que as propostas apresentadas se referem exclusivamente às do prestador do mercado em linha; (iii) de que a comparação de propostas se baseia em diferentes circunstâncias, não apresentando essa comparação como um desconto; (iv) sobre a identificação e o estatuto da outra parte contratante; (v) sobre a atribuição e partilha de responsabilidades contratuais entre o empresário parte no contrato e o prestador do mercado em linha; e

47 Sobre as plataformas eletrónicas, vide GUIMARÃES, M. RAQUEL, *As Plataformas "Colaborativas" enquanto Prestadoras de Serviços da Sociedade de Informação*, 474 e ss., in: Carvalho, M./ Sousa, A. (coord.), "Economia Colaborativa", 468-498, UMinho Editora, Braga, 2023.

(vi) sobre as percentagens de redução e o preço mais baixo anteriormente praticado, no caso de vendas com redução de preço.[48]

IV. Particular destaque merece aqui a *identificação da parte contratante* – que obriga o prestador em linha a informar o consumidor sobre se o terceiro que oferece os bens, serviços ou conteúdos digitais é ou não um profissional, com base nas declarações prestadas por aquele ao prestador do mercado em linha e, em caso negativo, a informação de que os direitos do consumidor não se aplicam ao contrato celebrado (art. 4.º, nº 1, d) e e) da LCCD) – e ainda a *atribuição de responsabilidades contratuais* – que obriga aquele prestador em linha a informar o consumidor sobre o modo como as obrigações contratuais são partilhadas entre o terceiro que oferece os bens, serviços ou conteúdos digitais e o prestador do mercado em linha, sem prejuízo da responsabilidade do prestador do mercado em linha ou do terceiro profissional em relação ao contrato resultante de outras disposições das leis europeias ou nacionais (art. 4.º, f) da LCCD).[49]

V. Por último, advirta-se que o prestador do mercado em linha que disponibilize o acesso a *avaliações efetuadas por consumidores* está ainda obrigado a adotar um conjunto de medidas de diligência adequadas, designadamente a assegurar a verificação de existência prévia de transação comercial efetuada por aquele consumidor, sempre que a avaliação esteja anunciada como tendo por base a aquisição prévia do produto ou serviço oferecido; identificar, de forma clara e inequívoca, as avaliações feitas em troca de algum benefício, quando disso tenha ou deva ter conhecimento; garantir que as avaliações são publicadas sem demora e que o seu autor pode, a qualquer momento, editar o seu conteúdo; e garantir que todas as avaliações, positivas ou negativas,

48 Sobre o ponto, vide SIMÃO, J. CARITA/ SOARES, S. ASSUNÇÃO, *Práticas Comerciais Desleais em Geral e em Linha: A Diretiva (EU) 2019/2161, do Parlamento Europeu e do Conselho, de 7 de novembro, a sua Transposição Parcial para o Decreto-Lei nº 109-G/2021, de 10 de dezembro, e o Reforço da Proteção dos Direitos dos Consumidores*, 671 e ss., in: Ataíde, R./ Rocha, F/ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. I, 649-681, Almedina, Coimbra, 2023.

49 Sobre o ponto, em especial a responsabilidade solidária do prestador do mercado em linha (arts. 44.º a 46.º da LVBC), vide ANTUNES, J. ENGRÁCIA, *A Compra e Venda de Consumo,* em curso de publicação. Relevantes são também as exigências de transparência relativa aos *sistemas de classificação* dos produtos e serviços oferecidos pelos empresários, mormente em função do tratamento automatizado e algorítmico dos resultados das pesquisas realizadas pelos consumidores (arts. 4.º-A, nº 1 da LCCD). Sobre a figura congénere dos sistemas de recomendação das plataformas eletrónicas, também sujeitos a requisitos de transparência no âmbito do Regulamento dos Serviços Digitais (art. 25.º do Regulamento UE/2022/2065, de 19 de outubro), vide ANTUNES, J. ENGRÁCIA, *Os Contratos Eletrónicos B2C*, em curso de publicação.

permanecem disponíveis por idêntico período, não inferior a seis meses (art. 4.º-B, nº 1 da LCCD).[50]

5.3. Regime

I. O regime deste extenso elenco de deveres informativos prévios à celebração de um contrato à distância abrange uma diversidade de aspetos – de que aqui se dá sucintamente nota.

II. As informações pré-contratuais possuem uma natureza jurídica *imperativa e vinculativa* para as partes contratantes: com efeito, tais informações são parte integrante do contrato e não podem ser alteradas salvo acordo contrário das partes anterior à celebração do contrato (art. 4.º, nº 4 da LCCD)[51]. A delimitação do *perímetro* das informações pré-contratuais relevantes deverá ser feita perante cada contrato em concreto: com efeito, as informações constantes do elenco legal dos arts. 4.º e 4.º-A da LCCD foram concebidas para os contratos à distância em geral e abstrato, tendo diversas delas uma aplicação eventual ou condicionada nos casos concretos ("se aplicável") (v.g., alíneas g), h), i), l) e z) do art. 4.º, nº 1, alínea c) do art. 4.º-A). A declaração do empresário contendo tais informações pré-contratuais consubstanciará, em princípio, um mero *convite a contratar*, e não uma proposta contratual: com efeito, o cumprimento desses deveres legais informativos assegura a proteção do consumidor almejada pela lei, não devendo coartar a autonomia privada do empresário.[52]

III. As informações pré-contratuais devem ser prestadas *"em tempo útil e de forma clara e compreensível"* (art. 4.º, nº 1 da LCCD) – isto é, deverão ser prestadas pelo empresário em momento anterior à celebração do contrato e apresentadas de modo a que um consumidor médio as pudesse apreender diretamente e sem dificuldade, sem

---

50 Além disso, o prestador do mercado em linha deve disponibilizar as avaliações aos consumidores preferencialmente por ordem cronológica, indicando o critério utilizado (art. 4.º-B, nº 3 da LCCD) e deve disponibilizar mecanismos de reporte de avaliações falsas ou abusivas, permitindo ao fornecedor de bens ou prestador de serviços responder às avaliações apresentadas (art. 4.º-B, nº 3 da LCCD).

51 Tal regime já não se aplica às alterações dos termos do contrato posteriores à respetiva celebração, para quais poderão ser relevantes as disposições da LCCG.

52 Assim também, BARATA, C. LACERDA, *Contratos Celebrados Fora do Estabelecimento Comercial*, 81, in: V "Estudos de Direito do Instituto do Consumo" (2017), 41-127; CHEN, CHEN, *Contratos à Distância em Geral,* 786, in: Ataíde, R./ Rocha, F./ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. I, 777-801, Lisboa, 2023. Em sentido contrário, CARVALHO, J. MORAIS, *Manual de Direito do Consumo*, 317 e ss., 8ª edição, Almedina, Coimbra, 2022.

prejuízo das eventuais especificidades decorrentes do público-alvo ou das técnicas de comunicação utilizadas (art. 5.º, nº 1 da LCCD)[53] – e o *ónus da prova* do cumprimento desses deveres informativos recai sobre o empresário (art. 4.º, nº 8 da LCCD) – a qual resultará, via da regra, da confirmação do contrato à distância fornecida em suporte duradouro (art. 6.º, nº 1 da LCCD).

IV. Finalmente, o *incumprimento* destes deveres pré-contratuais de informação pode ser fonte de um conjunto de consequências para o empresário: entre elas, incluem-se a responsabilidade pré-contratual (art. 227.º, nº 1 do CCivil), a responsabilidade pelos danos causados ao consumidor (art. 8.º, nº 5 da LDC), a isenção do pagamento de custos ou encargos por parte do consumidor (arts. 4.º, nº 5 e 13.º, nº 2, a) da LCCD), a extensão do prazo para o exercício do direito de resolução (art. 10.º, nº 2 da LCCD), e a responsabilidade contraordenacional (art. 31.º, nº 4 da LCCD).

5.4. Outros

I. A terminar, deve ainda ser referido que os deveres informativos pré-contratuais previstos da LCCD não prejudicam a aplicação simultânea das disposições em matéria de informação pré-contratual do consumidor previstas *noutras leis de consumo* ou aplicáveis a determinados contratos especiais de consumo.

II. Pense-se assim, por exemplo, no dever de informação geral aos consumidores (art. 8.º da LDC), nos deveres informativos nos contratos de adesão (arts. 5.º e 6.º da LCCG)[54], nos deveres informativos prévios à celebração de contratos relativos aos serviços de comunicações eletrónicas (art. 120.º da LComunE), nos deveres de informação mínima nos contratos eletrónicos (art. 28.º, nº 1 da LCD)[55], já sem falar nos

---

53 Especialmente relevante é que não basta fornecer as informações pré-contratuais como simples parte das condições contratuais gerais que o consumidor venha a aceitar (Acórdão do TJUE de 24-II-2022 *(«Tiketa» UAB c. M. Š.*), in: ECLI:EU:C:2022:112). Sobre tais questões, vide desenvolvimentos em CARVALHO, J. MORAIS, *Prestação de Informações nos Contratos Celebrados à Distância*, in: AA.VV., "Direito Privado e Direito Comunitário", 13-144, Âncora Editora, Lisboa, 2009; PINTO, P. MOTA, *Princípios Relativos aos Deveres de Informação no Comércio à Distância*, in: 5 "Estudos de Direito do Consumidor" (2003), 183-206; REBELO, F. NEVES, *O Direito à Informação do Consumidor nos Contratos à Distância*, in: "Liber Amicorum Mário Frota*"*, 103-153, Almedina, Coimbra, 2012.

54 ANTUNES, J. ENGRÁCIA, *Os Contratos Comerciais de Adesão*, em curso de publicação; NUNES, P. CAETANO, *Comunicação de Cláusulas Contratuais Gerais*, in: "Estudos em Homenagem ao Prof. Doutor C. Ferreira de Almeida", vol. II, 507-534, Almedina, Coimbra, 2011.

55 Cf. ANTUNES, J. ENGRÁCIA, *Os Contratos Eletrónicos B2C*, em curso de publicação; BARROS, J. LEITE, *Os Contratos de Consumo Celebrados pela Internet*, 798 e ss., in: 3 "Revista Jurídica Luso-

próprios deveres de informação pré-contratuais decorrentes das normas civis gerais (v.g., em sede da culpa "in contrahendo": cf. art. 227.º, nº 1 do CCivil). Particular destaque merece o conjunto de elementos de "informação substancial" de que o consumidor necessita para tomar uma decisão negocial esclarecida, previstos nos arts. 9.º, nº 1, a) e 10.º da LPCD.[56]

6. Formação

6.1. Princípio Geral

I. A formação dos contratos à distância está dominada pelo *princípio geral da liberdade de forma* (art. 219.º do CCivil), já que, com exceção dos celebrados por telefone (cf. art. 5.º, nº 8 da LCCD), a celebração destes contratos não se encontra sujeita a forma especial imposta por lei. Em contrapartida, já se encontra subordinada às *regras específicas* relativas ao particular meio de comunicação à distância utilizado na sua celebração (designadamente, LI, LR, LTV, CPub, etc.).[57]

6.2. Regras Especiais

I. Assim, no que diz respeito a contratos celebrados através de *correspondência postal*, o conteúdo contratual mínimo deve integrar, além dos elementos gerais do art. 4.º, nº 1, os elementos adicionais previstos no art. 21.º da LCCD, sendo ainda de ter presentes as normas do art. 23.º do CPub e da Lei nº 6/99, de 27 de janeiro.

II. No que respeita a contratos celebrados através de *telefone*, a lei exigiu a assinatura da proposta contratual do empresário ou o consentimento escrito do consumidor (exceto nos casos em que o primeiro contato telefónico seja efetuado pelo

---

Brasileira" (2017), 781-843; OLIVEIRA, E. DIAS, *A Protecção dos Consumidores nos Contratos Celebrados Através da Internet*, 65 e ss., Almedina, Coimbra, 2002.

56 ANTUNES, J. ENGRÁCIA, *As Práticas Comerciais Desleais*, em curso de publicação. Dado que o elenco dos deveres informativos pré-contratuais previsto no art. 4.º da LCCD é mais amplo e pormenorizado do que o elenco do art. 10.º da LPCD, o empresário que cumpra o primeiro estará também a cumprir o último, o que não prejudica, todavia, que ainda assim possa incorrer em situações de omissão enganosa decorrentes de outros requisitos de transparência previstos neste último diploma.

57 Cf. Lei nº 2/99, de 13 de janeiro (Lei da Imprensa ou LI), Lei nº 54/2010, de 24 de dezembro (Lei da Rádio ou LR), e Lei nº 27/2007, de 20 de julho (Lei da Televisão ao LTV).

próprio consumidor: cf. art. 5.º, nº 8 da LCCD)[58], sendo ainda de ter presente outras regras especiais porventura aplicáveis (v.g., Decreto-Lei nº 134/2009, de 2 de junho, relativo aos centros telefónicos de relacionamento).

III. Finalmente, no que respeita a contratos celebrados por *rádio ou televisão*, a celebração do contrato deve ser precedida da prestação de um conteúdo mínimo de informação (art. 5.º, nºs 5 e 6 da LCCD), além da observância das regras especiais previstas no CPub (art. 8.º), na LTV (arts. 40.º e segs.) e na LR (art. 40.º).

7. Cumprimento

I. No âmbito do cumprimento dos contratos à distância, avultam duas obrigações do empresário: a obrigação de confirmação do conteúdo do contrato (art. 6.º, nº 1 da LCCD) e a obrigação de execução do contrato (art. 19.º da LCCD).

7.1. Confirmação do Conteúdo Contratual

I. A *obrigação de confirmação do conteúdo do contrato* encontra-se prevista no art. 6.º da LCCD: nos termos do nº 1 deste preceito, "o fornecedor de bens ou prestador de serviços deve confirmar a celebração do contrato à distância, em suporte duradouro, no prazo de cinco dias contados dessa celebração e, o mais tardar, no momento da entrega do bem ou antes do início da prestação do serviço".

II. Encontramo-nos assim diante de uma *obrigação acessória* do empresário, relativa ao conteúdo do contrato e não à sua conclusão: a finalidade deste dever é reforçar a segurança e a proteção jurídicas do consumidor, assegurando a este, já depois da celebração do contrato, o conhecimento cabal das principais condições do contrato por forma a facilitar o exercício informado e tempestivo da sua prerrogativa legal de manutenção ou desistência do contrato (art. 10.º da LCCD) e a facultar-lhe de um meio de prova do conteúdo do contrato em caso de litígio de consumo (arts. 342.º e segs. do CCivil, 5.º do CPC).

---

58 Regra semelhante encontrava-se prevista a respeito da celebração dos contratos de serviços de comunicações eletrónicas (art. 48.º, nº 3 da anterior LComunE). Cf. ROCHA, F. RODRIGUES/ FIDALGO, V. PALMELA/ RODRIGUES, A. BARROSO, *Comunicações Eletrónicas,* 84, in: Ataíde, R./ Rocha, F./ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. II, 67-139, Almedina, Coimbra, 2023.

III. Esta obrigação realiza-se através da entrega ao consumidor do conjunto das informações pré-contratuais obrigatórias (art. 6.º, nº 2 da LCCD); deve ser efetuada em suporte duradouro (v.g., papel, chave USB, CD-ROM, DVD: cf. art. 3.º, v) da LCCD)[59], salvo se o profissional já tiver prestado essa informação antes da celebração do contrato em suporte idêntico (v.g., um catálogo de vendas por correspondência, uma mensagem SMS, um e-mail": cf. art. 6.º, nº 2, "in fine", da LCCD); e deve ser realizada no prazo de cinco dias contados dessa celebração ou, no máximo, no momento da entrega do bem ou antes do início da prestação do serviço (art. 6.º, nº 1 da LCCD). O incumprimento desta obrigação constitui uma contraordenação económica grave, nos termos do art. 31.º, nº 2 da LCCD.

7.2. Execução do Contrato

I. A *obrigação de execução do contrato* encontra-se prevista no art. 19.º da LCCD: nos termos do nº 1 deste preceito, "salvo acordo em contrário entre as partes, o fornecedor de bens ou prestador de serviços deve dar cumprimento à encomenda no prazo máximo de 30 dias, a contar do dia seguinte à celebração do contrato".

II. Trata-se da *obrigação principal* do empresário fornecedor ou prestador, cujo incumprimento sujeita este a reembolsar o consumidor dos montantes pagos ou mesmo a devolver o preço em dobro (nºs 2 e 3), sem prejuízo da possibilidade de prestar bem ou serviço de qualidade e preço equivalentes se tal houver sido convencionado e o consumidor nisso tenha consentido expressamente (nº 4) e, em tal caso, sem prejuízo do

59 Por *suporte duradouro* entende-se qualquer instrumento que permita ao consumidor armazenar informações que lhe sejam pessoalmente dirigidas, de modo a que, no futuro, possa ter acesso fácil às mesmas durante um período de tempo adequado aos fins a que as informações se destinam e que permita a respetiva reprodução: estão aqui abrangidos, para além do papel, as chaves "Universal Serial Bus" (USB), vulgo "pen", os "Compact Disc Read-Only Memory" (CD-ROM), os "Digital Versatile Disc" (DVD), os cartões de memória, os discos rígidos do computador, os extratos impressos em terminais automáticos, e as mensagens em caixas de correio eletrónicas integradas em sítios da "internet" que permaneçam invioláveis e acessíveis ao consumidor. Sobre a noção de suporte duradouro, vide, na doutrina, DEMOULIN, MARIE, *La Notion de «Support Durable» dans les Contrats à Distance*, in: 4 "Revue Européenne de Droit de la Consommation" (2000), 361-377; na jurisprudência, os Acórdãos do TJUE de 5-VI-2012 (*Content Services Ltd c. Bundesarbeitskammer*) – segundo o qual as hiperligações no sítio "internet" da empresa fornecedora nos contratos à distância não podem ser consideradas como suporte duradouro para estes efeitos (in: ECLI:EU:C:2012:419 [§ 51]) – e de 25-I-2017 (*BAWAG PSK Bank AG c. Verein für Konsumenteninformation*) – segundo o qual poderão ser qualificados como suporte duradouro os sítios "internet" que permitem ao consumidor armazenar as informações que lhe são pessoalmente dirigidas, desde que esteja garantida a sua permanente acessibilidade e inalterabilidade durante um período adequado de tempo e seja acompanhada de um comportamento ativo do prestador relativamente à sua existência (ECLI:EU:C:2017:38 [§§ 43 e ss.].

direito de desistência do consumidor, correndo as despesas de devolução a cargo do empresário (nº 5).

7.3. Transferência da Propriedade e do Risco

I. Aspeto relevante neste contexto é ainda a *transferência da propriedade e do risco*. Tratando-se de uma compra e venda, o consumidor torna-se proprietário do bem com a respetiva celebração (art. 408.º do CCivil) e pode fruir plenamente do mesmo (art. 1305.º do CCivil), inclusivamente durante o decurso do prazo de desistência, sem prejuízo dos ónus a que se encontra então sujeito nos termos do art. 14.º da LCCD (utilização normal, sob pena de responsabilidade pela respetiva depreciação).

II. Do mesmo modo, o risco da perda ou deterioração dos bens passa a correr por conta do consumidor a partir do momento em que estes lhe tenham sido entregues pelo empresário (art. 796.º do CCivil), "rectius", do momento da entrada do consumidor na posse física dos bens (a determinar nos termos do art. 13.º, nº 1, b) da LCCD), independentemente de estes terem ou não sido inspecionados pelo consumidor para detetar eventuais defeitos ou avarias (sem prejuízo da obrigação geral de conformidade e das regras de distribuição do ónus da prova, previstas na LVBC).[60]

7.4. Outros Aspetos

I. Finalmente, embora num plano delitual, merece ser sublinhado que as vicissitudes do cumprimento das obrigações do empresário se encontram sujeitas a um regime de *fiscalização, sancionamento e responsabilidade contraordenacional* previsto nos arts. 30.º a 32.º da LCCD. Além disso, nos termos do art. 21.º do Regulamento UE/2017/2394, de 12 de dezembro, as autoridades nacionais responsáveis pela legislação de proteção dos consumidores que participem numa ação coordenada no caso

60 Sobre a garantia legal de conformidade com o contrato na LVBC de 2021, vide, entre outros, ANTUNES, J. ENGRÁCIA, *A Compra e Venda de Consumo*, em curso de publicação; CARVALHO, J. MORAIS, *Compra e Venda e Fornecimento de Conteúdos e Serviços Digitais – Anotação ao Decreto-Lei nº 84/2021, de 18 de Outubro*, Almedina, Coimbra, 2022; LEITÃO, L. MENEZES, *Desconformidade e Meios de Tutela do Adquirente na Venda de Bens de Consumo,* in: Ataíde, R./ Rocha, F./ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. II, 161-185, Almedina, Coimbra, 2023.

de infrações transfronteiriças "generalizadas" devem tomar medidas para as fazer cessar ou proibir.[61]

8. Extinção

8.1. O Direito de Desistência

I. Os contratos à distância encontram-se sujeitos, em princípio, às causas gerais da cessação e extinção dos contratos (v.g., caducidade, revogação, denúncia): tal como sucede com os demais contratos de consumo, todavia, a "joia da coroa" ou traço identitário do seu processo extintivo reside no *direito de desistência do consumidor*.[62]

II. O regime deste direito fundamental – que o legislador designou aqui de "direito de livre resolução" – é vasto e minucioso, encontrando-se contido nos arts. 10.º a 17.º da LCCD. Entre os aspetos mais relevantes, que aqui serão referidos sucintamente, destacam-se o *prazo*, as *modalidades*, a *natureza*, os *efeitos* e as *exceções* ao exercício deste direito.

8.2. Prazo

I. O consumidor tem o direito de resolver ou desistir do contrato à distância no *prazo de 14 dias* (art. 10.º, nº 1 da LCCD)[63]. Trata-se de conceder ao consumidor risco um período de reflexão ("colling-off period", "delais de refléxion") destinado a protegê-lo contra os riscos tipicamente associados à contratação à distância, designadamente o frequente desconhecimento da identidade e localização exatos da sua contraparte

61 O art. 24.º da Diretiva 2011/83/CE, de 25 de outubro (aditado pela Diretiva UE/2019/2161, de 27 de novembro) veio mesmo exigir que, para este tipo particular de infrações, os Estados-membros contemplem a possibilidade de aplicar coimas por meio de procedimentos administrativos ou de intentar uma ação judicial para aplicação de coimas, ou ambas, sendo o montante máximo dessas coimas de, pelo menos, 4% do volume de negócios anual do empresário ou, não existindo informação disponível sobre este, de pelo menos 2 milhões de euros.

62 Sobre o direito de desistência, enquanto traço distintivo da contratação de consumo, vide ANTUNES, J. ENGRÁCIA, *Direito do Consumo*, 147 e ss., Almedina, Coimbra, 2019; ANTUNES, J. ENGRÁCIA, *O Regime Geral da Contratação de Consumo,* 157 e ss., in: 2 "Anuário do Nova Consumer Lab – Yearbook of the Nova Consumer Lab" (2020), 123-163.

63 Trata-se de um prazo legal mínimo, podendo as partes fixar convencionalmente um prazo mais amplo (art. 10.º, nº 5 da LCCD).

contratual e a ausência de contato direto ou exame físico dos produtos adquiridos antes de os encomendar e pagar.

II. Sendo aqui aplicáveis as regras gerais de contagem dos prazos previstas no Código Civil (arts. 279.º e 296.º), a LCCD previu diferentes datas de início dessa contagem consoante se trate de contratos relativos à compra e venda de bens (em que releva, em princípio, a data da entrega ou da posse física dos bens) ou contratos de serviços ou relativos ao fornecimento de água, gás ou eletricidade (em que releva a data da celebração contratual)[64]. Sublinhe-se que este prazo poderá ser alargado em 12 meses caso o empresário fornecedor de bens ou prestador de serviços não tenha informado o consumidor, antes da celebração do contrato, da existência, prazo e modo de exercício do direito de desistência, juntamente com a entrega do formulário respetivo (art. 10.º, nº 2 da LCCD), o qual será interrompido se e quando o empresário cumprir tais obrigações de informação e entrega, começando então a correr novo prazo de 14 ou 30 dias (art. 10.º, nº 3 da LCCD).

8.3. Modalidades

I. O direito de desistência contratual pode ser exercido pelo consumidor através de três modalidades alternativas: o envio de qualquer *declaração inequívoca* de desistência por meio da qual este comunique ao empresário a decisão de cessar o contrato, v.g., carta, contacto telefónico, correio eletrónico, ou devolução do bem com manifestação de vontade de retratação (art. 11.º, nºs 1 e 2 da LCCD); o envio ao empresário do *modelo de "Livre Resolução"* devidamente preenchido (art. 11.º, nº 1 e parte B do anexo da LCCD); ou ainda o envio de *declaração eletrónica de resolução no sítio "web"* do empresário, que está obrigado a acusar a sua receção no prazo de 24 horas em suporte duradouro (art. 11.º, nº 4 da LCCD).

II. O ónus da prova do exercício do direito de desistência compete ao consumidor (art. 11.º, nº 5 da LCCD, art. 342.º, nº 1 do CCivil), o qual terá assim toda a vantagem

64 Sendo um prazo estabelecido em favor do consumidor, nada impede que desista do contrato mesmo antes de os bens chegarem à sua posse ou possa recusar tomar posse destes. Por exemplo, se, após encomendar um produto ao empresário A, o consumidor encontrar uma melhor oferta no mercado junto do empresário B, dever-lhe-á ser lícito notificar A do exercício do seu direito de desistência mesmo antes de aquele lhe ter sido entregue ou até recusar essa entrega, v.g., informando A que não levantará a encomenda no local de entrega convencionado (v.g., balcão do estabelecimento, posto dos correios).

em enviar as declarações e modelos em apreço por carta registada com aviso de receção ou por correio eletrónico com aviso de leitura.

8.4. Natureza

I. O direito de desistência pode possuir uma *natureza resolutiva* ou *suspensiva*. É sabido que o direito de desistência consiste num direito potestativo do consumidor se desvincular de um contrato de consumo celebrado, através de mera declaração unilateral e discricionária. Todavia, os respetivos efeitos sobre o contrato variam consoante o objeto deste.

II. Nos contratos sobre bens, o direito terá uma eficácia *resolutiva*, ou seja, o contrato celebrado é válido e eficaz entre as partes, vendo os seus efeitos extinguir-se com o exercício tempestivo daquele direito por parte do consumidor: tal significa que, tratando-se de uma compra e venda, o consumidor se torna proprietário do bem (art. 408.º do CCivil) e o risco passa a correr por sua conta (art. 796.º do CCivil), podendo utilizar o bem com os ónus previstos no art. 14.º da LCCD.[65]

III. Já nos contratos sobre serviços, o direito terá uma eficácia *suspensiva*, ou seja, o contrato será originariamente ineficaz, vendo os seus efeitos suspensos até ao termo do prazo legal sem que sobrevenha o respetivo exercício por parte do consumidor (art. 15.º, nº 1, "a contrario sensu", da LCCD). A lei permite todavia ao consumidor evitar este resultado, exigindo ao empresário o cumprimento imediato do contrato mediante pedido expresso em suporte duradouro (art. 15.º, nºs 1 e 7 da LCCD)[66], sem perder o seu direito de desistência (exceto se o serviço já tiver sido integralmente prestado: cf. art. 15.º, nº 1 da LCCD) e sem custos adicionais (art. 15.º, nº 5 da LCCD), embora naturalmente sujeito ao pagamento de um montante proporcional aos serviços efetivamente prestados até ao momento do exercício desse direito (art. 15.º, nºs 3 e 4 da LCCD).

---

65 Sobre estes ónus, vide BARATA, C. LACERDA, *Contratos Celebrados Fora do Estabelecimento Comercial*, 97, in: V "Estudos do Instituto de Direito do Consumo" (2017), 41-127.

66 Esta faculdade foi prevista pelo legislador com vista a assegurar a plena consecução dos fins subjacentes ao próprio direito de desistência no âmbito dos contratos de prestação de serviços, já que, ficando o contrato suspenso durante o decurso do prazo legal, o consumidor não terá possibilidade de avaliar o serviço prestado por forma a poder decidir sobre o seu interesse em manter ou desistir do contrato celebrado.

8.5. Efeitos

I. O exercício do direito de desistência despoleta um conjunto de *efeitos*. Os principais efeitos consistem na extinção das obrigações de execução do contrato e consequentes deveres recíprocos de restituição a cargo das partes contratantes.

II. Assim, o empresário terá o *dever de reembolsar o consumidor* de todos os montantes recebidos (incluindo os custos adicionais de entrega: cf. art. 12.º, nºs 2 e 3 da LCCD), no prazo de 14 dias após o conhecimento da desistência contratual e mediante utilização de meio de pagamento idêntico ao utilizado na transação inicial (art. 12.º, nº 2 da LCCD), sob pena de ficar sujeito a uma obrigação de reembolso em dobro e eventual obrigação de indemnização (art. 12.º, nº 6 da LCCD)[67].

III. Em contrapartida, o consumidor terá o *dever de devolver os bens ao empresário* ou a terceiro autorizado para o efeito no prazo de 14 dias após a comunicação da sua desistência contratual (art. 13.º, nº 1 da LCCD), estando obrigado a conservar os bens nas devidas condições de utilização de modo a não incorrer em qualquer responsabilidade (art. 13.º, nºs 3 e 4 da LCCD)[68] e, em princípio, a suportar os custos da respetiva devolução – exceto no caso de acordo das partes em sentido contrário ou de omissão de informação prévia por parte do empresário (art. 13.º, nº 2 da LCDD).[69]

IV. Aspeto relevante é que o cumprimento destes deveres das partes contratantes está sujeito ao princípio geral da boa fé (art. 9.º, nº 1 da LDC, arts. 334.º e 762.º do CCivil), e sendo sinalagmáticos, à regra geral da exceção de não cumprimento (art. 428.º do CCivil): nem o consumidor terá a obrigação de devolução do bem enquanto o

67 Sobre esta obrigação de reembolso em dobro, vide o Acórdão da Relação do Porto de 27-IV-2015 (CARLOS GIL), segundo o qual tal obrigação tem carácter sancionatório da mora do obrigado à devolução, dependendo dos pressupostos gerais do nascimento da obrigação de indemnização, salvo no que respeita à demonstração da existência e extensão do dano, que são legalmente ficcionadas pela própria lei em montante igual ao da devolução (in: www.dgsi.pt).

68 No Acórdão do TJUE de 3-IX-1993 (*Pia Messner c. Firma Stefan Krüger*) foi considerado que uma regulamentação nacional que imponha ao consumidor o ónus da prova de que não utilizou esse bem durante o prazo do direito de desistência, de uma forma que fosse além do necessário ao exercício útil deste, afetaria adversamente a eficácia e a efetividade desse mesmo direito (in: ECLI:EU:C:2009:502 [§ 27]).

69 O regime das obrigações de empresário e consumidor está sujeito a regras especiais no caso dos contratos que tenham por objeto prestações de serviços (art. 15.º da LCCD).

profissional não reembolsar o pagamento efetuado, nem este terá a obrigação de reembolso enquanto aquele se recusar a restituir-lhe o bem fornecido[70].

V. Ao lado destes efeitos principais, o direito de desistência envolve outros efeitos secundários. Entre eles, destacam-se a resolução automática dos *contratos acessórios* do contrato celebrado à distância (v.g., contrato de financiamento ou de seguro da aquisição, de instalação ou manutenção, garantia comercial adicional: cf. art. 3.º, g) da LCCD), não havendo lugar, em princípio, ao pagamento de qualquer indemnização ou de quaisquer encargos (art. 16.º da LCCD); e as obrigações especiais do empresário em matéria *dos dados pessoais do consumidor* à luz das regras do RGPD (art. 13.º, nºs 7 a 11 da LCCD, art. 36.º, nºs 3 a 5 da LVBC).

8.6. Exceções

I. Finalmente, o direito de desistência do consumidor encontra-se sujeito a um vasto conjunto de *exceções* previstas na lei, num total de treze (art. 17.º da LCCD).

De entre estas, entre algumas das mais relevantes no âmbito dos contratos à distância, podem citar-se os seguintes casos:

- bens confecionados de acordo com especificações do consumidor ou manifestamente personalizados, v.g., mobiliário especial fabricado a partir do catálogo do fabricante, automóvel com equipamento especial (art. 17.º, nº 1, c) da LCCD);[71]
- serviços tenham sido integralmente prestados após o prévio consentimento expresso do consumidor, v.g., serviços públicos essenciais (água, eletricidade, gás, etc.) ou de comunicações eletrónicas (telefone, televisão, "internet", etc.) imediatamente acionados a pedido daquele,

70 Sobre a boa fé nas relações jurídicas de consumo, vide CALDEIRA, MIRELLA, *A Boa-Fé Objetiva como Princípio Norteador das Relações de Consumo*, in: 2 "Revista da Faculdade de Direito da Universidade Metodista" (2005), 193-217; JÚNIOR, R. ROSADO, *A Boa-Fé na Relação de Consumo*, in: 14 "Revista de Direito do Consumidor" (1995), 20-27.

71 De acordo com a jurisprudência europeia, esta exceção é aplicável independentemente de o empresário ter ou não já começado a trabalhar na encomenda do consumidor (Acórdão do TJUE de 21-X-2020 (*Möbel Kraft GmbH & Co. KG c. ML*), in: ECLI:EU:C:2020:846 [§§ 27 a 29]), mas já não se aplica aos contratos de prestação de serviços que conduzam a resultados tangíveis (Acórdão do TJUE de 14-V-2020 (*NK c. MS e AS*), in: ECLI:EU:C:2020:382 [§§ 58 e 59]).

devidamente informado da perda do seu direito a desistir (arts. 15.º e 17.º, nº 1, a) da LCCD);

– bens selados não suscetíveis de devolução, por motivos de proteção da saúde ou de higiene quando abertos após a entrega, v.g., produtos cosméticos, escovas de dentes, etc. (art. 17.º, nº 1, d) da LCCD[72];

– gravações áudio ou vídeo seladas ou de programas informáticos selados, a que o consumidor tenha retirado o selo de garantia de inviolabilidade após a entrega, v.g., CD, DVD, "software" (art. 17.º, nº 1, h) da LCCD);

– serviços de alojamento, para fins não residenciais, transporte de bens, aluguer automóvel, restauração ou serviços relacionados com atividades de lazer com data ou período de execução específicos, v.g., reservas de hotéis, de casas de férias, de ingressos em eventos culturais ou desportivos (art. 17.º, nº 1, k) da LCCD)[73]; ou ainda

– conteúdos digitais sempre que o empresário tenha confirmado a celebração do contrato e a execução deste se tenha iniciado com o consentimento prévio e expresso do consumidor que revele o conhecimento deste relativamente à perda do seu direito a desistir (arts. 6.º, 10.º, nº 1, c), 15.º, nº 5, b) e 17.º, nº 1, l) da LCCD).[74]

72 O Acórdão do TJUE de 27-III-2019 *(Slewo c. Sascha Ledowski)* decidiu que esta exceção deverá ser aplicada caso a caso em função da natureza dos bens, admitindo que em determinadas vendas à distância o consumidor mantenha o seu direito de desistência do contrato mesmo quando tenha removido a selagem do bem comprado, exceto quando com tal remoção o bem deixar de estar definitivamente em condições de ser comercializado por motivos de proteção da saúde ou de higiene (in: ECLI:EU:C:2018:1041 [§40]).

73 Cf. CARVALHO, J. MORAIS, *Contrato para Assistência a Espetáculo Desportivo*, in: VIII "Desporto & Direito – Revista Jurídica do Desporto" (2011), 355-387. Na jurisprudência, vejam-se os Acórdãos do TJUE de 10-III-2005 (*easyCar (UK) Ltd c. Office of Fair Trading)* – que considerou esta exceção aplicável à disponibilização de meio de transporte ao consumidor (in: ECLI:EU:C:2005:150 [§§ 26 e 31] – e de 31-III-2022 (*DM c. CTS Eventim AG & Co. KGaA*) – que considerou esta exceção também aplicável aos contratos celebrados através de intermediários (in: ECLI:EU:C:2022:238 [§ 55]).

74 Sustentando uma interpretação restritiva desta exceção, vide o Acórdão do TJUE de 8-X-2020 (*EU c. PE Digital GmbH*), in: ECLI:EU:C:2020:808 [§§ 41 a 46].

9. O Caso Particular dos Serviços Financeiros à Distância

9.1. Aspetos Gerais

I. Os *contratos à distância sobre serviços financeiros* são contratos celebrados entre um prestador de serviços financeiros e um consumidor que, tendo por objeto a prestação de um ou mais serviços financeiros (bancários, seguradores, de investimento, etc.), se integra num sistema organizado de venda ou comercialização à distância do primeiro e foi negociado e concluído exclusivamente através de um meio de comunicação à distância.[75]

II. Encontrámo-nos diante de uma modalidade particular dos contratos à distância, que, tendo sido excluída do âmbito de aplicação da LCCD (art. 2.º, nº 3, a)), foi objeto de uma disciplina jurídica própria através do *Decreto-Lei nº 95/2006, de 29 de maio*, o qual veio transpor este nós a Diretiva 2002/65/CE, de 23 de setembro, relativa à comercialização à distância de serviços financeiros prestados a consumidores[76]. As razões desta autonomização são diversas: a enorme variedade e a complexidade dos serviços e produtos financeiros, a desmaterialização progressiva da informação e comercialização destes produtos e serviços (que deixaram de ser negociados em balcão para o serem crescentemente através dos sítios "web" dos seus prestadores) e o grau de iliteracia financeira dos consumidores são alguns dos motivos mais frequentemente invocados.

9.2. Âmbito de Aplicação

I. O âmbito objetivo de aplicação do regime legal é muito vasto, sendo aplicável aos *serviços financeiros*, entendendo-se por tal "qualquer serviço bancário, de crédito,

---

75 Sobre a figura, BOURA, MARTA, *Serviços Financeiros à Distância*, in: Ataíde, R./ Rocha, F./ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. I, 803-830, Lisboa, 2023; CORDEIRO, A. MENEZES, *A Tutela do Consumidor de Produtos Financeiros*, in: "Liber Amicorum Mário Frota – A Causa dos Direitos dos Consumidores", 51-60, Almedina, Coimbra, 2012; LIZ, J. PEGADO, *A Comercialização à Distância de Serviços Financeiros*, in: 25 "Revista Portuguesa de Direito do Consumo" (2001), 50-51; RODRIGUES, S. NASCIMENTO, *O Direito de Resolução do Investidor na Contratação de Serviços Financeiros à Distância*, in: AA.VV., "Direito dos Valores Mobiliários", vol. VII, 233-273, Almedina, Coimbra, 2007. Para mais desenvolvimentos, BRAVO, FABIO, *Commercializzazione a Distanza dei Servizi Finanziari ai Consumatori*, Ipsoa, Milano, 2003.

76 Merece ainda ser salientado que, como direito subsidiário, não foi prevista a aplicação da LCCD, mas sim o regime da LCE e do CVM (art. 39.º do Decreto-Lei nº 95/2006).

de seguros, de investimento ou de pagamento e os relacionados com a adesão individual a fundos de pensões abertos" (art. 1.º e 2.º, c) do Decreto-Lei nº 95/2006).

II. Estão assim aqui incluídos todos os contratos bancários – v.g., contratos de conta bancária, de crédito, de financiamento, de garantia (art. 4.º do RGIC) –[77], os contratos de intermediação financeira – v.g., contratos de investimento, contratos auxiliares, contratos derivados (arts. 289.º e segs. do CVM) –[78], os contratos de seguros – v.g., seguros de pessoas e danos, seguros de capitalização, instrumentos de captação de aforro estruturado, apólices "unit linked", PRIIPs (arts. 123.º e segs., 206.º e 207.º da LCS, art. 3.º do RGAS) –[79], os contratos de serviços de pagamento – v.g., gestão de contas de pagamento, depósitos e levantamentos de numerário, execução de operações de pagamento, transferências de fundos, emissão de instrumentos de pagamento (art. 11.º do RJSPME)[80] – e ainda os serviços de adesão individual a fundos de pensões abertos (arts. 8.º e 29.º do RJFP).

III. O âmbito subjetivo do regime legal não é menor, em consequência da amplitude do conceito de serviço financeiro acolhido. Estão aqui abrangidos os contratos à distância celebrados por qualquer "*prestador de serviços financeiros*" (art. 2.º, d) do Decreto-Lei nº 95/2006), incluindo assim as instituições de crédito e sociedades financeiras (arts. 2.º, 3.º, 5.º e 6.º do RGIC), as instituições de pagamento (art. 11.º do RJSPME), as instituições de moeda eletrónica (art. 12.º do RJSPME), os intermediários financeiros em valores mobiliários (art. 293.º do CVM, art. 1.º do REI), as empresas de seguros e resseguros (arts. 3.º, 5.º, nº 1, a) e d) do RGAS), os

77 Sobre os contratos bancários, vide ANTUNES, J. ENGRÁCIA, *Os Contratos Bancários,* in: AA.VV., "Estudos em Homenagem ao Professor Doutor Carlos Ferreira de Almeida", vol. II, 71-155, Almedina, Coimbra, 2011

78 Sobre os contratos de intermediação financeira, vide ANTUNES, J. ENGRÁCIA, *Os Contratos de Intermediação Financeira*, in: LXXXV "Boletim da Faculdade de Direito da Universidade de Coimbra" (2009), 277-319; ANTUNES, J. Engrácia, *Os Instrumentos Financeiros,* esp. 187 e ss., 4ª edição, Almedina, Coimbra, 2020.

79 Sobre os contratos de seguro, vide ANTUNES, J. ENGRÁCIA, *O Contrato de Seguro na LCS de 2008*, in: 69 "Revista da Ordem dos Advogados" (2009), vol. III/IV, 815-858. Em particular sobre os seguros à distância, ALVES, P. RIBEIRO, *Contrato de Seguro à Distância – O Contrato Eletrónico*, Almedina, Coimbra, 2009; FROTA, MÁRIO, *Contrato à Distância: O Contrato de Seguro,* in: 35 "Revista Portuguesa de Direito do Consumo" (2003), 13-26; MARTINS, A. SOVERAL, *Contratação à Distância e Contrato de Seguro,* in: 10 "Estudos de Direito do Consumidor" (2016), 91-153; MARTINEZ, P. ROMANO, *Celebração de Contratos à Distância e o Novo Regime do Contrato de Seguro*, in: 50 "Revista de Direito e de Estudos Sociais" (2009), 85-116.

80 Sobre os contratos de serviços de pagamento, vide GUIMARÃES, M. RAQUEL, *Os Contratos-Quadro de Prestação de Serviços de Pagamento*, in: "I Congresso de Direito do Consumo", 177-188, Almedina, Coimbra, 2016; ROCHA, F. RODRIGUES, *Do Giro Bancário: Reflexões à Luz do Novo Regime dos Serviços de Pagamento*, in: "Cadernos O Direito nº 9", 99-177, Almedina, Coimbra, 2014.

mediadores de seguros (Lei nº 7/2019, de 16 de janeiro) e as sociedades gestoras de fundos de pensões (arts. 64.º e segs. do RJFP). Por outro lado, em linha com o conceito geral de consumidor acolhido na ordem jurídica portuguesa e também consagrado na própria LCCD, o legislador abrangeu aqui apenas o *consumidor "pessoa singular"* (art. 2.º, d) do Decreto-Lei nº 95/2006), excluindo da tutela legal as pessoas coletivas[81]. Em qualquer caso, importa sublinhar que os investidores não profissionais não são idênticos mas apenas equiparados aos consumidores (art. 321.º, nº 3 do CVM), havendo assim uma convergência de fins (proteção dos contraentes débeis) mas não necessariamente de conceitos (tratando-se de "facti-species" legais distintas): por conseguinte, tal equiparação legal não é automática e tem um alcance limitado à aplicação da LCCG, devendo ser devidamente cotejada caso a caso para efeitos da extensão do demais regime jusconsumerista.[82]

9.3. Regime Aplicável

I. O regime legal encontra-se praticamente centrado em torno de três aspetos nucleares desta modalidade especial dos contratos à distância.

II. Por um lado, a disciplina da *informação pré-contratual* (art. 11.º a 18.º do Decreto-Lei nº 95/2006)**,** na qual o legislador teve por objetivo confesso conferir um elevado nível de tutela informativa ao consumidor, incluindo quanto à forma, momento e clareza da informação (arts. 11.º e 12.º) bem como às informações relativas ao prestador do serviço financeiro (art. 13.º), ao serviço financeiro propriamente dito (art. 14.º), ao contrato de prestação de serviços (art. 15.º), aos mecanismos de proteção (art. 16.º) e outra informação adicional (art. 17.º).

---

81 Sobre tal conceito de consumidor, vide ANTUNES, J. ENGRÁCIA, *O Conceito Jurídico de Consumidor*, in: III "Revista de Direito Civil" (2018), 771-796. Em sentido oposto, sustentando a extensão do regime aos consumidores coletivos, BOURA, MARTA, *Serviços Financeiros à Distância,* 813 e ss., in: Ataíde, R./ Rocha, F./ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. I, 803-830, Lisboa, 2023.

82 Sobre tal questão, vide ANTUNES, J. ENGRÁCIA, *Deveres e Responsabilidade do Intermediário Financeiro*, 51 e s., in: 56 "Cadernos do Mercado de Valores Mobiliários" (2017), 31-52; ALMEIDA, FÁBIO, *Publicidade Relativa a Instrumentos Financeiros Dirigidos a Consumidores*, 1029 e s., in: AA.VV., "Estudos de Direito do Consumo", vol. II, 1017-1047, Almedina, Coimbra, 2023; ASCENSÃO, J. OLIVEIRA, *A Proteção do Investidor*, 38 e ss., in: AA.VV., "Direito dos Valores Mobiliários", vol. IV, 13-40, Coimbra Editora, 2003; CÂMARA, PAULO, *Manual de Direito dos Valores Mobiliários,* 256 e ss., 4ª edição, Almedina, Coimbra, 2018; CORDEIRO, A. BARRETO, *Manual de Direito dos Valores Mobiliários,* 111 e ss., 2ª edição, Almedina, Coimbra, 2018. Noutros quadrantes, RIESENHUBER, KARL, *Anleger und Verbraucher*, in: 26 "Zeitschrift für Bankrecht und Bankwirtschaft" (2014), 134-149; WAGNER, KLAUS, *Sind Kapitalanleger Verbraucher?*, in: "Zeitschrift für Bank- und Kapitalmarktrecht" (2003), 649-656.

III. Por outro lado, o legislador ocupou-se da disciplina do *direito de desistência* ou de "livre resolução" do contrato (arts. 19.º a 25.º do Decreto-Lei nº 95/2006), incluindo o prazo (art. 20.º), a forma (art. 21.º) e os efeitos do seu exercício (art. 24.º), bem assim como as suas exceções (art. 22.º), a sua caducidade (art. 23.º) e o início da execução contratual "medio temporae" (art. 25.º).

IV. Finalmente, foi ainda previsto um substancial e relevante regime *fiscalizador e sancionatório* (arts. 26.º a 36.º, todos do Decreto-Lei nº 95/2006).

Abreviaturas

AA.VV.	Autores Vários
CCivil	Código Civil
CCom	Código Comercial
CPC	Código de Processo Civil
CPub	Código da Publicidade
CVM	Código dos Valores Mobiliários
LCCD	Lei dos Contratos Celebrados à Distância e Fora do Estabelecimento Comercial
LCCG	Lei das Cláusulas Contratuais Gerais
LCE	Lei do Comércio Eletrónico
LDE	Lei dos Documentos Eletrónicos
LcomunE	Lei das Comunicações Eletrónicas
LCS	Lei do Contrato de Seguro
LDC	Lei de Defesa do Consumidor
LPCD	Lei das Práticas Comerciais Desleais
LVBC	Lei das Vendas de Bens de Consumo
LTV	Lei da Televisão
PRIIP	Packaged Retail and Insurance-based Investment Products
REI	Regime das Empresas de Investimento
RGIC	Regime das Instituições de Crédito e Sociedades Financeiras
RGAS	Regime Geral da Atividade Seguradora e Resseguradora
RGPD	Regulamento Geral da Proteção de Dados
RJFP	Regime Jurídico dos Fundos de Pensões
RJSPME	Regime Jurídico dos Serviços de Pagamento e Moeda Eletrónica
STJ	Supremo Tribunal de Justiça
TJUE	Tribunal de Justiça da União Europeia

Bibliografia

ALMEIDA, FÁBIO, *Publicidade Relativa a Instrumentos Financeiros Dirigidos a Consumidores.* In: AA.VV., "Estudos de Direito do Consumo", vol. II, 1017-1047, Almedina, Coimbra, 2023.

ALVES, P. RIBEIRO, *Contrato de Seguro à Distância – O Contrato Eletrónico.* Almedina, Coimbra, 2009.

ANTUNES, J. ENGRÁCIA, *Deveres e Responsabilidade do Intermediário Financeiro*. In: 56 "Cadernos do Mercado de Valores Mobiliários" (2017), 31-52.

ANTUNES, J. ENGRÁCIA, *Direito do Consumo.* Almedina, Coimbra, 2019.

ANTUNES, J. ENGRÁCIA, *Direito dos Contratos Comerciais.* 7ª reimpressão, Almedina, Coimbra, 2021.

ANTUNES, J. ENGRÁCIA, *O Conceito Jurídico de Consumidor*. In: III "Revista de Direito Civil" (2018), 771-796.

ANTUNES, J. ENGRÁCIA, *O Contrato de Seguro na LCS de 2008*. In: 69 "Revista da Ordem dos Advogados" (2009), vol. III/IV, 815-858.

ANTUNES, J. ENGRÁCIA, *O Regime Geral da Contratação de Consumo.* In: 2 "Anuário do Nova Consumer Lab – Yearbook of the Nova Consumer Lab" (2020), 123-163.

ANTUNES, J. ENGRÁCIA, *Os Contratos Bancários.* In: AA.VV., "Estudos em Homenagem ao Professor Doutor Carlos Ferreira de Almeida", vol. II, 71-155, Almedina, Coimbra, 2011.

ANTUNES, J. ENGRÁCIA, *Os Contratos de Intermediação Financeira*, in: LXXXV "Boletim da Faculdade de Direito da Universidade de Coimbra" (2009), 277-319.

ANTUNES, J. ENGRÁCIA, *Os Contratos Fora do Estabelecimento.* In: Ataíde, R./ Rocha, F./ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. I, 767-775, Lisboa, 2023.

ANTUNES, J. ENGRÁCIA, *Os Instrumentos Financeiros.* 4ª edição, Almedina, Coimbra, 2020.

ASCENSÃO, J. OLIVEIRA, *A Proteção do Investidor.* In: AA.VV., "Direito dos Valores Mobiliários", vol. IV, 13-40, Coimbra Editora, 2003.

BARATA, C. LACERDA, *Contratos Celebrados Fora do Estabelecimento Comercial*. In: V "Estudos de Direito do Instituto do Consumo" (2017), 41-127.

BARROS, J. LEITE, *Os Contratos de Consumo Celebrados pela Internet.* In: 3 "Revista Jurídica Luso-Brasileira" (2017), 781-843.

BETTENCOURT, M. ORTINS, *A Proteção do Consumidor em Contratos Digitais: Análise dos Contratos Celebrados com Dados Pessoais como Contraprestação*. In: 3 "Anuário do Nova Consumer Lab" (2021), 387-476.

BOURA, MARTA, *Serviços Financeiros à Distância.* In: Ataíde, R./ Rocha, F./ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. I, 803-830, Lisboa, 2023.

BRAVO, FABIO, *Commercializzazione a Distanza dei Servizi Finanziari ai Consumatori*. Ipsoa, Milano, 2003.

BRITO, I. RODRIGUES, *Dever de Informação nos Contratos à Distância e ao Domicílio*. In: 5 "Estudos de Direito do Consumidor" (2005), 477-517

BRUNAUX, GEOFFRAY, *Le Contrat à Distance au XXI^{ème} Siècle*. LGDJ, Paris, 2010.

CALDEIRA, MIRELLA, *A Boa-Fé Objetiva como Princípio Norteador das Relações de Consumo*. In: 2 "Revista da Faculdade de Direito da Universidade Metodista" (2005), 193-217.

CÂMARA, PAULO, *Manual de Direito dos Valores Mobiliários.* 4ª edição, Almedina, Coimbra, 2018.

CARVALHO, J. MORAIS, *Compra e Venda e Fornecimento de Conteúdos e Serviços Digitais – Anotação ao Decreto-Lei nº 84/2021, de 18 de Outubro*. Almedina, Coimbra, 2022.

CARVALHO, J. MORAIS, *Contrato para Assistência a Espetáculo Desportivo*. In: VIII "Desporto & Direito – Revista Jurídica do Desporto" (2011), 355-387.

CARVALHO, J. MORAIS, *Manual de Direito do Consumo.* 8ª edição, Almedina, Coimbra, 2022.

CARVALHO, J. MORAIS, *Prestação de Informações nos Contratos Celebrados à Distância*. In: AA.VV., "Direito Privado e Direito Comunitário", 13-144, Âncora Editora, Lisboa, 2009.

CARVALHO, J. MORAIS/ PINTO-FERREIRA, J. PEDRO/ CARVALHO, J. Campos, *Manual de Resolução Alternativa de Litígios de Consumo,* Almedina, Coimbra, 2017.

CHEN, CHEN, *Contratos à Distância em Geral.* In: Ataíde, R./ Rocha, F./ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. I, 777-801, Lisboa, 2023.

COEHEN-ADT, GREGOR, *Der Fernabsatzvertrag: Anwendungsvoraussetzungen und -probleme beim Versandhandel*. Logos Verlag, Berlin, 2009.

COELHO, J. GALHARDO, *Publicidade Domiciliária – O Marketing Direto.* Almedina, Coimbra, 1999

CORDEIRO, A. BARRETO, *Manual de Direito dos Valores Mobiliários.* 2ª edição, Almedina, Coimbra, 2018.

CORDEIRO, A. MENEZES, *A Tutela do Consumidor de Produtos Financeiros*. In: "Liber Amicorum Mário Frota – A Causa dos Direitos dos Consumidores", 51-60, Almedina, Coimbra, 2012.

CORREIA, M. PUPO, *Contratos à Distância: Uma Fase na Evolução da Defesa do Consumidor na Sociedade de Informação?*. In*:* 4 "Estudos de Direito do Consumidor" (2002), 165-180.

COSTA, I. SILVA, A *Proteção da Pessoa na Era dos Big Data: A Opacidade do Algoritmo e as Decisões Automatizadas*. In: 24 "Revista Electrónica de Direito" (2021), 33-82.

DEMOULIN, MARIE, *La Notion de «Support Durable» dans les Contrats à Distance*. In: 4 "Revue Européenne de Droit de la Consommation" (2000), 361-377.

DINIS, MARISA, *Contratos Celebrados à Distância e Contratos Celebrados Fora do Estabelecimento Comercial*. In: 77 "Revista Portuguesa de Direito do Consumo" (2014), 11-38.

DODSWORTH, TIMOTHY, *Intermediaries as Sellers – A Commentary on «Wathelet»*. In: 5 "Journal of European Consumer and Market Law" (2017), 213-215.

DUARTE, MARIANA, *O Novo Regime dos Contratos Celebrados à Distância e Fora do Estabelecimento Comercial: Reforço da Protecção do Consumidor?*. In: 2 "Ab Instantia - Revista do Instituto do Conhecimento AB" (2014), 115-119.

FALCÃO, DAVID, *Análise à Nova Lei das Garantias: DL 84/2021, de 18 de Outubro*. In: 81 "Revista da Ordem dos Advogados" (2021), 493-541.

FARINHA, MARTIM, *Os Limites da Proteção dos Consumidores no Regime de Tratamento de Dados Pessoais Contraprestação na Diretiva (EU)2019//770*. In: Carvalho, J. Morais/ Crispim, Inês/ Silva, M. Oliveira/ Farinha, Martim, "Diretivas 2019/770 e 2019/771 e Decreto-Lei n.º 84/2021: Compra e Venda, Fornecimento de Conteúdos e Serviços Digitais, Conformidade, Sustentabilidade e Dados Pessoais", 143-185, Almedina, Coimbra, 2022.

FERNANDES, L. CARVALHO, *Teoria Geral do Direito Civil*. Volume II, 5ª edição, UC Editora, Lisboa, 2010.

FRATERNALE, ANTONIO, *I Contratti a Distanza*. Giuffrè Editore, Milano, 2002.

FROTA, MÁRIO, *Contrato à Distância: O Contrato de Seguro*. In: 35 "Revista Portuguesa de Direito do Consumo" (2003), 13-26.

GUIMARÃES, M. RAQUEL, *As Plataformas "Colaborativas" enquanto Prestadoras de Serviços da Sociedade de Informação*. In: Carvalho, M./ Sousa, A. (coord.), "Economia Colaborativa", 468-498, UMinho Editora, Braga, 2023.

GUIMARÃES, M. RAQUEL, *Os Contratos-Quadro de Prestação de Serviços de Pagamento*. In: "I Congresso de Direito do Consumo", 177-188, Almedina, Coimbra, 2016.

JÚNIOR, R. ROSADO, *A Boa-Fé na Relação de Consumo*. In: 14 "Revista de Direito do Consumidor" (1995), 20-27.

LEITÃO, L. MENEZES, *Desconformidade e Meios de Tutela do Adquirente na Venda de Bens de Consumo*. In: Ataíde, R./ Rocha, F./ Fidalgo, V. (cor.), "Estudos de Direito do Consumo", vol. II, 161-185, Almedina, Coimbra, 2023.

LIZ, J. PEGADO, *A Comercialização à Distância de Serviços Financeiros*. In: 25 "Revista Portuguesa de Direito do Consumo" (2001), 50-51.

MAIA, PEDRO, *Contratação à Distância e Práticas Comerciais Desleais.* In: 9 "Estudos de Direito do Consumidor" (2015), 143-175.

MARTINEZ, P. ROMANO, *Celebração de Contratos à Distância e o Novo Regime do Contrato de Seguro*. In: 50 "Revista de Direito e de Estudos Sociais" (2009), 85-116.

MARTINS, A. SOVERAL, *Contratação à Distância e Contrato de Seguro.* In: 10 "Estudos de Direito do Consumidor" (2016), 91-153.

MELO, MANUEL, *Regime Jurídico dos Centros Telefónicos de Relacionamento ("Call-Centers").* Dissertação, Lisboa, 2016.

MENDES, I. PEREIRA, *Direito Real de Habitação Periódica*. Almedina, Coimbra, 1993.

MONTEIRO, A. PINTO, *O Novo Regime da Contratação à Distância.* In: 9 "Estudos de Direito do Consumidor" (2015), 11-18.

MOREIRA, TERESA, *Novos Desafios para a Contratação à Distância – A Perspetiva da Defesa do Consumidor*. In: 9 "Estudos de Direito do Consumidor" (2015), 19-36.

NUNES, P. CAETANO, *Comunicação de Cláusulas Contratuais Gerais.* In: "Estudos em Homenagem ao Prof. Doutor C. Ferreira de Almeida", vol. II, 507-534, Almedina, Coimbra, 2011.

OLIVEIRA, A. FILIPE, *Dos Contratos Negociados à Distância.* In: 7 "Revista Portuguesa de Direito do Consumo" (1996), 52-96.

OLIVEIRA, E. DIAS, *A Protecção dos Consumidores nos Contratos Celebrados Através da Internet*. Almedina, Coimbra, 2002.

OLIVEIRA, M. PERESTRELO, *Definição de Perfis e Decisões Individuais Automatizadas no Regulamento Geral sobre a Proteção de Dados*. In: Cordeiro, A./ Oliveira, A./ Duarte, D. (coord.), "Fintech – Novos Estudos sobre Tecnologia Financeira", 61-88, Almedina, Coimbra, 2019.

PASSINHAS, SANDRA, *Jurisprudência Relevante em Matéria de Contratação à Distância*. In: 9 "Estudos de Direito do Consumidor" (2015), 251-277.

PÉREZ, N. FERNÁNDEZ, *El Nuevo Régimen de Contratación a Distancia con Consumidores*. La Ley, Madrid, 2009.

PINTO, P. MOTA, *Notas Sobre a Lei nº 6/99, de 27 de janeiro – Publicidade Domiciliária, por Telefone e por Telecópia.* In: 1 "Estudos de Direito do Consumidor" (1999), 117-176.

PINTO, P. MOTA, *O Novo Regime Jurídico dos Contratos à Distância e dos Contratos Celebrados Fora do Estabelecimento Comercial.* In: 9 "Estudos de Direito do Consumidor" (2015), 51-91.

PINTO, P. MOTA, *Princípios Relativos aos Deveres de Informação no Comércio à Distância*. In: 5 "Estudos de Direito do Consumidor" (2003), 183-206.

PINTO-FERREIRA, J. PEDRO/ CARVALHO, J. MORAIS, *Contratos Celebrados à Distância e Fora do Estabelecimento Comercial*, Almedina, Coimbra, 2014.

REBELO, F. NEVES, *O Direito à Informação do Consumidor nos Contratos à Distância.* In: "Liber Amicorum Mário Frota*"*, 103-153, Almedina, Coimbra, 2012.

RIESENHUBER, KARL, *Anleger und Verbraucher*. In: 26 "Zeitschrift für Bankrecht und Bankwirtschaft" (2014), 134-149.

ROCHA, F. Rodrigues, *Do Giro Bancário: Reflexões à Luz do Novo Regime dos Serviços de Pagamento*. In: "Cadernos O Direito nº 9", 99-177, Almedina, Coimbra, 2014.

ROCHA, F. RODRIGUES/ FIDALGO, V. PALMELA/ RODRIGUES, A. BARROSO, *Comunicações Eletrónicas.* In: Ataíde, R./ Rocha, F./ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. II, 67-139, Almedina, Coimbra, 2023.

RODRIGUES, S. NASCIMENTO, *O Direito de Resolução do Investidor na Contratação de Serviços Financeiros à Distância*. In: AA.VV., "Direito dos Valores Mobiliários", vol. VII, 233-273, Almedina, Coimbra, 2007.

SANTO, L. ESPÍRITO, *O Contrato de Viagem Organizada*. Almedina, Coimbra, 2016.

SCHAFFER, FERNANDA, *Procedimentos Médicos – Realizados à Distância e o Código de Defesa do Consumidor*. Juruá Editora, Curitiba, 2006.

SILVA, D. SOUSA, *Contratos à Distância – O Ciberconsumidor*. In: 5 "Estudos de Direito do Consumidor" (2003), 423-456.

SILVA, F. SANTOS, *Dos Contratos Negociados à Distância*. In: 5 "Revista Portuguesa de Direito do Consumo" (1996), 45-58.

SIMÃO, J. CARITA/ SOARES, S. ASSUNÇÃO, *Práticas Comerciais Desleais em Geral e em Linha: A Diretiva (EU) 2019/2161, do Parlamento Europeu e do Conselho, de 7 de novembro, a sua Transposição Parcial para o Decreto-Lei nº 109-G/2021, de 10 de dezembro, e o Reforço da Proteção dos Direitos dos Consumidores*. In: Ataíde, R./ Rocha, F/ Fidalgo, V. (coord.), "Estudos de Direito do Consumo", vol. I, 649-681, Almedina, Coimbra, 2023.

SOUSA, A. TEIXEIRA, *O Direito de Arrependimento nos Contratos Celebrados à Distância e Fora do Estabelecimento: Algumas Notas*. In: "Estudos de Direitos do Consumo: Homenagem a M. Ataíde Ferreira, 18-41, Almedina/ Deco, Lisboa, 2016.

WAGNER, KLAUS, *Sind Kapitalanleger Verbraucher?*. In: "Zeitschrift für Bank- und Kapitalmarktrecht" (2003), 649-656.

O *Cryptojacking* e o seu Enquadramento Jurídico-Penal

DUARTE RODRIGUES NUNES*

SUMÁRIO: Resumo; I. As criptomoedas (*Bitcoin* e *Altcoins*). O funcionamento das operações com criptomoedas; II.Os vários "atores" dos mercados de criptomoedas; III. O *Cryptojacking*; IV. Furto de energia elétrica por via do consumo de energia derivado da utilização não autorizada de um sistema informático alheio? ; V. Burla informática e nas comunicações através da utilização não autorizada e sem qualquer pagamento do sistema informático alheio?; VI. Falsidade informática; VII. Acesso ilegítimo; VIII. Sabotagem informática; IX. Dano relativo a programas ou outros dados informáticos; X. O confisco de vantagens obtidas por via da mineração de criptomoedas com utilização não autorizada de sistemas informáticos alheios; XI. Conclusões; XII. Bibliografia

RESUMO:

A realização das operações com criptomoedas e a sua inserção na *Blockchain* (que funciona como uma espécie de livro de contabilidade digital descentralizado, em que são registadas todas as transações realizadas pelos membros de uma grande comunidade de utilizadores) depende da sua validação (mineração ou criptomineração). A criptomineração é realizada por mineradores, que disponibilizam os seus sistemas informáticos para a validação e o consequente registo de transações na *Blockchain*, recebendo uma determinada contrapartida paga em criptomoedas.

Dado que o pagamento só é feito ao primeiro minerador que "decifrar" o *puzzle* relativo a cada transação, existe uma enorme competição entre os mineradores, que terão de possuir a maior capacidade de computação possível (o que implica um grande dispêndio em energia e em material informático). Por isso, alguns mineradores optam por levar a cabo o *Cryptojacking*, que consiste na utilização não autorizada de um sistema informático (incluindo a sua ligação à Internet) e de energia elétrica alheios para a mineração de criptomoedas.

O *Cryptojacker* irá aceder, sem autorização, a sistemas informáticos alheios e aos dados neles guardados e consumir energia elétrica, que será paga pelo utilizador desse sistema informático. Além disso, irá alterar as configurações do editor de registo do sistema operativo para permitir que a mineração comece (sem que o utilizador se aperceba disso) ou pare automaticamente consoante estejam ou deixem de estar verificadas as condições definidas pelo agente para evitar a deteção pelo utilizador, bem

como o acesso remoto, pelo agente, ao computador *zumbi* através de uma ligação à Internet protegida por uma *password*. E neutralizará os dispositivos de proteção como as *firewalls,* os antivírus, o *antispyware*, etc., para que não bloqueiem o acesso ao sistema nem as operações de mineração.

Deste modo, o *Cryptojacker* poderá cometer os crimes de burla informática, falsidade informática, acesso ilegítimo e dano relativo a programas ou outros dados informáticos, pelo que os pagamentos que recebe pela mineração de criptomoedas constituem vantagens provenientes da prática de crimes e, por isso, são passíveis de confisco nos termos do artigo 110.º, n.º 1, al. b), do Código Penal.

Além disso, se for condenado pela prática de crimes de dano relativo a programas ou outros dados informáticos e/ou de acesso ilegítimo (desde que a sua conduta seja subsumível a alguma das situações mencionadas no artigo 1.º, n.º 1, al. m), da Lei n.º 5/2002, de 11 de janeiro) e estejam verificados os demais pressupostos legais do confisco "alargado", o património do *Cryptojacker* que não seja congruente com os seus rendimentos lícitos (após a dedução das suas despesas) será alvo de confisco "alargado", nos termos do artigo 7.º da Lei n.º 5/2002.

Palavras-Chave: Criptomoeda – Mineração de criptomoedas – *Botnet* – Cibercrime – *Cryptojacking*

***ABSTRACT**:*

The performance of operations with cryptocurrencies and their insertion in the Blockchain (which works as a kind of decentralized digital accounting book, in which all transactions carried out by members of a large community of users are registered) depends on their validation (mining or cryptomining). Cryptomining is carried out by cryptominers, who make their computer systems available for the validation and subsequent registration of transactions on the Blockchain, receiving a payment in cryptocurrencies.

Since payment is made only to the first Cryptominer who "deciphers" the puzzle related to each transaction, there is huge competition between Cryptominers, who must have the greatest possible computing capacity (which implies a large expenditure on

energy and on computer equipment). For this reason, some Cryptominers choose to carry out Cryptojacking, which consists of the unauthorized use of a computer system (including Internet access) and of electricity from others to Cryptomining.

Cryptojacker will access, without authorization, other computer systems and the data stored in them and consume electricity, which will be paid by the user of that computer system. Furthermore, he will change the settings of the operating system registry to allow Cryptomining automatically to start (without the user noticing it) or stop depending on whether the conditions defined by the criminal are or are not checked to avoid detection by the user, as well as remote access by the criminal to the zombie computer via a password-protected Internet connection. And he will neutralize protection devices such as firewalls, antivirus, antispyware, etc., so they won't block neither system access nor Cryptomining operations.

Thus, Cryptojacker may commit crimes of computer-related fraud, computer-related forgery, illegal access and data interference, so the payments he receives for mining cryptocurrencies are proceeds of crimes and, therefore, are liable to forfeiture, pursuant to article 110, paragraph 1, b) of the Penal Code.

In addition, if Cryptojacker is convicted of crimes of data interference and/or illegal access (provided that his conduct is subsumable to any of the situations mentioned in article 1, paragraph 1, m) of Law No. 5/2002, of 11 January 2002) and if the other legal requirements for "extended" confiscation are verified, his assets that are not consistent with its lawful income (after deducting its expenses) will be subject to "extended" confiscation, pursuant to article 7 of Law No. 5/2002.

***Keywords**: Cryptocurrency – Cryptomining – Botnet – Cybercrime – Cryptojacking*

I. As criptomoedas (*Bitcoin* e *Altcoins*). O funcionamento das operações com criptomoedas

As criptomoedas são moedas virtuais utilizadas para a realização de pagamentos em transações comerciais, que se distinguem das moedas convencionais ou fiduciárias (euro, dólar, rublo, iene, libra) por possuírem quatro características específicas.

A criptomoeda mais conhecida e mais utilizada é o *Bitcoin*, embora existam muitas outras, normalmente designadas por *Altcoins*, ou seja, criptomoedas alternativas ao *Bitcoin* (*v.g.*, *Litecoin, Ethereum, Ethereum Classic, Zcash, Namecoin, Peercoin, Ripple, Monero*, etc.).

As características que distinguem as criptomoedas das moedas convencionais ou fiduciárias são: natureza completamente virtual, descentralização, anonimato e gratuitidade da transação, sendo que a natureza completamente virtual e a gratuitidade da transação não carecem de maiores desenvolvimentos, pois, como facilmente se percebe, consistem, respetivamente, em tudo ocorrer no mundo informático-digital e em a realização das transações *ex se* não envolver qualquer custo económico para os intervenientes.

Por seu turno, a descentralização significa que as criptomoedas são independentes da intervenção de um banco central e/ou do Estado para a sua regulamentação, variando a sua cotação apenas em função do funcionamento do mercado e sendo o sistema *Blockchain*[1] o único elemento central que intervém no processo, funcionando como uma espécie de livro de contabilidade digital (descentralizado) em que são registadas todas as transações realizadas pelos membros de uma grande comunidade de utilizadores após a sua validação pelos mineradores (pois a mineração é *conditio sine qua non* da sua efetivação e consequente inserção na *Blockchain*). Tal permite a

---

* Professor Associado da Universidade Europeia. Professor Associado Convidado da Universidade Lusíada – Angola. Doutor em Direito pela Faculdade de Direito de Lisboa. Investigador do IDPCC e do CIJIC. Jurisconsulto. Conferencista. Exerceu as funções de Juiz de Direito entre setembro de 2005 e janeiro de 2022, estando atualmente em situação de licença sem retribuição. Endereço eletrónico: duarterodriguesnunes@hotmail.com.

1 A tecnologia ***Blockchain*** ("cadeia de blocos" em inglês) é um tipo de base de dados que funciona como um registo de contabilidade pública (saldos e transações de contas), onde são registadas as transações com criptomoedas. A tecnologia ***Blockchain*** permite que esses dados informáticos sejam **transmitidos** entre todos os participantes da rede (nós P2P) de uma forma descentralizada e transparente.

verificação pública e rápida no banco de dados e dificulta a atuação dos *Crackers*[2], que, no mundo das criptomoedas, levam a cabo atividades de *Phishing* para obterem as chaves privadas e apropriarem-se da moeda armazenada na carteira[3].

As transações com criptomoedas também garantem um relativo anonimato ao utilizador, que terá de possuir uma carteira (*wallet*)[4]. Esse anonimato é grandemente incrementado (podendo tornar-se num completo anonimato) nos casos em que a utilização de criptomoedas seja acompanhada pela utilização de programas como o Tor ou o Freenet e a transação seja realizada no âmbito da *Dark Web*. De resto, numa transação de criptomoedas, a única informação pública que consta da *Blockchain* é a realização de uma transferência de uma carteira – representada por um determinado endereço (pois cada carteira pode ter mais do que um endereço) – para outra carteira, sendo que, em regra, nenhuma dessas carteiras surge associada a qualquer pessoa física ou coletiva identificada nessa informação publicamente acessível.

As criptomoedas são guardadas em carteiras (*wallets*), que possuem uma chave pública e uma chave privada, servindo a primeira para que outras pessoas enviem criptomoedas para uma determinada carteira (funcionando como uma espécie de

---

2 O *Cracker* é um dos agentes do *Hacking* não ético. O *Hacking* consiste em atividades ilícitas de acesso e penetração em sistemas informáticos alheios (em regra, do Estado, de empresas ou de outras organizações), com a finalidade de obter informações sobre o seu funcionamento ou informações armazenadas nesses sistemas. No âmbito do *Hacking*, costuma distinguir-se entre *Hacking* não ético (aquele que visa provocar prejuízos à vítima ou obter benefícios para o agente ou para terceiro) e *Hacking* ético (aquele em que não são provocados quaisquer prejuízos, podendo existir, inclusivamente, uma cooperação com o detentor do sistema visado, avisando-o de eventuais falhas de segurança).

O agente do *Hacking* ético é o *Hacker*, ao passo que o agente do *Hacking* não ético pode ser um *Cracker* (que pratica o *Hacking* com a finalidade de aceder ao sistema informático alheio para aí causar prejuízos, como, por exemplo, roubar informações, obter *passwords* e outros códigos de acesso, espionagem, entravamento do sistema, destruição de dados), um *Phreaker* (que pratica o *Hacking* acedendo e manipulando redes de telecomunicações ligadas à rede pública, com o objetivo de copiar cartões, realizar interceções de comunicações, realizar chamadas telefónicas sem pagar, usufruir de serviços de televisão sem pagar, etc.) ou um *Carder* (que pratica o *Hacking* com a finalidade de aceder ao sistema informático alheio para roubar códigos de acesso e códigos de cartões de crédito para realizar compras *online*, realizar levantamentos de dinheiro em caixas automáticas, etc.) (cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 154-155 (nota 228).

3 Cfr. EUROPOL, Internet Organised Crime Threat Assessment, 2019, p. 54, em que se refere um caso em que os *Crackers* criaram *websites* em tudo similares aos de *exchangers* e de *wallet providers* legítimos para furtarem chaves privadas e criptomoedas dos utilizadores, tendo atingido um total de cerca de 4.000 vítimas.

4 As *wallets* podem incluir um ou vários endereços (correspondendo cada endereço, *grosso modo*, a uma conta bancária) e consistem numa identificação única, que permite enviar e receber criptomoedas de forma rápida, segura e fácil. As *wallets* podem ser "quentes" (*hot wallets*) – as que funcionam *online*, sendo mais facilmente acessíveis pelo seu utilizador, mas são mais vulneráveis à atuação dos *Crackers* – ou "frias" (*cold wallets*) – as que funcionam *offline*, estando armazenadas em suportes de *hardware* (*v.g.*, numa *pen drive*), o que torna a sua utilização menos "ágil", mas são menos vulneráveis a ataques de *Crackers*.

número de conta público) e a segunda para permitir a utilização das criptomoedas armazenadas na carteira (para realizar pagamentos e/ou transferências para outras carteiras), apenas sendo conhecida pelo proprietário da carteira ou por outras pessoas a quem ele permita a obtenção desse conhecimento (ainda que inadvertidamente).

Pelas suas características e porque os cibercriminosos se adaptam facilmente às mudanças no contexto social e aproveitam todas as novas oportunidades que lhes surgem por via dessas alterações (*maxime* ao nível da prática de novas atividades criminosas e da maior eficácia na execução de atividades criminosas já existentes ou na sua proteção face atuação das autoridades)[5], as criptomoedas são sistematicamente utilizadas em atividades criminosas como o tráfico de drogas, armas, pessoas ou órgãos (desde logo, para o pagamento do fornecimento desses bens ou da prestação desses serviços ilícitos), pagamento de homicídios ou de subornos, branqueamento de capitais e financiamento do terrorismo, extorsão (incluindo o *Ransomware,* a *Sextortion* e os resgates exigidos para pôr fim a ataques de DDoS[6 7])[8], pagamento de acesso a conteúdos de pedofilia e pornografia infantil, etc., independentemente de se tratar de criminosos "individuais" ou de organizações (ou associações) criminosas ou terroristas ou de se tratar de *blue-collar criminals* ou de *white-collar criminals*. E também podem ser utilizadas para fins de investimentos lícitos, tendo em conta a grande valorização que as criptomoedas têm registado, sobretudo no caso do *Bitcoin*.

II. Os vários "atores" dos mercados de criptomoedas

São vários os intervenientes no mercado de criptomoedas: utilizadores (*Users*), mineradores (*Miners* ou *Cryptominers*), prestadores de serviços de câmbio

5 No mesmo sentido, EUROPOL, Internet Organised Crime Threat Assessment, 2020, p. 13.
6 O ataque do tipo *DDoS* (*Distributed Denial of Service*) consiste em um sistema informático "mestre" controlar um número bastante elevado de sistemas informáticos (*zumbis* ou *zombies*), que irão ser "escravizados" para acederem, conjunta e ininterruptamente, ao mesmo recurso de um dado sistema informático, a fim de o sobrecarregar e impedir os seus utilizadores de acederem a esse sistema (que tanto pode ficar bloqueado como reiniciar continuamente, dependendo do recurso que foi atingido pelo ataque).
7 Cfr. MÁRIO ANTUNES/BALTAZAR RODRIGUES, Introdução à Cibersegurança, p. 236, MONIKA SIMMLER/SINE SELMAN/DANIEL BURGMEISTER, "Beschlagnahme von Kryptowährungen", *in* Aktuelle Juristische Praxis - Pratique Juridique Actuelle, n.º 8/2018, pp. 965-966, e EUROPOL, Internet Organised Crime Threat Assessment, 2019, p. 54, e também em Internet Organised Crime Threat Assessment, 2020, p. 17.
8 Cfr. HEINE, "Bitcoins und Botnetze – Strafbarkeit und Vermögenabschöpfung bei illegalem Bitcoin-Mining", *in* NStZ, 2016, p. 441, EUROPOL, Internet Organised Crime Threat Assessment, 2019, p. 54, e MÁRIO ANTUNES/BALTAZAR RODRIGUES, Introdução à Cibersegurança, p. 236.

(*Exchangers*), plataformas de *trading*, prestadores de serviços de carteiras virtuais (*Wallet Providers*), prestadores de serviços de "mistura" de criptomoedas (*Tumblers* ou *Mixers*), inventores (*Inventors*) e emitentes (*Issuers* ou *Offerors*).

Os utilizadores (*Users*) são as pessoas singulares ou coletivas que adquirem e utilizam criptomoedas (para investimento, pagamentos de bens ou serviços, recebimento de pagamentos de bens ou serviços que prestem a título oneroso, etc.).

Os emitentes de criptomoedas (*Issuers* ou *Offerors*) são as pessoas singulares ou coletivas que criam uma nova criptomoeda, lançando-a no mercado, mediante o pagamento de um determinado preço, ao passo que os inventores (*Inventors*) são as pessoas singulares ou coletivas que desenvolvem o aspeto técnico e as normas de protocolo de uma nova criptomoeda.

Os mineradores (*Miners* ou *Cryptominers*) – que são aqueles que nos interessam no âmbito do presente artigo – são as pessoas singulares ou coletivas que disponibilizam os seus sistemas informáticos para a validação e o consequente registo de transações em criptomoedas na *Blockchain*, recebendo, em contrapartida, uma determinada taxa paga em criptomoedas. Na medida em que o pagamento dessa validação só é feito a quem tenha "decifrado" o *puzzle* criptográfico relativo a cada transação em primeiro lugar, estabelece-se uma enorme competição entre os vários mineradores, o que requer que cada um possua a maior capacidade de computação possível e implica igualmente um grande dispêndio em energia e em material informático.

Os prestadores de serviços de câmbios (*Exchangers*) são aqueles que prestam serviços de câmbio entre criptomoedas e moedas fiduciárias (euros, dólares, etc.) e vice-versa ou entre criptomoedas diversas (*v.g. Bitcoins* por *Zcash*), podendo prestar também serviços de guarda de carteiras (*wallets*), o que implica que tenham acesso às chaves criptográficas do utilizador em causa.

As plataformas de *Trading* são mercados digitais que permitem que a compra e venda de criptomoedas entre *Users* ou entre *Issuers* e *Users*. Distinguem-se dos *Exchangers* pelo facto de estas plataformas apenas proporcionarem o "espaço" onde os vendedores e os compradores de criptomoedas realizam as transações entre si, não realizando a plataforma qualquer transação.

Os prestadores de serviços de carteiras (*Wallet Providers*) são as pessoas singulares ou coletivas que disponibilizam aos *Users* as *wallets* onde poderão armazenar as suas criptomoedas e a partir das quais realizam as transações igualmente em criptomoedas, podendo incluir as respetivas chaves criptográficas ou não. Os *Wallet Providers* podem prestar igualmente serviços de guarda de *wallets* nos mesmos termos que referimos quanto aos *Exchangers*.

Por último, os *Mixers* ou *Tumblers* são as pessoas singulares ou coletivas que prestam serviços de "mistura" de criptomoedas, a fim de incrementar o grau de anonimato do utilizador, dificultando o rastreio e a identificação da origem, do destino e dos intervenientes na transação, ou seja, esses serviços poderão – no caso de criptomoedas provenientes de atividades criminosas ou adquiridas com fundos obtidos dessa forma – configurar operações de branqueamento de capitais ou – no caso de se destinarem a financiar ações terroristas ou organizações terroristas – de financiamento do terrorismo.

Tendo em conta a utilização das criptomoedas por criminosos (incluindo organizações criminosas e terroristas e criminosos de colarinho branco) para pagamento de bens e serviços ilícitos ou de dinheiro exigido a título de extorsão, branqueamento de capitais, financiamento do terrorismo, etc., é premente a presença efetiva de um novo "ator": as entidades públicas de regulação, a fim de, se não erradicar, pelo menos, minimizar/dificultar o mais possível a utilização das criptomoedas para fins criminosos e tornar essa utilização mais arriscada para os criminosos através da sua maior deteção (que também poderá constituir a *notitia criminis* e/ou mesmo uma prova do crime associado a essa transação de criptomoedas).

III. O *Cryptojacking*

Como referimos, o pagamento da validação das transações em criptomoedas só é feito a quem tenha "decifrado" o *puzzle* criptográfico relativo a cada transação em primeiro lugar e, por isso, estabelece-se uma enorme competição entre os vários mineradores. Para além disso, essa competição e o grau elevado de criptografia utilizada nas operações com criptomoedas requer que cada minerador possua a maior capacidade

de computação possível, o que implica igualmente um grande dispêndio em energia e em material informático[9].

Por isso, alguns mineradores, com o objetivo de aumentar a sua capacidade de computação e evitar dispêndios com energia elétrica e com a aquisição de material informático, optam por levar a cabo atividades de *Cryptojacking*[10], que consiste na utilização não autorizada de um sistema informático (incluindo a sua ligação à Internet) e de energia elétrica alheios para fins de mineração de criptomoedas[11]. Essa utilização pode ser levada a cabo direta (infetando um sistema informático alheio com *malware*, a fim de "furtar" ciclos de processamento nos momentos definidos pelo *Cryptojacker*) ou indiretamente ("furtando" ciclos de processamento enquanto a vítima visita um determinado *website*)[12].

E o aumento da capacidade de computação será tanto maior quanto maior for o número de sistemas informáticos alheios utilizados, razão pela qual os agentes do crime tentarão construir *botnets*[13] para esse fim[14], o que se torna particularmente necessário no caso do *Bitcoin*, cuja mineração requer uma capacidade de computação muito mais exigente do que no caso de *Altcoins* como o Monero[15]. Na criação das *botnets*, os

---

9 No mesmo sentido, HEINE, "Bitcoins und Botnetze – Strafbarkeit und Vermögenabschöpfung bei illegalem Bitcoin-Mining", *in* NStZ, 2016, p. 441, e Sentença do *Bundesgerichtshof* de 27/07/2017.

10 Cfr. HEINE, "Bitcoins und Botnetze – Strafbarkeit und Vermögenabschöpfung bei illegalem Bitcoin-Mining", *in* NStZ, 2016, p. 441, e Sentença do *Bundesgerichtshof* de 27/07/2017.

11 Cfr. EUROPOL, Internet Organised Crime Threat Assessment, 2018, pp. 4 e 19.

12 Cfr. JOHN MADDISON, Is Cryptojacking Replacing Ransomware as the Next Big Threat?, EUROPOL, Internet Organised Crime Threat Assessment, 2018, p. 19, e também em Internet Organised Crime Threat Assessment, 2019, p. 26, e MICHAEL NADEAU, What is cryptojacking? How to prevent, detect, and recover from it. Como refere MICHAEL NADEAU, o "furto" de ciclos de processamento enquanto a vítima visita um determinado *website* pode ser levado a cabo através da inserção de um *script* nesse *website* ou da "distribuição" de um anúncio para múltiplos *websites* e, desse modo, o "furto" não passa pela instalação de qualquer dado informático, apenas dependendo da permanência no *website* ou do correr do anúncio.

13 A *botnet* consiste numa rede de sistemas informáticos infetados por *bots* semelhantes. Os agentes do crime irão disseminar *malware* num grande número de sistemas informáticos com o objetivo de os transformar em *zumbis* ou *zombies* (também designados por *bots*), passando a executar, de forma automatizada e sem que o seu utilizador se aperceba, tarefas na Internet para fins de envio de *spam*, disseminação de vírus, de ataque a sistemas informáticos (incluindo ataques do tipo DDoS – inclusive para a ulterior prática de atos de extorsão – e de ciberterrorismo), de cometimento de fraudes ou de *Criptojacking*, etc.

14 Cfr. HEINE, "Bitcoins und Botnetze – Strafbarkeit und Vermögenabschöpfung bei illegalem Bitcoin-Mining", *in* NStZ, 2016, pp. 443 e ss., e Sentença do *Bundesgerichtshof* de 27/07/2017; aliás, num processo julgado nos Tribunais alemães, um criptomineiro criou uma *botnet* com 327.379 sistemas informáticos graças aos utilizadores terem instalado um *software* que, sob a aparência de um *software* para baixar ficheiros de música, continha também um Cavalo de Troia (cfr. Sentenças do *Bundesgerichtshof* de 21/07/2015 e 27/07/2017).

15 Assim, EUROPOL, Internet Organised Crime Threat Assessment, 2018, p. 19.

criminosos irão utilizar metodologias próprias de outras atividades próprias do cibercrime (*maxime* o *Phishing* e o *Ransomware*[16]), como sucedeu, por exemplo, com o *malware* "*Eternal Blue*", que fora utilizado no ataque de *Ransomware* "*WannaCry*"[17]. Uma forma de criar ou de expandir uma *botnet* pode passar pela utilização de um *malware* com capacidades de *worm*, que permitirá que o *malware* se expanda e autoinstale noutros sistemas informáticos pertencentes à mesma rede informática[18].

Nos casos em que é levado a cabo diretamente, o *Cryptojacking* requer, antes de mais, o acesso do minerador aos sistemas informáticos alheios que irão constituir a *botnet* como sistemas informáticos *zumbis* ou *zombies*, que passarão a ser comandados pelo sistema informático do agente do crime (*Central Command and Control Center*)[19]. Tal depende da instalação de um *malware*, que irá "furtar" ciclos de processamento da CPU para realizar as operações necessárias à mineração de criptomoedas.

As formas de instalação do *malware* poderão passar pelo envio à vítima ou a um seu colaborador (*v.g.*, o funcionário de uma empresa, de um organismo público ou de um banco) um *e-mail* falso, simulando ter sido enviado por uma pessoa conhecida da vítima ou do seu colaborador ou por uma entidade legítima (*v.g.*, uma instituição bancária, uma entidade policial, etc.), convidando-o(a) a baixar um dado ficheiro, abrir um anexo, clicar e abrir um *link*, etc. (incluindo campanhas massivas de *Spear Phishing*[20], utilizando o método "*spray and pray*"[21]) ou a aceder a um *website* falso e/ou

16 Cfr. MICHAEL NADEAU, What is cryptojacking? How to prevent, detect, and recover from it.
17 Cfr. JOHN MADDISON, Is Cryptojacking Replacing Ransomware as the Next Big Threat?.
18 Assim, MICHAEL NADEAU, What is cryptojacking? How to prevent, detect, and recover from it.
19 Cfr. JOHN MADDISON, Is Cryptojacking Replacing Ransomware as the Next Big Threat?, e EUROPOL, Internet Organised Crime Threat Assessment, 2018, p. 19.
20 O *Phishing* consiste na obtenção *online*, de forma fraudulenta, de dados pessoais (*v.g.*, credenciais de acesso a contas bancárias) para ulterior utilização maliciosa (*v.g.*, efetuar movimentos nas contas bancárias da vítima, aquisições de bens ou transferências para contas pertencentes ao agente do crime). Em regra, o *Phishing* inicia-se com o envio de um *e-mail*, aparentemente de uma fonte confiável, que encaminha o alvo para um *site* falso onde está o *malware* ou contém um ficheiro ou *link* que, sendo aberto, instala o *malware* no sistema informático, dando acesso a esse sistema e aos dados nele armazenados para ulterior utilização maliciosa.
Por seu turno, o *Spear Phishing* é uma forma de *Phishing* que se caracteriza por consistir num ciberataque que atinge um ou mais alvos específicos e determinados, em vez de ataques amplos e dispersos.
21 O método "*spray* and *pray*" consiste em disponibilizar ficheiros infetados para *download*, enviar (em regra massivamente) *e-mails* infetados, etc., esperando que alguém, desconhecendo que estão infetados e não possuindo um sistema informático suficientemente protegido, baixe os ficheiros infetados ou os destinatários dos *e-mails* atuem de acordo com o sugerido nesses *e-mails* (baixando um dado ficheiro, abrindo um anexo, clicando e abrindo um *link*, etc.) (cfr. JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal

infetado, o que, sendo feito, permite a instalação *sub-reptícia* de *malware*, que dará ao agente o acesso ao sistema e/ou aos dados, pela disponibilização de *software* infetado para *download* gratuito na Internet[22].

Em 2018 e 2019, a EUROPOL[23] previa que o *Ransomware* (que era a atividade de cibercrime mais frequente) viesse a ser ultrapassado pela mineração de criptomoedas com recurso ao *Cryptojacking* (como forma de aumentar a capacidade de computação) como a maior ameaça à cibersegurança, uma vez que se trata de uma atividade muito mais atrativa para os cibercriminosos, por exigir pouco ou nenhum envolvimento de vítimas, por ser menos "visível" para as vítimas (que podem nem se aperceber de que o seu sistema informático está a ser utilizado de forma abusiva por terceiros)[24], por ainda merecer pouca atenção das autoridades (dado que a mineração de criptomoedas, em si mesma, não é ilegal)[25] e por, tendo em conta os valores que as criptomoedas haviam atingido (especialmente o *Bitcoin*), a mineração de criptomoedas poder proporcionar lucros mais elevados do que o *Ransomware.*

Contudo, nos seus *Internet Organised Crime Threat Assessments* de 2020, 2021 e 2023, a EUROPOL já nem sequer faz qualquer referência ao *Cryptojacking*, continuando, pelo contrário, o *Ransomware* a ser a atividade criminosa mais frequente (embora apresentando novas características), acompanhada de outras atividades de

---

considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, p. 12).

22 Cfr. MICHAEL NADEAU, What is cryptojacking? How to prevent, detect, and recover from it.

23 EUROPOL, Internet Organised Crime Threat Assessment, 2018, p. 26, e também em Internet Organised Crime Threat Assessment, 2019, p. 26.

24 Ao ponto de os agentes do crime programarem o *malware* para nunca "consumir" mais do que uma determinada percentagem da CPU disponível ou não operar quando o utilizador esteja a usar o sistema informático (cfr. JOHN MADDISON, Is Cryptojacking Replacing Ransomware as the Next Big Threat?). Por exemplo, no caso *sub juditio* nas Sentenças do *Bundesgerichtshof* de 21/07/2015 e 27/07/2017, os agentes tinham programado o *malware* para a mineração só se iniciar após 120 segundos de inatividade nos sistemas informáticos *zumbis*, nunca ocorrendo enquanto o sistema estivesse a ser usado pelo seu utilizador.

No fundo, enquanto o *Ransomware* implica que a vítima se aperceba de que está a ser alvo de um ataque informático (desde logo, no momento em que lhe é exigido o pagamento do resgate ou mesmo antes, quando se apercebe de que o acesso aos dados foi bloqueado), no *Cryptojacking*, o agente do crime tudo fará para que a utilização ilícita do sistema informático alheio não seja detetada pela vítima.

Como referem MICHAEL NADEAU, What is cryptojacking? How to prevent, detect, and recover from it, e EUROPOL, Internet Organised Crime Threat Assessment, 2019, p. 54, o *Cryptojacking* é mais utilizado para minerar criptomoedas – como o Monero ou o Zcashh – cuja mineração requer menos capacidade computacional ("consumindo" menos capacidade de *hardware* e, por isso, as probabilidades de a vítima de aperceber são bastante menores) e não tanto o *Bitcoin*, cujo processamento é mais "pesado" e requer mais recursos de memória do computador *zumbi*.

25 Cfr. EUROPOL, Internet Organised Crime Threat Assessment, 2019, p. 26, e MICHAEL NADEAU, What is cryptojacking? How to prevent, detect, and recover from it.

criminalidade informática que já podem considerar-se "clássicas" (como o *Phishing* – que também apresenta novas características –, burlas praticadas através da Internet, criminalidade sexual *online* e ataques DDoS – com a particularidade de serem seguidos de atos de extorsão com vista ao pagamento de resgates como forma de os criminosos pararem com os ataques –) e de novas formas de cibercriminalidade como a disponibilização de *malware* e de outros meios digitais a cibercriminosos (*cybercrime-as-a-service, malware-as-a-service, bulletproof hosting*).

Contudo, tal não significa que não existam criminosos que continuam a levar a cabo o *Cryptojacking*, pois as cotações das criptomoedas mantêm-se elevadas.

Embora, diversamente do *Ransomware* e do *Phishing*, a mineração de criptomoedas não seja, em si mesma ilícita, levanta-se a questão da eventual ilicitude (inclusivamente penal, que é aquela de que nos ocupamos no âmbito do presente artigo) do *Cryptojacking* por via da utilização e acesso abusivos de/a sistemas informáticos e energia elétrica alheios, bem como da obtenção do acesso a esses mesmos sistemas informáticos. Assim, o objeto do presente artigo consiste em determinar quais os ilícitos criminais que poderão ser praticados pelo *Cryptojacker*.

De todo o modo, quanto à eventual relevância criminal da utilização abusiva de um sistema informático e do consumo abusivo de energia elétrica alheios, é de afastar *in limine* a subsunção de tais condutas ao crime de furto de uso (p. e p. pelo artigo 208.º do Código Penal), dado que, na nossa ordem jurídica, o furto de uso só é punido quando o objeto da ação seja um automóvel ou outro veículo motorizado, uma aeronave, um barco ou uma bicicleta.

IV. Furto de energia elétrica por via do consumo de energia derivado da utilização não autorizada de um sistema informático alheio?

A primeira possibilidade que poderá colocar-se, em abstrato, quanto à responsabilidade penal do agente do *Cyptojacking* é a subsunção da sua conduta – na parte em que incide sobre o consumo abusivo de energia elétrica – ao crime de furto simples, p. e p. pelo artigo 203.º, n.º 1, do Código Penal ou mesmo do crime de furto qualificado (nos termos do artigo 204.º, n.ºs 1 e 2, do Código Penal.

Nos termos do artigo 203.º, n.º 1, do Código Penal, «*Quem, com ilegítima intenção de apropriação para si ou para outra pessoa, subtrair coisa móvel ou animal alheios, é punido com pena de prisão até 3 anos ou com pena de multa*».

O crime de furto protege o património (em sentido amplo) na sua vertente propriedade, tutelando-se, não tanto o direito de propriedade tal como delimitado no Direito civil, mas sim a especial relação de facto sobre a coisa, o poder de facto sobre a coisa, ou seja, a detenção ou mera posse sobre a coisa, no sentido da disponibilidade material da coisa, da disponibilidade da fruição das utilidades da coisa com um mínimo de representação jurídica[26].

Além disso, o furto é um crime de resultado e de dano, porquanto, para se consumar, é necessário que se produza um evento espácio-temporalmente destacado da ação (resultado) e a efetiva lesão da propriedade de um terceiro (que consubstancia igualmente o resultado)[27].

Quanto ao tipo objetivo, são elementos objetivos do crime de furto simples:

a) a subtração de uma coisa;

b) a coisa subtraída ser móvel e alheia;

c) a coisa subtraída possuir um qualquer valor patrimonial (elemento implícito);

d) não se verificar nenhuma das circunstâncias referidas nos n.ºs 1 e 2 do artigo 204.º do Código Penal ou, verificando-se, o valor dos bens furtados ser inferior ao valor de 1 unidade de conta à data da prática dos factos.

Abstraindo do terceiro elemento objetivo e do valor da coisa e começando pela subtração, existe subtração sempre que a posse exercida pelo ofendido seja violada e a coisa seja integrada na esfera patrimonial do agente ou de um terceiro. No fundo, terá de existir uma eliminação do domínio de facto que outrem detinha sobre a coisa, fazendo entrar no domínio do facto do agente ou de um terceiro (que não o ofendido) as utilidades da coisa que anteriormente estavam no domínio de facto do ofendido, mesmo que esse desapossamento/apossamento não se concretize numa apreensão manual e não

26 Cfr. FARIA COSTA, "Art. 203º", *in* Comentário Conimbricense do Código Penal, II, pp. 30 e 32, e PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 883.
27 Cfr. PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 883.

implique o dispêndio de energias físicas pessoais nem a mudança da localização coisa, não sendo igualmente necessária a utilização da coisa pelo agente ou pelo terceiro beneficiário[28].

Quanto à natureza móvel da coisa, a noção de coisa para efeitos do Direito penal não se confunde com o conceito civilístico de coisa plasmado no artigo 202.º do Código Civil *(«tudo aquilo que pode ser objeto de relações jurídicas*»), sendo que, seguindo de perto as palavras de SIMAS SANTOS/LEAL-HENRIQUES[29], «*Coisa, para efeitos penais e particularmente no âmbito dos crimes de furto, é toda a substância em princípio corpórea, material, susceptível de apreensão, pertencente a alguém e que tenha um valor qualquer, mas juridicamente relevante*», incluindo-se as coisas fora do comércio (como bens do domínio público, bens ilícitos, obras de arte protegidas), coisas destacadas de bens imóveis (árvores, pedra, terra) e mesmo algumas coisas imóveis (como a água[30])[31].

No plano do Direito penal, devem ser consideradas coisas móveis todas as coisas (na aceção referida supra) que sejam passíveis de ser espacialmente deslocadas, ou seja, tudo aquilo que, num dado momento, esteja num determinado local, mas, num momento seguinte, possa passar a estar noutro local[32].

No que tange ao caráter de coisa móvel e à corporeidade da coisa, com pertinência para o presente artigo, suscita-se a questão de saber se a energia elétrica (independentemente do modo como é produzida) deve ser considerada coisa móvel para efeitos do crime de furto, sendo que, no plano do Direito civil, como nos dá conta MENEZES CORDEIRO[33], a energia é, com exceção do Direito alemão, considerada uma coisa móvel na generalidade das ordens jurídicas. Entre nós, a Doutrina penal maioritária e a Jurisprudência vêm considerando a energia elétrica como passível de

---

28 Neste sentido FARIA COSTA, "Art. 203º", *in* Comentário Conimbricense do Código Penal, II, pp. 43-44, SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 750, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, pp. 886-887, e MAIA GONÇALVES, Código Penal Português Anotado e Comentado, 12ª Edição, pp. 615-616.
29 SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 751.
30 Nos termos do artigo 204.º, n.º 1, al. b), do Código Civil, as águas são um coisa imóvel.
31 No mesmo sentido, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, pp. 883-884.
32 Cfr. FARIA COSTA, "Art. 203º", *in* Comentário Conimbricense do Código Penal, II, pp. 40-41, e PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 884.
33 MENEZES CORDEIRO, Tratado de Direito Civil Português, I, Parte Geral, Tomo II, Coisas, 2.ª Edição, p. 141.

constituir uma coisa (móvel) para efeitos de crime de furto[34], punindo como furto condutas como, por exemplo:

a) na sequência de o fornecimento de energia elétrica à sua habitação ter sido suspenso por falta de pagamento de anteriores consumos, o agente, pelos seus próprios meios e contra a vontade do fornecedor, continua a retirar energia da rede[35]; ou

b) o agente proceder à abertura de um furo na carcaça instalada pelo fornecedor na sua residência, por contrato de fornecimento de energia elétrica, de forma a introduzir, através do mesmo, um corpo estranho ao funcionamento do aparelho para fazer parar o disco metálico do referido contador, impedindo a contagem das quantidades de energia elétrica consumida e, desse modo, em seu proveito, foge ao controlo efetivo e real da empresa fornecedora de energia elétrica e prejudica-a na medida em que os gastos contados são inferiores aos realmente realizados[36].

Quanto à natureza alheia da coisa, a coisa subtraída terá de ter um dono. Daí que não sejam coisas alheias as coisas sem dono (*res nullius*), as coisas abandonadas pelo seu dono (*res dereclicta*) ou as coisas insuscetíveis de ocupação na sua totalidade (*res commune omnium*)[37]; diversamente, os bens em situação de compropriedade, composse ou comunhão em mão própria (*v.g.*, bens comuns do casal e de entes jurídicos sem personalidade jurídica) de que o agente seja contitular constituem coisas alheias para efeitos do crime de furto, contanto que sejam divisíveis e o agente se aproprie de uma

---

34 Cfr. FARIA COSTA, "Art. 203º", *in* Comentário Conimbricense do Código Penal, II, pp. 39-40, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 884, SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 752, MAIA GONÇALVES, Código Penal Português Anotado e Comentado, 12ª Edição, p. 616, e Acórdãos da Relação do Porto de 23/05/1990, 29/04/2009, 29/09/2010 e 24/01/2018, da Relação de Guimarães de 20/02/2018 e 13/01/2020 e da Relação de Évora de 12/09/2017, 10/03/2020, 22/09/2020 e 23/02/2021; contra, FIGUEIREDO DIAS, Direito Penal, Parte Geral, I, 3.ª Edição, p. 222, e TAIPA DE CARVALHO, Direito Penal, Parte Geral, 3.ª Edição, p. 178, por entenderem que, pela falta do corporeidade, a consideração da energia elétrica como coisa móvel para efeitos da punição por crime de furto viola o princípio da proibição do recurso à analogia *in malam partem*.

35 Cfr. Acórdãos da Relação do Porto de 29/04/2009 e 29/09/2010.

36 Cfr. Acórdão da Relação do Porto de 23/05/1990.

37 Cfr. FARIA COSTA, "Art. 203º", *in* Comentário Conimbricense do Código Penal, II, p. 41, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 885, MAIA GONÇALVES, Código Penal Português Anotado e Comentado, 12ª Edição, p. 617, e SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 752.

quantidade superior ao seu quinhão/quota ideal[38] (caso contrário, o agente que se aproprie de um bem indivisível de que seja parcialmente proprietário sem exceder o correspondente ao seu quinhão/quota ideal não comete qualquer crime[39], sem prejuízo de eventual responsabilidade civil).

As coisas perdidas (*res depertida*) são alheias para efeitos do crime de acessão de coisa achada, mas não para o crime de furto[40].

A apropriação, por um sócio, de bens pertencentes à pessoa coletiva de que é sócio (e, eventualmente, legal representante) é passível de constituir um crime de furto[41] (ou, nos casos subsumíveis ao artigo 205.º do Código Penal, um crime de abuso de confiança).

De referir ainda que, tratando-se de um crime de resultado, de acordo com a teoria da adequação, a conduta adotada pelo agente terá de ser adequada a produzir o resultado, que consiste na lesão do direito de propriedade de um terceiro.

Passando ao tipo subjetivo, o crime de furto simples só é punível a título de dolo (cfr. artigos 13.º e 203.º, ambos do Código Penal), bastando o dolo eventual. Todavia, o crime de furto é um "crime de intenção" (*Absichtsdelikt*) ou de "resultado cortado"[42], uma vez que o legislador exige, além do dolo genérico quanto aos elementos objetivos do tipo, que o agente atue com uma intenção, um *animus* (que nada tem a ver com o dolo relativo aos elementos objetivos do tipo), que consiste na "ilegítima intenção de apropriação para si ou para outra pessoa".

A "ilegítima intenção de apropriação para si ou para outra pessoa" consiste em o agente, além de saber que a coisa subtraída é móvel e alheia e atuar com uma vontade dirigida a adquirir um poder de facto sobre essa coisa, fazendo cessar o correspondente

---

38 Cfr. FARIA COSTA, "Art. 203º", *in* Comentário Conimbricense do Código Penal, II, p. 43, e SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 753; contra, não operando a distinção entre bens divisíveis e bens indivisíveis, MAIA GONÇALVES, Código Penal Português Anotado e Comentado, 12ª Edição, p. 618.
39 Cfr. FARIA COSTA, "Art. 203º", *in* Comentário Conimbricense do Código Penal, II, p. 43, e SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 753.
40 Cfr. PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 885, FARIA COSTA, "Art. 203º", *in* Comentário Conimbricense do Código Penal, II, p. 42, MAIA GONÇALVES, Código Penal Português Anotado e Comentado, 12ª Edição, p. 617, e SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 752.
41 Assim, MAIA GONÇALVES, Código Penal Português Anotado e Comentado, 12ª Edição, p. 618.
42 Sobre o conceito de crime de "resultado cortado", *vide* DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, 2.ª Edição, p. 264.

poder de facto da vítima sobre essa mesma coisa, agir com a intenção de se apropriar da coisa, seja para si ou para outra pessoa (que terá de ser diversa do dono da coisa subtraída), ou seja, o agente terá de agir com o dolo genérico quanto à subtração de coisa móvel e alheia – *i.e.*, quanto à desapropriação – e com intenção ilegítima de apropriação quanto à apropriação[43]. Ademais, os motivos que presidem a essa apropriação terão de ser injustificados, ilegítimos à luz da ordem jurídica[44], o que não se confunde com a exigência da não verificação de causas de justificação.

Revertendo para o âmbito do presente artigo, o que aqui está em causa quanto à utilização ilegítima de energia elétrica, que o proprietário ou utilizador legítimo do sistema informático *zombie* terá de custear (apesar de não ser ele quem verdadeiramente utiliza essa energia), não é o "desvio" da mesma para o agente do crime, mas apenas o consumo (obviamente) ilegítimo e não autorizado de energia elétrica alheia como consequência necessária da utilização abusiva (por não autorizada) do sistema informático alheio.

Deste modo, tendo em conta o que referimos supra quanto à subtração e à ilegítima intenção de apropriação, não existe uma subtração nos termos referidos e, ainda que existisse, jamais poderia dizer-se que o agente atua com ilegítima intenção de apropriação da energia elétrica, visto que a sua intenção prende-se, apenas e só, com a utilização de um sistema informático alheio para minerar criptomoedas. E, nessa conformidade, o agente do *Cryptojacking* não comete o crime de furto quanto à energia elétrica cujo consumo a utilização abusiva do sistema informático comporta[45].

---

43 Como referem FARIA COSTA, "Art. 203º", *in* Comentário Conimbricense do Código Penal, II, p. 46, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 887, e SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 754.

44 Cfr. FARIA COSTA, "Art. 203º", *in* Comentário Conimbricense do Código Penal, II, p. 33, e PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 887.

45 Cfr., embora à luz do Direito alemão [tendo em conta o tipo objetivo do crime de furto de energia elétrica, p. e p. pelo §248c StGB (*Strafgesetzbuch*), que exige que a energia seja subtraída de uma estrutura de produção, transformação ou distribuição ou de uma instalação elétrica)], HEINE, "Bitcoins und Botnetze – Strafbarkeit und Vermögenabschöpfung bei illegalem Bitcoin-Mining", *in* NStZ, 2016, p. 442, e HALIME EREZ, "Das Schürfen von Bitcoins unter heimlicher Nutzung fremder Computer", *in* KriPoZ, 2020, p. 9.

V. Burla informática através da utilização não autorizada e sem qualquer pagamento do sistema informático alheio?

Uma segunda possibilidade que poderá colocar-se, em abstrato, quanto à responsabilidade penal do agente do *Cryptojacking* é a subsunção da sua conduta – na parte em que consiste na utilização não autorizada e sem qualquer pagamento do sistema informático alheio – ao crime de burla informática e nas comunicações.

No artigo 221.º do Código Penal pune-se a burla informática (n.º 1) e nas comunicações (n.º 2). Dispõe este artigo:

«*1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.*

2 - A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos eletrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.

(...)

5 - Se o prejuízo for:

a) De valor elevado, o agente é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias;

b) De valor consideravelmente elevado, o agente é punido com pena de prisão de 2 a 8 anos.

(...)».

O crime de burla informática e nas comunicações protege o património[46], não se exigindo que seja provocado um engano na vítima como no crime de burla (aqui, o engano é criado através da manipulação de um dispositivo informático ou eletrónico ou programa ou do tratamento de dados), e estabelecendo-se a conexão com a informática pelo modo como a conduta é levada a cabo, *i.e.*, interferindo no resultado do tratamento de dados mediante a estruturação incorreta de programa informático, a utilização incorreta ou incompleta de dados, a utilização de dados sem autorização ou a intervenção, por qualquer outro modo, não autorizada no processamento (no caso da burla informática), bem como pela utilização de programas, dispositivos eletrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou a exploração de serviços de telecomunicações (no caso da burla nas comunicações)[47].

Além disso, a burla informática e nas comunicações é um crime de resultado e de dano, porquanto, para se consumar, é necessário que se produza um evento espácio-temporalmente destacado da ação (resultado) e ocorra uma efetiva causação de um prejuízo no património de um terceiro[48], sendo, ainda, um crime de execução vinculada, posto que, sem prejuízo das cláusulas gerais constantes dos n.ºs 1 e 2 do artigo 221.º do

---

46 Cfr. A.M. ALMEIDA COSTA, "Art. 221º", *in* Comentário Conimbricense do Código Penal, II, pp. 329 e 333, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 955, JOEL TIMÓTEO PEREIRA, Compêndio Jurídico da Sociedade da Informação, p. 520, PEDRO VERDELHO, "A Convenção sobre o Cibercrime do Conselho da Europa – Repercussões na Lei portuguesa", *in* Direito da Sociedade da Informação, VI, p. 263, e Acórdãos do Supremo Tribunal de Justiça de 20/09/2006, 05/11/2008, 20/10/2010 e 12/09/2012.

Discordamos do Acórdão do Supremo Tribunal de Justiça de 01/04/2020 quando considera que o crime de burla informática é um crime composto ou complexo, que incorpora um crime contra o património e um crime de acesso ilícito a sistema informático, na medida em que confunde o bem jurídico tutelado com o modo de atentar contra o bem jurídico. E também não podemos concordar com os Acórdãos do Supremo Tribunal de Justiça de 10/01/2001 e 14/07/2004 e da Relação do Porto de 03/02/2016, quando aí se entende que o crime de burla informática protege não só o património, mas também a fiabilidade dos dados e a sua proteção, na medida em que a fiabilidade dos dados informáticos apenas é protegida de forma reflexa (no mesmo sentido, Acórdão do Supremo Tribunal de Justiça de 20/10/2010), posto que o bem jurídico tutelado em primeira linha é o património, tendo em conta, não só a inserção sistemática da norma incriminadora, mas também a ênfase que o legislador coloca na dicotomia prejuízo patrimonial/enriquecimento ilegítimo na descrição do tipo objetivo do crime.

47 Cfr. GARCIA MARQUES/LOURENÇO MARTINS, Direito da Informática, 2.ª Edição, p. 677, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 955, e Acórdãos do Supremo Tribunal de Justiça de 12/07/2006, 20/09/2006, 05/11/2008 e 12/09/2012 e da Relação do Porto de 03/2/2016

48 Cfr. A.M. ALMEIDA COSTA, "Art. 221º", *in* Comentário Conimbricense do Código Penal, II, pp. 329 e 333, SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 1010, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 955, JOEL TIMÓTEO PEREIRA, Compêndio Jurídico da Sociedade da Informação, p. 520, e Acórdãos do Supremo Tribunal de Justiça de 20/09/2006 e 05/11/2008 e da Relação do Porto de 03/02/2016.

Código Penal ("intervenção por qualquer outro modo não autorizada no processamento" e "usando (…) outros meios que, separadamente ou em conjunto (…)", respetivamente) e de as enumerações deles constantes serem meramente exemplificativas, exige-se a criação de um engano através da manipulação de um dispositivo informático ou eletrónico ou programa ou do tratamento de dados[49], ou seja, o sistema informático é "enganado" pelo agente do crime[50].

De todo o modo, para efeitos do presente artigo interessa-nos apenas a burla informática (p. e p. pelo artigo 221.º, n.º 1, do Código Penal).

Quanto ao tipo objetivo, são elementos objetivos do crime de burla informática simples:

a) A causação de um prejuízo patrimonial;

b) Interferência no resultado do tratamento de dados através da estruturação incorreta de programa informático, da utilização incorreta ou incompleta de dados, da utilização de dados sem autorização ou da intervenção, por qualquer outro modo, não autorizada no processamento;

c) O prejuízo causado não ser de valor elevado nem consideravelmente elevado[51.]

Abstraindo do terceiro elemento objetivo (que apenas tem a ver com o valor do prejuízo causado), no que tange ao primeiro elemento objetivo, terá de ocorrer um prejuízo para a vítima (que terá de ser uma pessoa diversa do agente ou do terceiro "beneficiário), devendo a existência, ou não, desse prejuízo ser aferida através da aplicação de critérios objetivos de natureza económica à concreta situação patrimonial da vítima, concluindo-se pela existência de um dano sempre que ocorra uma diminuição do valor económico por referência à posição em que a vítima se encontraria se o agente

49 Neste sentido, A.M. ALMEIDA COSTA, "Art. 221º", *in* Comentário Conimbricense do Código Penal, II, pp. 329 e 333, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 955, e Acórdãos do Supremo Tribunal de Justiça de 12/07/2006, 20/09/2006 e 05/11/2008.
50 Cfr. Acórdão do Supremo Tribunal de Justiça de 01/04/2020.
51 Ou seja, o prejuízo terá de ser inferior ou igual ao valor correspondente a 50 unidades de conta avaliadas no momento da prática do facto, ou seja, atualmente, o prejuízo terá de ser igual ou inferior a €5.100,00.

não tivesse adotado a conduta que adotou[52]. Tratando-se de um crime de resultado, de acordo com a teoria da adequação, a conduta adotada pelo agente terá de ser adequada a produzir o resultado, que consiste na lesão do direito de propriedade de um terceiro. Todavia, diversamente do que sucede com o crime de burla (p. e p. pelos artigos 217.º e ss. do Código Penal), no crime de burla informática não se exige um duplo nexo de imputação objetiva[53], concretizando-se o crime «*num atentado direto ao património, ou seja, num processo executivo que não contempla, de permeio, a intervenção de outra pessoa e cuja única peculiaridade reside no facto de a ofensa ao bem jurídico se observar através da utilização de meios informáticos*»[54].

No que tange ao segundo elemento objetivo, terá de ocorrer uma interferência no resultado do tratamento de dados, que consiste em interferir na disposição patrimonial através da utilização do sistema informático (executando diretamente ou criando as condições para que o sistema execute automaticamente)[55], devendo essa interferência ocorrer mediante uma destas formas:

a) Estruturação incorreta de programa informático, que consiste na modificação do programa de molde a que as suas instruções sejam diferentes das inicialmente concebidas pelo proprietário (*v.g.*, introduzindo novas instruções ou funções no programa, eliminando ou alterando o seu processo de funcionamento ou modificando os sistemas de controlo do próprio

---

52 Cfr. A.M. ALMEIDA COSTA, "Art. 217º", *in* Comentário Conimbricense do Código Penal, II, pp. 283-284.

53 No crime de burla exige-se a verificação de um duplo nexo de causalidade (1) entre a conduta enganosa do agente e a prática, pelo burlado, de atos tendentes à diminuição do património e (2), subsequentemente, entre os atos tendentes à diminuição do património praticados e a efetiva verificação do prejuízo patrimonial, aferido à luz da teoria da adequação (cfr. A.M. ALMEIDA COSTA, "Art. 217º", *in* Comentário Conimbricense do Código Penal, II, pp. 293 e ss., e PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 944). Contudo, o crime de burla também poderá ser cometido através de meios informáticos sem que isso "converta" a conduta numa burla informática. Na verdade, tem-se assistido ultimamente à prática massiva de crimes de burla através de meios informáticos ao nível da venda de produtos *online*, arrendamento de imóveis, investimentos em criptomoedas, etc.

54 A.M. ALMEIDA COSTA, "Art. 221º", *in* Comentário Conimbricense do Código Penal, II, p. 330.

55 Assim, SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 1011, e PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 955.

Nos casos em que o agente forneça os dados falsos a quem tenha a incumbência de os introduzir no sistema informático, haverá que distinguir: se essa pessoa for a pessoa enganada (agindo com base em informação manipulada pelo agente), estaremos perante um crime de burla e não de burla informática (cfr. PAULO PINTO DE ALBUQUERQUE, *Ibidem*), mas já estaremos perante um crime de burla informática se essa pessoa não for a pessoa enganada (cfr. SIMAS SANTOS/LEAL-HENRIQUES, *Ibidem*), porquanto o prejuízo pode ser causado a uma pessoa diversa do proprietário ou utilizador do sistema e/ou dos programas informáticos (cfr. PAULO PINTO DE ALBUQUERQUE, *Ibidem*).

programa), subvertendo o funcionamento do programa (que funcionará de uma forma contrária à finalidade para que foi criado) e, consequentemente, os resultados desse funcionamento, que serão contrários à finalidade originária do programa [56]; essa estruturação incorreta pode ser conseguida mediante a manipulação de um programa já existente ou a criação de um novo programa com essa finalidade[57];

b) Uso incorreto ou incompleto de dados, que consiste na sua utilização de forma incorreta ou na introdução incorreta ou incompleta de dados verdadeiros ou mesmo na introdução de dados falsos[58];

c) Aproveitamento de dados sem autorização, que consiste na utilização não autorizada pelo legítimo titular ou para além da autorização concedida, de dados informáticos, mas sem que a integridade dos dados seja atingida (*v.g.*, utilização de cartões de crédito ou de débito nas caixas automáticas ou em terminais automáticos de pagamento, levantamento ou transferência de fundos de contas bancárias ou realização de pagamentos com esses fundos sem autorização do respetivo titular[59])[60]; ou

d) Intervenção, por qualquer outro modo, não autorizada no processamento (onde se inclui a interferência no processamento mecânico do sistema informático, como sucede com a manipulação do *hardware*[61]), que constitui uma cláusula geral criada pelo legislador, de modo a que qualquer intervenção não autorizada no processamento de dados (que até poderá ser tecnicamente possível apenas no futuro) de que resulte um prejuízo patrimonial para um terceiro e que seja levada a cabo com a intenção de o agente obter para si ou para um terceiro, um enriquecimento ilegítimo possa

56 Cfr. SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 1011, e PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 956.
57 Cfr. PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 956.
58 No mesmo sentido, SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 1011, e PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 956.
59 Como sucede habitualmente nos casos de *Phishing*.
60 Cfr. SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 1011, e PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 956.
61 Cfr. PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 5.ª Edição, p. 956.

ser subsumida ao artigo 221.º, n.º 1, do Código Penal, a fim de obstar a lacunas de punibilidade[62].

Passando ao tipo subjetivo, o crime de burla informática simples só é punível a título de dolo (cfr. artigos 13.º e 221.º, ambos do Código Penal), bastando o dolo eventual. Todavia, o crime de burla informática é um "crime de intenção" (*Absichtsdelikt*) ou de "resultado cortado" [63], uma vez que que o legislador exige, além do dolo genérico quanto aos elementos objetivos do tipo, que o agente atue com uma intenção, um *animus* (que nada tem a ver com o dolo relativo aos elementos objetivos do tipo), que consiste na "intenção de obter para si ou para terceiro enriquecimento ilegítimo".

A "intenção de obter para si ou para terceiro enriquecimento ilegítimo" consiste em o agente, além de saber que está a causar um prejuízo patrimonial a um terceiro através do "engano" do sistema informático por via da manipulação do tratamento/uso abusivo e/ou deliberadamente incorreto ou incompleto de dados ou programas informáticos e atuar com uma vontade orientada nesse sentido, agir com a intenção de obter um enriquecimento patrimonial para si para outra pessoa (que terá de ser diversa do lesado),ou seja, o agente terá de agir com o dolo genérico quanto à causação do prejuízo através de uma das formas referidas e com intenção ilegítima de enriquecimento quanto à obtenção desse enriquecimento. Esse enriquecimento pode consistir no aumento patrimonial dos bens do agente ou do terceiro beneficiário ou na não diminuição patrimonial dos bens do agente ou do terceiro beneficiário (*v.g.*, através da extinção de uma dívida que tinha para com um terceiro credor)[64], sendo esse enriquecimento aferido através da aplicação de critérios objetivos de natureza económica à concreta situação patrimonial do agente ou do terceiro "beneficiário", concluindo-se pela existência de um enriquecimento sempre que ocorra um aumento ou uma não diminuição do valor económico por referência à posição em que agente ou o

62 No mesmo sentido, SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 1011, e A.M. ALMEIDA COSTA, "Art. 221º", *in* Comentário Conimbricense do Código Penal, II, p. 329.
63 Sobre o conceito de crime de "resultado cortado", *vide* DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, 2.ª Edição, p. 264.
64 No mesmo sentido, SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 931.

terceiro "beneficiário" se encontrariam se o agente não tivesse adotado a conduta que adotou[65].

Tal enriquecimento terá de ser igualmente ilegítimo, consistindo essa ilegitimidade na não correspondência – objetiva e/ou subjetivamente – do aumento patrimonial dos bens a qualquer direito ou interesse legalmente protegido[66] ou na não realização de uma prestação juridicamente devida.

Revertendo para o âmbito do presente artigo, está em causa a manipulação do funcionamento dos dados do sistema (dado que o *malware* instala-se no editor de registo do sistema operativo do sistema informático, influenciando o resultado do seu funcionamento) de que resulta um prejuízo económico para o utilizador do sistema informático *zumbi* (consubstanciado no consumo adicional de energia elétrica que a utilização abusiva do sistema pelo agente acarreta e que será pago pelo utilizador do sistema) e, concomitantemente, a obtenção de um enriquecimento do agente (por via da poupança no pagamento de energia elétrica e na aquisição de material informático que seriam necessários para o aumento da capacidade mineradora que é obtido por via do *Cryptojacking*).

Deste modo, consideramos que o agente de *Cryptojacking* comete, com a sua conduta, o crime de burla informática, p. e p. pelo artigo 221.º, n.º 1, do Código Penal[67].

VI. Falsidade informática

Como referimos, nos casos em que é levado a cabo diretamente, o *Cryptojacking* requer, antes de mais, o acesso do minerador aos sistemas informáticos alheios que irão constituir a *botnet* como sistemas informáticos *zumbis* ou *zombies*, dependendo esse acesso da instalação de *malware*, que irá "furtar" ciclos de processamento da CPU para realizar as operações necessárias à mineração de criptomoedas.

---

65 Cfr. A.M. ALMEIDA COSTA, "Art. 217º", *in* Comentário Conimbricense do Código Penal, II, pp. 284-285.
66 Cfr. SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, III, 4.ª Edição, p. 931.
67 Cfr., embora à luz do Direito alemão, HALIME EREZ, "Das Schürfen von Bitcoins unter heimlicher Nutzung fremder Computer", *in* KriPoZ, 2020, p. 12; contra, HEINE, "Bitcoins und Botnetze – Strafbarkeit und Vermögenabschöpfung bei illegalem Bitcoin-Mining", *in* NStZ, 2016, pp. 442-443, e Sentença do *Bundesgerichtshof* de 27/07/2017.

E, como também referimos, as formas de instalação do *malware* poderão passar pelo envio à vítima ou a um seu colaborador (*v.g.*, o funcionário de uma empresa, de um organismo público ou de um banco), um *e-mail* falso, simulando ter sido enviado por uma pessoa conhecida da vítima ou do seu colaborador ou por uma entidade legítima (*v.g.*, uma instituição bancária, uma entidade policial, etc.), convidando-o(a) a baixar um dado ficheiro, abrir um anexo, clicar e abrir um *link*, etc. (incluindo campanhas massivas de *Spear Phishing*, utilizando o método "*spray and pray*") ou a aceder a um *website* falso e/ou infetado, o que, sendo feito, permite a instalação *sub-reptícia* de *malware*, que dará ao agente o acesso ao sistema e/ou aos dados, pela disponibilização de *software* infetado para *download* gratuito na Internet.

O envio de *e-mail* falso simulando ter sido enviado por uma pessoa conhecida da vítima ou por uma entidade legítima com a finalidade de, por ação de quem recebe o *e-mail*, ser instalado *malware*, que permitirá ao agente aceder ao sistema informático-alvo, configura a prática de um crime de falsidade informática, p. e p. pelo artigo 3.º da Lei n.º 109/2009, nos termos do qual:

«*1 - Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.*

2 - Quando as ações descritas no número anterior incidirem sobre os dados registados, incorporados ou respeitantes a qualquer dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.

3 - Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objeto dos atos referidos no n.º 1 ou dispositivo no qual se encontrem registados, incorporados ou ao qual respeitem os dados objeto dos atos referidos no número anterior, é punido com as penas previstas num e noutro número, respetivamente.

4 - Quem produzir, adquirir, importar, distribuir, vender ou detiver qualquer dispositivo, programa ou outros dados informáticos destinados à prática das ações previstas no n.º 2, é punido com pena de prisão de 1 a 5 anos.

5 - Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.».

A essência do crime de falsidade informática reside na manipulação dos dados inseridos num sistema informático ou do seu tratamento, de que resultará a criação de documentos ou dados falsos, lesando a segurança e a fiabilidade dos documentos no tráfico jurídico-probatório (que é o bem jurídico tutelado por esta incriminação)[68]; esta incriminação visa equiparar, no plano do Direito penal, a adulteração de documentos eletrónicos à adulteração de documentos na aceção da alínea a) do artigo 255.º do Código Penal no âmbito do crime de falsificação de documento, p. e p. pelo artigo 256.º do Código Penal [69].

Quanto ao tipo objetivo do crime de falsidade informática simples, encontramos cinco modalidades de conduta típica no artigo 3.º, n.ºs 1 a 4, da Lei n.º 109/2009, de 15 de setembro[70]:

a) Introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos (n.º 1);

b) Introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados,

---

68 Cfr. FARIA COSTA, "Algumas reflexões sobre o estatuto dogmático do chamado "Direito penal informático"", *in* Direito Penal da Comunicação, p. 109, e DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 42.

Todavia, discute-se, na Doutrina e na Jurisprudência, qual é o bem jurídico tutelado pelo crime de falsidade informática (cfr. DUARTE RODRIGUES NUNES, *Idem*, pp. 45 e ss.).

69 Cfr. PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, pp. 505-506, e DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 42.

70 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 51 e ss. (com maiores detalhes e referências doutrinais e jurisprudenciais). O que referimos na obra citada deverá ser atualizado em face das alterações introduzidas pela Lei n.º 79/2021, de 24 de novembro, no art. 3.º da Lei n.º 109/2009, estando atualmente em vias de publicação uma 2.ª Edição desta nossa obra, que já contempla as alterações introduzidas pela Lei n.º 79/2021 na Lei n.º 109/2009.

No artigo 3.º, n.º 5, da Lei n.º 109/2009 incrimina-se o crime de falsidade informática agravado, consistindo a circunstância modificativa agravante na qualidade de funcionário do agente (*vide*, a este respeito, DUARTE RODRIGUES NUNES, *Idem*, pp. 74-75).

produzindo dados ou documentos não genuínos, sempre que os dados que sejam alvo dessa manipulação estejam registados ou incorporados em dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado (n.º 2);

c) Usar documento produzido a partir de dados informáticos que foram objeto de introdução, modificação, apagamento ou supressão ou cujo tratamento informático foi alvo de interferência por qualquer outra forma (n.º 3, 1.ª parte);

d) Usar documento produzido a partir de dados informáticos registados ou incorporados em dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado e que foram objeto de introdução, modificação, apagamento ou supressão ou cujo tratamento informático foi alvo de interferência por qualquer outra forma (n.º 3, 2.ª parte);

e) Produzir, adquirir, importar, distribuir, vender ou detiver qualquer dispositivo, programa ou outros dados informáticos destinados a aceder a sistema de comunicações ou a serviço de acesso condicionado (n.º 4).

Tendo em conta o objeto do presente estudo, está em causa a primeira conduta típica, cujos elementos objetivos são introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, devendo a expressão "dados informáticos" ser entendida na aceção do artigo 2.º, al. b), da Lei n.º 109/2009. Esta modalidade de conduta típica configura um crime de resultado (pois da atuação do agente resulta uma modificação do mundo exterior, *in casu*, a produção de dados ou de documentos não genuínos) e de perigo abstrato (uma vez que a Lei não exige uma lesão efetiva da segurança e da fiabilidade dos documentos eletrónicos no tráfico jurídico-probatório nem que esse bem jurídico seja efetivamente colocado em perigo)[71].

Quanto aos atos de "*introduzir, modificar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados*":

71 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 48 e ss.

a) Introduzir consiste em inserir dados informáticos num sistema informático ou num suporte autónomo;

b) Modificar consiste em alterar os dados informáticos armazenados/instalados num sistema informático ou num suporte autónomo;

c) Apagar consiste na eliminação de dados que se encontrem num sistema informático;

d) Suprimir consiste em reter, ocultar, tornar temporariamente indisponíveis dados que aí se encontrem; e

e) Interferir consiste em influenciar o modo de tratamento informático de dados, a fim de esse tratamento não ocorrer do modo como, sem a atuação do agente, ocorreria. Dado que a introdução, modificação, apagamento ou supressão de dados informáticos são formas de interferência no tratamento automático desses dados, a referência da Lei a "ou por qualquer outra forma interferir num tratamento informático de dados" significa que o legislador quis criar uma cláusula geral, de modo a que toda e qualquer interferência (que até poderá ser tecnicamente possível apenas no futuro) relativamente ao tratamento de dados por um sistema informático caiba nesta norma incriminatória, a fim de obstar a lacunas de punibilidade[72].

No que tange ao tratamento de dados informáticos, a Lei n.º 109/2009 não possui qualquer conceito, pelo que podemos socorrer-nos do Relatório Explicativo da Convenção sobre o Cibercrime, onde se refere que «*a expressão "tratamento de dados" significa que os dados no sistema informático são operados através da execução de um programa de computador. Um "programa de computador" é um conjunto de instruções passíveis de serem executadas pelo computador para obter o resultado*». Assim, o agente vai influenciar essas operações com a finalidade de que elas sejam executadas de modo diverso daquele como seriam executadas sem essa atuação do agente[73].

O legislador exige também que, por via da interferência no tratamento automático de dados informáticos, sejam produzidos dados ou documentos não genuínos. E, tendo em conta o bem jurídico protegido por esta incriminação e o dolo específico "intenção

72 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 52-53.
73 Assim, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 53.

de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes", esses dados ou documentos terão de ser suscetíveis de servir como meio de prova[74].

O crime de falsidade informática não está limitado à manipulação de dados informáticos (ou do seu tratamento) alheios, pelo que, se o agente manipular os dados ou o seu tratamento no âmbito de um programa ou de um sistema informático seus, desde que se verifiquem os demais elementos objetivos e subjetivos do tipo, comete o crime de falsidade informática[75].

Dado que, como vimos, esta modalidade de conduta típica configura um crime de resultado, de acordo com a teoria da adequação, o ato concretamente adotado pelo agente terá de ser apto a manipular os dados informáticos ou a interferir no seu tratamento[76].

Quanto ao tipo subjetivo, o crime de falsidade informática apenas poderá ser cometido com dolo (cfr. artigo 3.º da Lei n.º 109/2009, conjugado com o artigo 13.º do Código Penal), bastando que o agente atue com dolo eventual.

No entanto, à exceção da conduta prevista no n.º 1 do artigo 3.º da Lei 109/2009, o legislador exige, para além do dolo relativamente aos elementos objetivos do tipo, um dolo específico, que consiste na intenção de que os dados ou documentos não genuínos sejam considerados ou utilizados para finalidades juridicamente relevantes e, desse modo, causar engano nas relações jurídicas.

Apesar da redação da Lei, consideramos que se trata de "duas intenções" que se podem resumir a apenas "uma intenção única"[77], sendo certo, que, apesar de surgirem separadas, uma delas – a intenção de causar engano nas relações jurídicas – refere-se à

---

74 Acerca desta exigência, *vide* DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 53.
75 Cfr. OLIVEIRA ASCENSÃO, "Criminalidade informática", *in* Direito da Sociedade da Informação, II, p. 222, e DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 56.
76 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 56.
77 No mesmo sentido, falando numa redundância nos elementos subjetivos do tipo legal, PEDRO DIAS VENÂNCIO, Lei do Cibercrime Anotada e Comentada, p. 39, e também em Lições de Direito do Cibercrime, p. 81 (nota 107); contra, exigindo um duplo dolo, no sentido, de, num primeiro momento, em termos lógicos, o agente do crime estar imbuído do intuito de provocar engano nas relações jurídicas e, subsequentemente, ter a intenção de que os documentos digitais sejam considerados ou utilizados para finalidades juridicamente relevantes, como se fossem verdadeiros, PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, p. 506 (nota 5) e, se bem entendemos o raciocínio subjacente ao aresto, Acórdão da RP de 15/02/2023.

conduta de manipulação dos dados ou do seu tratamento e a outra – a intenção de que os documentos ou dados não genuínos sejam considerados ou utilizados para finalidades juridicamente relevantes – refere-se ao resultado dessa manipulação.

Daí que essa (aparentemente) dupla intenção deva ser lida no sentido de o legislador exigir que o agente atue com a intenção de que os documentos ou dados não genuínos sejam considerados ou utilizados para finalidades juridicamente relevantes, surgindo a intenção de causar engano nas relações jurídicas, pela natureza das coisas, como a consequência necessária da consideração/utilização dos documentos ou dados não genuínos para finalidades juridicamente relevantes. Na verdade, a única consequência consideração/utilização dos documentos ou dados não genuínos para finalidades juridicamente relevantes é a causação de engano nas relações jurídicas, sendo que a finalidade de causar engano nas relações jurídicas estará muitas vezes associada ao prejuízo para outrem e/ou ao benefício para o agente ou para um terceiro[78].

Por isso, a verdadeira intenção do agente ao praticar os atos de manipulação dos dados ou do seu tratamento é causar engano nas relações jurídicas (em regra, para prejudicar outrem ou obter um benefício para si ou para terceiro[79]), funcionando a intenção de que os documentos ou dados não genuínos sejam considerados ou utilizados para finalidades juridicamente relevantes como uma intenção "intermédia", "instrumental".

Deste modo, a intenção de que os documentos ou dados não genuínos sejam considerados ou utilizados para finalidades juridicamente relevantes e, desse modo, causar engano nas relações jurídicas consiste em o agente, ao manipular os dados informáticos ou o seu tratamento, atuar com o propósito de os documentos ou dados não genuínos que resultarão dessa manipulação virem a ser considerados ou utilizados para

78 Cfr. LOURENÇO MARTINS, "Criminalidade informática", *in* Direito da Sociedade da Informação, IV, p. 22, e DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 73.

Cremos que o propósito do legislador, ao exigir a intenção de causar engano nas relações jurídicas em vez da a intenção de causar um prejuízo a outrem ou de obter um benefício ilegítimo passa por obstar a lacunas de punibilidade nos casos (tendencialmente menos do que aqueles em que esta intenção existe) em que o agente possa não atuar com a intenção prejudicar outrem ou obter um benefício para si ou para terceiro, embora atue com a intenção de causar engano nas relações jurídicas mediante a consideração e/ou a utilização dos documentos ou dados não genuínos para finalidades juridicamente relevantes.

79 Sendo que, nessas situações, a verdadeira intenção do agente é prejudicar outrem ou obter um benefício para si ou para terceiro, funcionando também a intenção de causar engano nas relações jurídicas como uma intenção "intermédia", "instrumental" (cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, *Ibidem*).

finalidades juridicamente relevantes e, desse modo, causarem engano nas relações jurídicas[80].

Concordamos com PEDRO DIAS VENÂNCIO[81] quando considera que os dados ou documentos não genuínos terão de possuir, efetivamente, o valor probatório com o qual o agente pretende causar engano nas relações jurídicas, devendo, por isso, observar os requisitos de validade e eficácia e o valor probatório previstos no regime jurídico dos atos, documentos e comunicações eletrónicas consagrado no DL n.º 12/2021, de 9 de fevereiro.

Assim, ao criar e enviar o *e-mail* falso, o agente do crime está a introduzir dados informáticos (falsos) no sistema informático em que esse *e-mail* é criado e enviado, produzindo (e enviando) um *e-mail* falso, com a intenção de que seja considerado genuíno pelo destinatário, que, crendo na sua genuinidade, adotará a conduta "solicitada" nesse *e-mail* (*v.g.*, baixar um ficheiro, abrir um anexo, clicar e abrir um *link*, entrar numa dada página da Internet, etc.), permitindo que o agente, posteriormente, aceda ao sistema informático-alvo.

Deste modo, o *Cryptojacker*, nos casos em que, para poder ter acesso ao sistema informático *zumbi* crie e envie um *e-mail* falso, com a intenção de que seja considerado genuíno pelo destinatário, comete o crime de falsidade informática, p. e p. pelo artigo 3.º, n.º 1, da Lei n.º 109/2009, sendo que, na medida em que ambas as incriminações tutelam bens jurídicos diversos, existe uma relação de concurso efetivo entre os crimes de falsidade informática e de burla informática[82].

VII. Acesso ilegítimo

Conseguido o acesso ao sistema informático *zumbi*, o *Cryptojacker* irá utilizá-lo na mineração de criptomoedas, sendo que terá acesso aos dados armazenados nesse

80 No mesmo sentido, PEDRO DIAS VENÂNCIO, Lei do Cibercrime Anotada e Comentada, p. 39, e também em Lições de Direito do Cibercrime, p. 81 (nota 107).
81 PEDRO DIAS VENÂNCIO, Lei do Cibercrime Anotada e Comentada, pp. 38-39, e também em Lições de Direito do Cibercrime, p. 82.
82 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 81-82 (com referências bibliográficas e jurisprudenciais).

sistema, o que suscita a questão do eventual cometimento de um crime de acesso ilegítimo, p. e p. pelo artigo 6.º da Lei n.º 109/2009, nos termos do qual:

«*1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.*

2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.

3 - A pena é de prisão até 2 anos ou multa até 240 dias se as ações descritas no número anterior se destinarem ao acesso para obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.

4 - A pena é de prisão até 3 anos ou multa se:

a) O acesso for conseguido através de violação de regras de segurança; ou

b) Através do acesso, o agente obtiver dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.

5 - A pena é de prisão de 1 a 5 anos quando:

a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou

b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

6 - A tentativa é punível, salvo nos casos previstos nos n.ºs 2 e 3.

7 - Nos casos previstos nos n.ºs 1, 4 e 6 o procedimento penal depende de queixa».

A essência do crime de acesso ilegítimo assenta em o agente do crime aceder a um sistema informático alheio sem autorização legal ou do respetivo titular ou, existindo uma tal autorização, violando os limites da mesma[83]. Estamos perante uma conduta que, além de constituir crime por si mesma, também facilita o cometimento de outros crimes (*v.g.*, os crimes de dano relativo a programas ou outros dados informáticos, de sabotagem informática, de interceção ilegítima ou de burla informática e nas comunicações), podendo a criminalização do acesso ilegítimo ser vista como uma proteção antecipada e indireta contra os danos que afetem dados informáticos e a espionagem informática[84].

O crime de acesso ilegítimo tutela a segurança dos sistemas informáticos[85].

Quanto ao tipo objetivo, o crime de acesso ilegítimo simples inclui duas modalidades de conduta típica: (1) aceder, de qualquer modo, a um sistema informático, sem permissão legal ou sem para tanto estar autorizado pelo proprietário ou por outro titular do direito do sistema ou de parte dele e (2) produzir, vender, distribuir ou, por qualquer outra forma, disseminar ou introduzir, num ou mais sistemas informáticos, dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a permitir o acesso, de qualquer modo, a um sistema informático.

Atento o objeto do presente artigo, interessa-nos a primeira modalidade de conduta típica, que, como referimos, consiste em aceder, de qualquer modo, a um sistema informático, sem permissão legal ou sem para tanto estar autorizado pelo proprietário ou por outro titular do direito do sistema ou de parte dele. Esta modalidade

---

83 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 152, PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, p. 516, e Acórdãos da Relação de Lisboa de 11/04/2018, da Relação do Porto de 08/01/2014 e da Relação de Coimbra de 17/02/2016.

De acordo com PEDRO VERDELHO, *Ibidem*, «*o crime de acesso ilegítimo dirige-se às modernas ameaças à segurança dos sistemas informáticos que ponham em causa as respectivas confidencialidade, integridade e disponibilidade*».

84 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 152-153, e LOPES ROCHA, "A lei da criminalidade informática (Lei n.º 109/91 de 17 de Agosto). Génese e técnica legislativa", *in* Cadernos de Ciência de Legislação, n.º 8, p. 75.

85 Cfr. LOURENÇO MARTINS, "Criminalidade informática", *in* Direito da Sociedade da Informação, IV, p. 29, PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, p. 516, e DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 157.

Todavia, discute-se, na Doutrina e na Jurisprudência, qual é o bem jurídico tutelado pelo crime de acesso ilegítimo (cfr. DUARTE RODRIGUES NUNES, *Idem*, pp. 156-157).

de conduta típica configura um crime de mera atividade (pois apenas ocorre um acesso a um sistema informático, não se verificando qualquer modificação do mundo exterior) e de perigo abstrato (dado que o legislador se limita a presumir que tal conduta é passível de constituir um perigo para a segurança dos sistemas informáticos, sem exigir a criação de um perigo efetivo nem a lesão do bem jurídico)[86].

Quanto à descrição da conduta típica, a expressão "sistema informático" deverá ser entendida na aceção da al. a) do artigo 2.º da Lei n.º 109/2009[87], sendo que aceder significa entrar, no todo ou em parte, num sistema informático (*hardware*, componentes, dados armazenados nesse sistema, diretorias, ficheiros, dados de tráfego, dados de conteúdo, etc.) acessível através de redes de telecomunicações públicas ou num outro sistema informático pertencente à mesma rede no âmbito de uma organização (*v.g.*, um funcionário que acede ao sistema informático do administrador da empresa ou de um outro funcionário), como uma LAN ou *Intranet*[88].

O crime consuma-se com o mero acesso deliberado e não autorizado ao sistema informático, não sendo necessário que o agente se aproprie ("furte") dados informáticos nem que tome conhecimento efetivo das informações armazenadas no sistema informático, sendo que a incriminação do acesso ilegítimo visa suprir a impossibilidade de subsumir a "apropriação" do conteúdo de dados informáticos ao crime de furto (cujo tipo foi configurado tendo em vista apenas a apropriação de coisas corpóreas)[89].

Um outro elemento típico prende-se com a conduta do agente ter de ser levada a cabo sem permissão legal ou sem autorização do proprietário ou de outro titular do direito do sistema ou de parte dele. No que concerne à autorização legal, bastará que exista uma previsão na nossa ordem jurídica no sentido de, naquela situação concreta, ser permitido ao agente aceder àquele sistema informático[90].

---

86 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 157 e ss.
87 Assim, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 159.
88 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 159-160, e PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, p. 516.
89 Cfr. FARIA COSTA/HELENA MONIZ, "Algumas reflexões sobre a criminalidade informática em Portugal", *in* BFDUC, 1997, p. 331, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 157 e 160, e Acórdãos da Relação de Lisboa de 15/12/2009 e 22/03/2011 e da Relação do Porto de 14/04/2004 e 15/07/2009.
90 Encontramos exemplos de normas que permitem o acesso a sistemas informáticos nos arts. 14.º a 17.º da Lei n.º 109/2009, onde se preveem a injunção para apresentação ou concessão do acesso a dados (na vertente de concessão do acesso), a pesquisa de dados informáticos, a apreensão de dados informáticos e

A autorização do proprietário ou de outro titular do direito do sistema ou de parte dele constitui uma situação de acordo que exclui a tipicidade e que se distingue do consentimento enquanto causa de justificação pelo facto de, no acordo, estar em causa o exercício do direito de liberdade pela pessoa que o concede, correndo a realização da conduta no mesmo sentido da tutela do bem jurídico, pelo que não pode falar-se de uma lesão do bem jurídico; diversamente, no caso do consentimento, ocorre uma lesão efetiva do bem jurídico, cuja ilicitude é afastada por via da colisão entre o interesse jurídico-penal na preservação de bens jurídicos com o interesse, igualmente com relevo jurídico-penal, na salvaguarda da autorrealização do titular do bem jurídico (que terá de ser disponível), da sua autonomia pessoal e da sua vontade[91].

O crime de acesso ilegítimo apenas poderá ser cometido com dolo (cfr. artigo 6.º da Lei n.º 109/2009, conjugado com o artigo 13.º do Código Penal), bastando que o agente atue com dolo eventual.

Com relevância para o presente artigo, o crime de acesso ilegítimo possui cinco formas qualificadas (n.ºs 3, 4, als. a) e b), e 5, als. a) e b), do artigo 6.º da Lei n.º 109/2009), relevando aqui todas as circunstâncias modificativas agravantes previstas na Lei.

Assim, no caso do n.º 3, está em causa a preparação, a facilitação ou a possibilitação, através da adoção de alguma das condutas previstas no n.º 2 do art. 6.º, do acesso cm vista à obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento [*v.g.*, dados informáticos incorporados num cartão de débito ou crédito, numa *wallet* de criptomoedas, em dispositivos de *hardware* (computadores, *tablets*, *smartphones*, suportes autónomos, como uma *pendrive*, etc.) que permitam o acesso a redes de pagamentos ou transferências de dinheiro como as redes Multibanco, Visa, *Mastercard*, *American Express* ou *Paypal*, plataformas de

---

a apreensão de correio eletrónico e registos de comunicações de natureza semelhante, bem como a busca *online* (enquanto forma específica de pesquisa de dados informáticos). Relativamente a estes meios de obtenção de prova, *vide* DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 105 e ss. e 481 e ss., e também em Curso de Direito Processual Penal, 1, pp. 864 e ss.

91 Acerca da distinção entre consentimento e acordo (que exclui a tipicidade), *vide* COSTA ANDRADE, Consentimento e Acordo em Direito Penal, pp. 257 e ss. e 506 e ss., FIGUEIREDO DIAS, Direito Penal, Parte Geral, I, 3.ª Edição, pp. 555 e ss., e DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, 2.ª Edição, p. 260.

trading de criptomoedas, etc.][92]. As condutas referidas no art. 6.º, n.º 3, da Lei n.º 109/2009, terão de ser levadas a cabo de forma ilegítima, ou seja, o agente terá de atuar sem permissão legal ou sem autorização do proprietário ou de outro titular do direito do sistema ou de parte dele.

No que concerne à circunstância modificativa agravante prevista no artigo 6.º, n.º 4, al. a), da Lei n.º 109/2009, estão em causa as situações em que o acesso seja conseguido através da violação de regras de segurança, que, como refere ROGÉRIO BRAVO[93], consistem em «*qualquer acto suportado por tecnologias de informação e de comunicação, que constitua a transformação, a simulação, a decifração, a neutralização temporária ou a anulação, de meios técnicos destinados a assegurar a autenticação de serviços resultantes da acção de programas informáticos e de utilizadores legítimos, bem como a procura activa de elementos que possam permitir o acesso perante um sistema ou uma rede informática ou de comunicações.*». A violação de regras de segurança poderá consistir em o acesso ocorrer mediante a utilização de um PIN, *password* ou outro código de acesso ilegitimamente obtido pelo agente (o que inclui os tradicionais meios de autenticação simétrica e os meios de autenticação assentes no recurso a técnicas biométricas, bem como outros que venham a ser disponibilizados pelo progresso tecnológico) ou através da neutralização de dispositivos ou programas destinados a impedir o acesso ao sistema informático como as *firewalls*, os antivírus, o *antispyware*, etc.[94].

Relativamente à circunstância modificativa agravante prevista no artigo 6.º, n.º 4, al. b), da Lei n.º 109/2009, está em causa o acesso e a obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento [*v.g.*, dados informáticos incorporados num cartão de débito ou crédito, numa *wallet* de criptomoedas, em dispositivos de *hardware* (computadores, *tablets*, *smartphones*, suportes autónomos, como uma *pendrive*, etc.) que permitam o acesso a redes de

92 Cfr. DUARTE RODRIGUES NUNES, "Reflexões sobre as alterações às disposições penais materiais da Lei do Cibercrime", *in* Privacy and Data Protection Magazine, n.º 5, p. 20.
93 ROGÉRIO BRAVO, O Crime de Acesso Ilegítimo na Lei da Criminalidade Informática e na CiberConvenção.
94 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 167, PEDRO VERDELHO, "Cibercrime", *in* Direito da Sociedade da Informação, IV, p. 366, e ROGÉRIO BRAVO, O Crime de Acesso Ilegítimo na Lei da Criminalidade Informática e na CiberConvenção.

pagamentos ou transferências de dinheiro como as redes Multibanco, Visa, *Mastercard*, *American Express* ou *Paypal*, plataformas de *trading* de criptomoedas, etc.][95].

A conduta terá de ser levada a cabo de forma ilegítima sem permissão legal ou sem autorização do proprietário ou de outro titular do direito do sistema ou de parte dele, mas, para além disso, o agente terá de obter, por via desse acesso não autorizado, dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.

Passando à circunstância modificativa agravante prevista no artigo 6.º, n.º 5, al. a), da Lei n.º 109/2009, estão em causa informações relativas à vida e organização de uma empresa que não são geralmente conhecidas ou facilmente acessíveis (na sua globalidade ou na configuração e ligação exatas dos seus elementos constitutivos) a pessoas dos círculos que lidam normalmente com o tipo de informações em questão, que tenham valor comercial por serem secretas e que tenham sido objeto de diligências consideráveis, atendendo às circunstâncias, por parte da pessoa que detém legalmente o controlo das informações, no sentido de as manter secretas[96]. Os "dados confidenciais protegidos por lei" são informações que não são dados pessoais nem dados de localização, de tráfego ou de base, podendo incluir as informações protegidas pelo sigilo profissional (incluindo o sigilo bancário, o sigilo de funcionário e o sigilo fiscal), religioso ou de Estado ou pelo segredo de Justiça (incluindo as informações relativas a processos que, formalmente, não estão sujeitos a segredo de Justiça, mas que, ainda assim, são de natureza reservada, enquanto essa reserva, se for temporária, se mantiver) e outras que sejam subsumíveis à tutela do direito à intimidade/privacidade, nos termos do artigo 26.º da Constituição[97].

Por fim, quanto à circunstância modificativa agravante prevista no artigo 6.º, n.º 5, al. b), da Lei n.º 109/2009, o benefício ou vantagem patrimonial inclui a obtenção de dinheiro ou de outros bens ou um qualquer outro benefício patrimonial e a evitação da

95 Cfr. DUARTE RODRIGUES NUNES, "Reflexões sobre as alterações às disposições penais materiais da Lei do Cibercrime", *in* Privacy and Data Protection Magazine, n.º 5, p. 20.
96 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 167-168 (como maiores aprofundamentos).
97 Assim, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 168.

perda (incluindo o pagamento devido) de dinheiro ou de outros bens patrimoniais[98], devendo a vantagem obtida ser de valor consideravelmente elevado[99].

Assim, ao aceder ao sistema informático (e, consequentemente, aos dados nele armazenados, que, alguns deles, terão de ser modificados – *maxime* o editor de registo e os dispositivos de proteção como as *firewalls*, os antivírus, o *antispyware*, etc. – para permitir o acesso ao sistema e a mineração) sem autorização legal ou do proprietário ou de outro titular do direito do sistema ou de parte dele, o agente adota uma conduta subsumível ao n.º 1 do artigo 6.º da Lei n.º 109/2009[100]. Contudo, o acesso ilegítimo tenderá a ocorrer com a utilização abusiva de credenciais de acesso e com o uso de mecanismos destinados a neutralizar a proteção proporcionada por dispositivos de proteção como as *firewalls*, os antivírus, o *antispyware*, etc., e, desse modo, será conseguido através da violação de regras de segurança, pelo que a conduta tenderá a ser subsumida ao n.º 4, al. a), e não ao n.º 1 do artigo 6.º da Lei n.º 109/2009.

Mas, atenta a fenomenologia do *Cryptojacking*, não será de excluir a subsunção da conduta a alguma das circunstâncias modificativas agravantes do n.º 5 do artigo 6.º da Lei n.º 109/2009[101]. Assim, desde logo nos casos em que a conduta criminosa seja dirigida contra sistemas informáticos de bancos, de empresas ou de organismos públicos, é altamente provável que, ao aceder ao sistema e aos dados, o agente acabe por tomar conhecimento de segredo comercial ou industrial ou de dados confidenciais protegidos por Lei.

Cumpre ainda referir que o agente, mesmo nos casos em que possua, de forma legítima, as credenciais de acesso, poderá cometer o crime de acesso ilegítimo, pois, como referimos, o crime de acesso ilegítimo inclui também os casos em que o agente

98 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 169.
99 Na medida em que a Lei n.º 109/2009 não contém qualquer definição de valor consideravelmente elevado, resta recorrer ao artigo 202.º, al. b), do Código Penal, nos termos do qual o valor consideravelmente elevado é «*aquele que exceder 200 unidades de conta avaliadas no momento da prática do facto*». Desde a data de entrada em vigor da Lei n.º 109/2009 e até à presente data, sendo o valor da unidade de conta de €102,00, para estarmos perante um benefício ou vantagem de valor consideravelmente elevado, o benefício ou a vantagem terão de ser superiores €20.400,00.
100 Cfr., embora à luz do Direito alemão, Sentenças do *Bundesgerichtshof* de 21/07/2015 e 27/07/2017.
101 Que afastarão a aplicabilidade do n.º 4, al. a), desse preceito, que funcionará apenas como circunstância a valorar ao nível da determinação da medida concreta da pena, mais concretamente como circunstância agravante (cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 176-177).

atua violando os limites de uma autorização legal ou do proprietário ou de outro titular do direito do sistema ou de parte dele[102].

Como vimos, o crime de falsidade informática surge como uma espécie de ato preparatório do crime de acesso ilegítimo. Mas o agente será sempre punido pelo crime de falsidade informática, pois, além de o crime de falsidade informática ser punido com uma pena mais elevada do que o crime de acesso ilegítimo[103], os bens jurídicos tutelados por ambas as incriminações são diversos, existindo, por isso, concurso efetivo[104]. E, sendo igualmente diversos os bens jurídicos tutelados pelo crime de burla informática e pelo crime de acesso ilegítimo (sendo que, no caso do *Cryptojacking*, trata-se de dois crimes que são cometidos paralelamente, não sendo um preparatório do outro), existe concurso efetivo entre ambas as incriminações[105].

VIII. Dano relativo a programas ou outros dados informáticos

102 A este respeito, a Relação do Porto, no seu Acórdão de 14/04/2004, considerou que o agente cometeu um crime de acesso ilegítimo num caso em que, quando cessou a relação laboral entre o agente e a assistente, aquele retirou do sistema informático desta o código-fonte de um programa que desenvolvera enquanto fora seu trabalhador.

Do mesmo modo, a Relação de Lisboa, nos seus Acórdãos de 25/11/2015 e 11/04/2018, considerou que o agente cometeu um crime de acesso ilegítimo num caso em que, sendo trabalhador do assistente e dispondo de uma chave de acesso única, pessoal e intransmissível (que lhe permitia aceder ao sistema informático do assistente e visualizar os elementos deste constantes, bem como realizar e autorizar operações bancárias através do mesmo), sem qualquer motivo ou razão de serviço que o justificasse (e extravasando a autorização de acesso que o assistente lhe conferira), acedeu ao sistema informático do assistente utilizando a sua *password* para proceder à consulta de várias contas de depósito de clientes e realizar transferências de dinheiro. E a mesma Relação, no seu Acórdão de 07/03/2018, chegou à mesma conclusão num caso em que os agentes, extravasando as suas competências funcionais, acederam a dados de tráfego de um jornalista junto de uma operadora de telecomunicações para fins exclusivamente pessoais.

Por seu turno, a Relação de Coimbra, no seu Acórdão de 17/02/2016, considerou que o agente cometeu um crime de acesso ilegítimo num caso em que, sendo inspetor tributário e, não obstante deter legitimamente, para o exercício das suas funções, *username* e PIN, por motivos estritamente pessoais, acedeu ao sistema informático da Autoridade Tributária para consultar declarações de IRS de outra pessoa.

103 A pena do crime de falsidade informática poderá chegar, mesmo na sua forma simples, a 5 anos de prisão, ao passo que, no caso do crime de acesso ilegítimo, só nos casos subsumíveis ao n.º 5 do artigo 6.º da Lei n.º 109/2009 é que a pena poderá atingir os 5 anos, não indo além de 1 ano nos casos subsumíveis aos n.ºs 1 e 2, de 2 anos nos casos subsumíveis ao n.º 3 e de 3 anos nos casos subsumíveis ao n.º 4 desse preceito. Daí que, caso se considerasse que existia um concurso aparente de crimes, sempre conduziria a uma situação de consunção impura, que, como sabemos, consiste em, nos casos em que o crime "dominado" seja punível com uma pena mais grave do que o crime "dominante", o agente ser punido por aquele crime e não por este (cfr. DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, I, 2.ª Edição, p. 751).

104 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 83 e 177.

105 Assim, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 178.

Conseguido o acesso ao sistema informático, a etapa seguinte será modificar determinados dados informáticos no sistema *zumbi* (*maxime* o editor de registo para permitir o acesso e a realização de operações de mineração – eventualmente para se iniciarem quando o sistema informático esteja inativo há um determinado período de tempo ou enquanto não atinja um determinado grau de utilização dos seus recursos de *hardware* e para serem interrompidas quando o utilizador esteja a utilizar o sistema, a fim de evitar a deteção – e desativar dispositivos de proteção como as *firewalls*, os antivírus, o *antispyware*, etc.), pelo que se suscita a questão da eventual prática de um crime de dano relativo a programas ou outros dados informáticos, p. e p. pelo artigo 4.º da Lei n.º 109/2009, nos termos do qual:

«*1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afetar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa. (…)*

3 - Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas nesse número.

4 - Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias.

5 - Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos.

(…)».

A essência do crime de dano relativo a programas ou outros dados informáticos reside na supressão, inutilização ou danificação de dados informáticos, visando-se conferir aos dados informáticos (enquanto bens incorpóreos), no plano do Direito penal,

uma proteção análoga à dos bens corpóreos através do crime de dano, p. e p. pelos artigos 212.º e ss. do Código Penal[106].

O crime de dano relativo a programas ou outros dados informáticos tutela a integridade dos dados e o bom funcionamento dos programas[107].

Quanto ao tipo objetivo, o crime de crime de dano relativo a programas ou outros dados informáticos simples[108] inclui duas modalidades de conduta típica: (1) apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis dados informáticos alheios ou, por qualquer forma, afetar a capacidade de uso dos mesmos sem permissão legal ou sem para tanto estar autorizado pelo proprietário ou por outro titular do direito do sistema ou de parte dele e (2) produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos, de forma ilegítima, dispositivos ou dados informáticos destinados a apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis dados informáticos alheios ou, por qualquer forma, afetar a capacidade de uso dos mesmos.

Atento o objeto do presente artigo, interessa-nos a primeira modalidade de conduta típica, que, como referimos, consiste em apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis dados informáticos alheios ou, por qualquer forma, afetar a capacidade de uso dos mesmos sem permissão legal ou sem para tanto estar autorizado pelo proprietário ou por outro titular do direito do sistema ou de parte dele. Esta modalidade de conduta típica configura um crime de dano (pois o agente apaga, altera, destrói, no todo ou em parte, danifica, suprime ou torna não utilizáveis ou não acessíveis dados informáticos alheios ou, por qualquer forma, afeta a capacidade de uso dos mesmos) e de resultado (dado que da conduta do

106 Cfr. PEDRO VERDELHO, "Cibercrime", *in* Direito da Sociedade da Informação, IV, p. 365, e DUARTE RODRIGUES NUNES, "O crime de dano relativo a programas ou outros dados informáticos", *in* Revista do Ministério Público, n.º 153, p. 141.

107 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 93.

Todavia, discute-se, na Doutrina e na Jurisprudência, qual é o bem jurídico tutelado por esta incriminação (cfr. DUARTE RODRIGUES NUNES, *Idem*, p. 93).

108 A Lei contém duas modalidades de crime de dano relativo a programas ou outros dados informáticos qualificado nos n.ºs 4 e 5 do artigo 4.º da Lei n.º 109/2009, prendendo-se as circunstâncias modificativas agravantes apenas com o valor do prejuízo causado.

agente decorre uma modificação do mundo exterior, *in casu* dos dados informáticos que foram objeto da atuação do agente)[109].

Quanto à descrição da conduta típica, as expressões "sistema informático" e "dados informáticos" deverão ser entendidas na aceção o artigo 2.º, als. a) e b), respetivamente, da Lei n.º 109/2009 e os dados informáticos não poderão pertencer, pelo menos *in totum*, ao agente[110].

No que tange aos atos referidos no artigo 4.º, n.º 1, da Lei n.º 109/2009, apagar consiste na eliminação de dados informáticos que se encontram num sistema informático ou suporte autónomo, alterar consiste na modificação de dados informáticos que se encontram num sistema informático ou suporte autónomo e suprimir consiste na retenção, ocultação, em tornar temporariamente indisponíveis dados que se encontram num sistema informático ou suporte autónomo[111].

Quanto aos atos de destruir e danificar são atos essencialmente relativos a coisas corpóreas e poderão surgir dificuldades quanto à sua aplicação a realidades incorpóreas como os dados informáticos, sendo que a referência a esses atos bem como ao ato de tornar não acessíveis ou não utilizáveis dados informáticos servirá essencialmente para permitir a punição de condutas que, sendo subsumíveis a uma dessas situações, não possam ser subsumidas aos conceitos de apagamento, alteração ou supressão[112]. De todo o modo, de forma a conferir relevância ao facto de o legislador falar em apagamento e em destruição, nos casos em que os dados apagados possam ser ainda recuperados, estaremos perante o apagamento dos dados e, nos casos em que não possam sê-lo, estaremos perante a destruição dos dados. E, no caso da danificação (que consistem atentados à substância ou à integridade física da coisa que não atinjam o limiar da destruição[113]), seguindo o mesmo critério, se os dados apagados puderem ser ainda recuperados, estaremos perante o apagamento parcial dos dados e, nos casos em que não possam ser recuperados, estaremos perante a danificação ou a destruição parcial dos dados. E, no que tange à cláusula geral ("por qualquer forma afetar a capacidade de uso de dados informáticos"), como refere BENJAMIM SILVA RODRIGUES, «*Trata-se de*

109 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 94 e ss.
110 Assim, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 96
111 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 96-97.
112 Assim, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 97 e ss.
113 Cfr. COSTA ANDRADE, "Art. 212º", *in* Comentário Conimbricense do Código Penal, II, p. 222.

uma "cláusula aberta" (...) que visa fazer face à alta mutação tecnológica que se verifica ao nível da criminalidade informático-digital. Pretende-se alargar, até onde isso é humanamente possível, a capacidade de prever e prover às futuras condutas agressivas, actualmente desconhecidas, mas já plausivelmente imaginadas e viáveis num futuro próximo»[114].

Dado que esta primeira modalidade de conduta típica configura um crime de resultado, de acordo com a teoria da adequação, o ato concretamente adotado pelo agente terá de ser apto, adequado a apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis outros dados informáticos alheios ou a, por qualquer forma, afetar a sua utilização.

Um outro elemento típico prende-se com a conduta do agente ter de ser levada a cabo sem permissão legal ou sem autorização do proprietário ou de outro titular do direito do sistema ou de parte dele, sendo que, neste último caso, o consentimento funciona como causa excludente da tipicidade e não da ilicitude, tal como referimos quanto ao crime de acesso ilegítimo.

No que concerne à autorização legal, basta que exista uma previsão na nossa ordem jurídica no sentido de, naquela situação concreta, ser permitido ao agente apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis dados informáticos alheios ou, por qualquer forma, afetar a capacidade de uso dos mesmos. Encontramos um exemplo de autorização legal no artigo 16.º, n.º 7, al. d), da Lei n.º 109/2009, onde se prevê, como uma das modalidades possíveis da apreensão de dados informáticos, a eliminação não reversível ou o bloqueio do acesso aos dados[115].

Nos casos de consentimento, *rectius* acordo, o acordo poderá ser prestado pelo proprietário ou por outro titular do direito do sistema ou de parte dele e, por conseguinte, o crime poderá ser cometido contra outras pessoas que usufruam das vantagens proporcionadas pelo normal funcionamento dos dados informáticos e não apenas contra o proprietário.

---

114 BENJAMIM SILVA RODRIGUES, Da Prova Penal, IV, pp. 143-144.
115 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 100-101.

Quanto ao tipo subjetivo, o crime de dano relativo a programas ou outros dados informáticos apenas poderá ser cometido com dolo (cfr. artigo 4.º da Lei n.º 109/2009, conjugado com o artigo 13.º do Código Penal), bastando que o agente atue com dolo eventual.

Assim, ao alterar as configurações do editor de registo do sistema operativo, a fim de permitir que a mineração comece (sem que o utilizador se aperceba disso) ou pare automaticamente consoante estejam ou deixem de estar verificadas as condições definidas pelo agente (para evitar a deteção pelo utilizador), e a possibilitar o acesso remoto, pelo agente, ao computador *zumbi* através de uma ligação à Internet protegida por uma *password* obtida sem o conhecimento/consentimento do seu titular, e ao neutralizar os dispositivos de proteção como as *firewalls*, os antivírus, o *antispyware*, etc. para que não bloqueiem o acesso do agente ao sistema nem as operações de mineração sem autorização legal ou do proprietário ou de outro titular do direito do sistema ou de parte dele, o agente adota uma conduta subsumível ao n.º 1 do artigo 4.º da Lei n.º 109/2009[116].

Em face da diversidade dos bens jurídicos tutelados, existirá sempre uma situação de concurso efetivo com os crimes de acesso ilegítimo[117] e de burla informática[118], sendo que, no caso do crime de falsidade informática, a solução terá de ser casuística (existindo, nuns casos, concurso efetivo e, noutros, concurso aparente)[119].

IX. Sabotagem informática

O crime de sabotagem informática está previsto no artigo 5.º da Lei n.º 109/2009, nos termos do qual:

«*1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir,*

116 Cfr., embora à luz do Direito alemão, HALIME EREZ, "Das Schürfen von Bitcoins unter heimlicher Nutzung fremder Computer", *in* KriPoZ, 2020, p. 11, HEINE, "Bitcoins und Botnetze – Strafbarkeit und Vermögenabschöpfung bei illegalem Bitcoin-Mining", *in* NStZ, 2016, pp. 443-444 (embora diferenciando consoante o sistema operativo em causa), e Sentenças do *Bundesgerichtshof* de 21/07/2015 e 27/07/2017.
117 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 116 e 178.
118 Assim, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 115.
119 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 82-83 e 114-115.

interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.

2 – Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior. (…).

4 – A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado.

5 – A pena é de prisão de 1 a 10 anos se:

a) O dano emergente da perturbação for de valor consideravelmente elevado;

b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma atividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.».

A essência do crime de sabotagem informática, que tutela a segurança dos sistemas informáticos[120], reside na «*destruição, inutilização ou paralisação dos sistemas informáticos e telemáticos, ou de dados ou informação contida, transferida ou transmitida nos mesmos, assim como das suas funções de processamento e tratamento, seja mediante a utilização de métodos lógicos, informáticos ou telemáticos, seja mediante o abuso de equipamentos físicos*»[121].

Tendo em conta o objeto do presente artigo e abstraindo das formas qualificadas do crime (cfr. n.ºs 4 e 5), interessa-nos apenas a conduta prevista no n.º 1, sendo que,

120 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 125-126 (com maiores aprofundamentos quanto à discussão acerca do bem jurídico tutelado pela incriminação da sabotagem informática).
121 BENJAMIM SILVA RODRIGUES, Da Prova Penal, IV, p. 149.

numa escala de gravidade decrescente, entravar consiste na incapacitação definitiva e total, na destruição integral do sistema informático (não sendo, contudo, necessária a sua destruição física, bastando que esse sistema informático deixe, em definitivo, de funcionar). Impedir consiste na incapacitação definitiva, mas não total do sistema informático, permitindo apenas o seu funcionamento parcial. Interromper consiste na incapacitação apenas temporária do sistema informático, que, de forma meramente temporária, deixará de funcionar, no todo ou em parte. E, por último, perturbar gravemente consiste nas situações, em que, apesar de o sistema não deixar de funcionar, o funcionamento ocorre com perturbações, interferências (*v.g.*, o sistema informático funciona de forma mais lenta ou obrigando a *restarts* do sistema), devendo essas perturbações ou interferências possuir algum relevo ou alguma gravidade, pelo que, por exemplo, a maior lentidão terá de ser significativa e não apenas ligeira[122].

Para além disso, a conduta de entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático terá de ser levada a cabo mediante a introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de dados informáticos ou de interferência, por qualquer outro modo, num sistema informático, sendo uma tal enumeração meramente exemplificativa[123].

Quanto ao tipo subjetivo, o crime de sabotagem informática apenas é punido a título de dolo (cfr. artigo 5.º da Lei n.º 109/2009, conjugado com o artigo 13.º do Código Penal), bastando que o agente atue com dolo eventual.

Todavia, atenta a fenomenologia do *Cryptojacking*, o agente não cometerá o crime de sabotagem informática, essencialmente por duas razões.

Em primeiro lugar, como referimos, os agentes do *Cryptojacking* costumam programar o *malware* para nunca "consumir" mais do que uma determinada percentagem da CPU disponível ou mesmo não atuar quando o utilizador esteja a usar o sistema informático, razão pela qual, do ponto de vista técnico, muito dificilmente o

122 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 129.
123 No mesmo sentido, BENJAMIM SILVA RODRIGUES, Da Prova Penal, IV, p. 153, e DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 129 (com maiores desenvolvimentos quanto à definição dos atos de introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de dados informáticos ou de interferência por qualquer outro modo num sistema informático).

sistema informático *zumbi* ficará entravado (pelo menos por causa do *Cryptojacking*), sendo certo que, como vimos, não é qualquer perturbação do funcionamento do sistema informático que poderá ser subsumida ao crime de sabotagem informática.

E, em segundo lugar, sendo a conduta apenas punida a título de dolo, tendo em conta as cautelas que o agente toma para que a utilização abusiva do sistema informático alheio não seja detetada (e o entravamento poderá alertar o utilizador de que algo se passará) e o facto de não ter qualquer interesse em que o sistema entrave (com a consequente perda dessa capacidade de computação na "corrida" pela mineração), antes pelo contrário, jamais se poderá concluir que o agente se conformou com a possibilidade de, com a sua conduta, entravar o sistema informático alheio.

X. O confisco de vantagens obtidas por via da mineração de criptomoedas com utilização não autorizada de sistemas informáticos alheios

Na medida em que o *Cryptojacker* receberá um pagamento em criptomoedas sempre que consiga validar operações com criptomoedas antes dos demais mineradores, dúvidas não restam de que esses pagamentos constituem uma vantagem, que é obtida através da prática de crimes (*maxime* de crimes de burla informática, falsidade informática, acesso ilegítimo e dano relativo a programas ou outros dados informáticos).

O confisco de vantagens provenientes da prática de crimes pode consistir no confisco de vantagens "clássico" (previsto nos artigos 110.º e ss. do Código Penal[124]), no confisco "alargado" (previsto nos artigos 7.º e ss. da Lei n.º 5/2002) ou no confisco civil *in rem*[125] através de uma ação cível *in rem* (que não está previsto no Direito português)[126].

---

124 E também nos artigos 36.º a 38.º do Decreto-Lei n.º 15/93, de 22 de janeiro, relativamente às infrações previstas nesse diploma.

125 Ao contrário das demais formas de confisco, que são *in personam*, no confisco civil *in rem*, o fundamento do confisco não assenta na culpa do proprietário dos bens (sendo a sua eventual culpa absolutamente irrelevante), mas numa *fictio juris* de que a culpa recai sobre os bens.

126 Embora nos pareça que a nossa Lei deveria prever esta forma de confisco, pelas razões que aduzimos em DUARTE RODRIGUES NUNES, "Sobre a admissibilidade do confisco civil *in rem* de vantagens do crime", *in* Anatomia do Crime, n.º 6, pp. 187 e ss.

O confisco de vantagens "clássico" incide sobre as vantagens económicas *efetiva*[127] e direta/indiretamente[128] provenientes da prática de um facto ilícito típico e as recompensas[129] prometidas ou dadas aos agentes de um facto ilícito típico, já cometido ou a cometer, para eles ou para outrem, ainda que tenham sido alvo de transformação ou de reinvestimento posteriores. O confisco abrange quaisquer ganhos quantificáveis que tenham resultado dessa transformação ou reinvestimento. Deste modo, está em causa a "expropriação" de quaisquer coisas, direitos de natureza patrimonial, benefícios de uso e evitações de dispêndios que os agentes de um crime tenham obtido/evitado devido à prática do facto ilícito típico[130].

Por isso, os pressupostos do confisco "clássico" são: (1) a prática do facto ilícito típico e (2) a existência de proventos *efetivamente* obtidos através da prática desse concreto ilícito típico (já cometido ou a cometer) ou prometidos como contrapartida da sua prática.

O confisco de vantagens "clássico" será decretado mesmo que nenhuma pessoa determinada possa ser punida pelo facto, incluindo em caso de morte do agente ou quando o agente tenha sido declarado contumaz[131].

Deste modo, os pagamentos que o agente do *Cryptojacking* tiver efetivamente recebido como contrapartida da mineração de criptomoedas são passíveis de confisco

---

127 No confisco "clássico" terá de ser feita prova de que as vantagens económicas (e os ganhos resultantes da transformação ou reinvestimento) obtidas ou prometidas resultam *efetivamente* de um facto ilícito típico, inexistindo qualquer presunção legal nesse sentido. O que não significa que o confisco não possa ser decretado com base em prova indiciária, atento o disposto no artigo 127.º do Código de Processo Penal (no mesmo sentido, CONDE CORREIA, Da proibição do confisco à perda alargada, p. 142).

128 *V.g.*, se o agente reinvestir o dinheiro que recebeu ou evitou pagar/gastar por via da prática do facto ilícito típico em produtos financeiros e voltar a reinvestir o dinheiro com o produto ganho na primeira transação, pode ser confiscado o montante ganho nas ulteriores transações que tenham lugar.

129 Embora as recompensas (pelo menos as dadas) constituam, também elas, uma forma de vantagem económica *lato sensu*, umas e outras distinguem-se entre si pelo facto de a recompensa se destinar a recompensar ou a premiar a prática do facto ilícito típico (*v.g.*, o suborno pago como contrapartida de um ato de corrupção), ao passo que a vantagem consiste naquilo que é adquirido através da prática do facto (*v.g.*, o dinheiro auferido através do tráfico de droga).

130 Cfr. FIGUEIREDO DIAS, Direito Penal Português, p. 633.

131 Cfr. artigo 110.º, n.º 5, do Código Penal. São igualmente subsumíveis ao art. 110.º, n.º 5, as situações em que o facto esteja prescrito ou tenha ocorrido uma amnistia. No fundo, o que aqui está em causa são, essencialmente, situações de extinção da responsabilidade penal nos termos dos artigos 118.º e ss. do Código Penal, a que acresce a declaração de contumácia nos termos do artigo 335.º do Código de Processo Penal, mas não os casos de inimputabilidade – como considera CONDE CORREIA Da proibição do confisco à perda alargada, p. 134 (nota 292) –, que são "salvaguardados" pela exigência da prática de um ilícito típico e não de um crime. O artigo 110.º, n.º 5, do Código Penal configura um caso de confisco não dependente de condenação penal, mas não constitui uma *actio in rem*.

nos termos do artigo 110.º, n.º 1, al. b), do Código Penal, porquanto se trata de vantagens obtidas através da prática de crimes.

Por seu turno, o confisco "alargado", que recai sobre uma parte ou mesmo a totalidade do património do arguido e não sobre bens em concreto (estando em causa a "expropriação" da parte incongruente do património do arguido e não de bens determinados[132]), assenta numa presunção de que o património do arguido que não seja congruente com os seus rendimentos lícitos (*vs.* despesas) foi obtido através da prática de crimes, visando-se – tal como no confisco de vantagens "clássico" – restabelecer a ordem jurídica violada, retirando as vantagens patrimoniais que, por terem sido obtidas ilicitamente, não deveriam tê-lo sido, promovendo uma ordenação dos bens adequada ao Direito[133] e privando as organizações criminosas e terroristas, os terroristas, os criminosos de colarinho branco e os cibercriminosos de recursos que podem ser usados para continuar e/ou dissimular a atividade criminosa[134]. Só que, por se tratar de formas de criminalidade de reduzida visibilidade exterior e que utilizam todos os meios à sua disposição para dissimular o património obtido através da sua atividade criminosa (o que dificulta o estabelecimento da ligação entre os proventos económicos e os crimes de que provêm em concreto[135]), a inversão do ónus da prova mostra-se absolutamente necessária[136].

Quanto aos pressupostos[137], em primeiro lugar, o arguido terá de ter sido condenado, por sentença transitada em julgado, pela prática de um dos crimes

---

132 Cfr. Acórdãos da Relação do Porto de 11/06/2014 e 16/03/2016.

133 Cfr. JORGE GODINHO, "Brandos costumes? O confisco penal com base na inversão do ónus da prova", *in Liber Discipulorum* para Jorge de Figueiredo Dias, p. 1351, CONDE CORREIA, Da proibição do confisco à perda alargada, pp. 63-64, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 404-405, e Acórdãos do Tribunal Constitucional n.ºs 392/2015, 476/2015 e 498/2019, da Relação de Lisboa de 27/03/2014 e da Relação de Coimbra de 25/01/2006 e 15/03/2006.

134 Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 405.

135 No mesmo sentido, FRANCISCO BORGES, "Perda alargada de bens: alguns problemas de constitucionalidade", *in* Estudos em homenagem ao Prof. Doutor Manuel da Costa Andrade, Volume I, p. 218.

136 Cfr. DUARTE RODRIGUES NUNES, "Admissibilidade da inversão do ónus da prova no confisco "alargado" de vantagens provenientes da prática de crimes", *in* Julgar Online, p. 12, e Acórdãos do Tribunal Constitucional n.ºs 392/2015, 476/2015 e 498/2019.

137 Quanto aos pressupostos do confisco "alargado", com maior aprofundamento e amplas referências bibliográficas, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 409 e ss.

previstos no artigo 1.º, n.º 1, da Lei n.º 5/2002[138], independentemente da concreta forma de comparticipação criminosa e da pena concretamente aplicada.

Em segundo lugar, o arguido terá de possuir um património, *i.e.,* um conjunto de ativos de qualquer tipo (corpóreos ou incorpóreos, móveis ou imóveis, tangíveis ou intangíveis) e os documentos ou instrumentos jurídicos que atestem a propriedade ou outros direitos sobre os referidos ativos que (1) estejam na titularidade do arguido ou em relação aos quais o mesmo tenha o domínio e o benefício à data da constituição como arguido ou posteriormente, (2) transferidos para terceiros a título gratuito ou mediante contraprestação irrisória nos cinco anos anteriores à constituição como arguido e (3) recebidos pelo arguido nos cinco anos anteriores à constituição como arguido, ainda que não se consiga determinar o seu destino[139].

Em terceiro lugar, pela sua "subsidiariedade" face ao confisco "clássico" de vantagens, o confisco "alargado" pressupõe que não se tenha provado que aquele património (ou parte dele) foi obtido por via do cometimento de crimes pelos quais o arguido tenha sido condenado (independentemente de serem do catálogo ou não), pois, nesse caso, os bens serão perdidos à luz do confisco "clássico", não sendo admissível que um bem seja objeto de perdimento com base no confisco "clássico" de vantagens e, subsequentemente, o seu valor seja considerado para efeitos de confisco "alargado".

E, em quarto lugar, o valor do património do arguido (correspondente ao somatório do valor dos bens que o integram nos termos do artigo 7.º, n.º 2, da Lei n.º 5/2002) terá de ser incongruente, desproporcionado, não condizente com os rendimentos lícitos do arguido concatenados com as suas despesas.

Entre os crimes previstos no artigo 1.º, n.º 1, da Lei n.º 5/2002 encontramos os crimes de dano relativo a programas ou outros dados informáticos e de sabotagem informática, bem como o crime de acesso ilegítimo (mas apenas nos casos em que, por via do acesso, o agente tenha tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais protegidos por Lei, tenha obtido um benefício ou vantagem patrimonial de valor consideravelmente elevado, o crime tenha sido cometido com a

138 O confisco é decretado na própria decisão condenatória, mas só é efetivado após o respetivo trânsito em julgado.
139 Cfr. artigo 7.º, n.º 2, da Lei n.º 5/2002, conjugado (quanto ao conceito de bens) com o artigo 2.º, al. d), da Convenção das Nações Unidas Contra a Criminalidade Organizada Transnacional, que, tendo sido ratificada, integra a nossa ordem jurídica (cfr. art. 8.º, n.º 2, da Constituição).

utilização de dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a aceder a um sistema informático ou integrar uma das condutas tipificadas no n.º 2 do artigo 6.º da Lei n.º 109/2009[140])[141].

Deste modo, o agente do *Cryptojacking*, caso seja condenado pela prática de crimes de dano relativo a programas ou outros dados informáticos (como tenderá a suceder) e/ou de acesso ilegítimo (desde que a sua conduta seja subsumível a alguma das situações mencionadas no artigo 1.º, n.º 1, al. m), da Lei n.º 5/2002) e estejam verificados os demais pressupostos legais do confisco "alargado", poderá ser alvo da aplicação deste mecanismo legal de confisco de vantagens provenientes da prática de crimes.

XI. Conclusões

1. As criptomoedas são moedas virtuais utilizadas para realizar pagamentos em transações comerciais, que possuem quatro características que as distinguem das moedas convencionais ou fiduciárias (euro, dólar, rublo, iene, libra).

2. Uma dessas características é a descentralização, que significa que as criptomoedas são independentes da intervenção de um banco central e/ou do Estado para a sua regulamentação, variando a sua cotação apenas em função do funcionamento do mercado e sendo o sistema *Blockchain* o único elemento central que intervém no processo e que funciona como uma espécie de livro de contabilidade digital (descentralizado) em que são registadas todas as transações realizadas pelos membros de uma grande comunidade de utilizadores.

3. *Conditio sine qua non* da efetivação das operações com criptomoedas e da consequente inserção na *Blockchain* é a validação das operações (mineração).

4. São vários os atores que intervém no mundo das criptomoedas, entre os quais estão os mineradores (*Miners* ou *Cryptominers*), que são as pessoas singulares ou coletivas que disponibilizam os seus sistemas informáticos para a validação e

140 Ilegitimamente produzir, vender, distribuir ou, por qualquer outra forma, disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a aceder a um sistema informático.
141 Cfr. artigo 1.º, n.º 1, al. m), da Lei n.º 5/2002.

o consequente registo de transações em criptomoedas na *Blockchain*, recebendo, em contrapartida, uma determinada taxa paga em criptomoedas.

5. Na medida em que o pagamento dessa validação só é feito a quem tenha "decifrado" o *puzzle* criptográfico relativo a cada transação em primeiro lugar, estabelece-se uma enorme competição entre os vários mineradores, o que requer que cada um possua a maior capacidade de computação possível (o que implica, igualmente, um grande dispêndio em energia e em material informático).

6. Por isso, alguns mineradores, com o objetivo de aumentar a sua capacidade de computação e evitar dispêndios com energia elétrica e com a aquisição de material informático, optam por levar a cabo atividades de *Cryptojacking*.

7. O *Cryptojacking* consiste na utilização não autorizada de um sistema informático (incluindo a sua ligação à Internet) e de energia elétrica alheios para fins de mineração de criptomoedas. Essa utilização pode ser direta (infetando um sistema informático alheio com *malware*) ou indiretamente ("furtando" ciclos de processamento enquanto a vítima visita um determinado *website*).

8. O aumento da capacidade de computação será tanto maior quanto maior for o número de sistemas informáticos alheio utilizados, razão pela qual os agentes do crime tentarão construir *botnets* para esse fim. Uma forma de criar ou de expandir uma *botnet* passa pela utilização de um *malware* com capacidades de *worm*, que permitirá que o *malware* se expanda e instale noutros sistemas informáticos pertencentes à mesma rede informática.

9. Nos casos em que é levado a cabo diretamente, o *Cryptojacking* requer que o minerador aceda aos sistemas informáticos alheios que irão constituir a *botnet* como sistemas informáticos *zumbis* ou *zombies*, que passarão a ser comandados pelo sistema informático do agente do crime (*Central Command and Control Center*), o que depende da instalação de um *malware* que irá "furtar" ciclos de processamento da CPU para realizar as operações necessárias à mineração de criptomoedas.

10. Ao realizarem as operações necessárias à mineração de criptomoedas, os agentes do crime irão aceder, sem autorização, a sistemas informáticos alheios e aos dados neles guardados, bem como consumir energia elétrica, que será paga pelo

utilizador desse sistema informático, causando-lhe, dessa forma, um prejuízo patrimonial. Além disso, irão alterar as configurações do editor de registo do sistema operativo, a fim de permitir que a mineração comece (sem que o utilizador se aperceba disso) ou pare automaticamente consoante estejam ou deixem de estar verificadas as condições definidas pelo agente (para evitar a deteção pelo utilizador), e proporcionar o acesso remoto, pelo agente, ao computador *zumbi* através de uma ligação à Internet protegida por uma *password* obtida sem o conhecimento/consentimento do seu titular e neutralizar os dispositivos de proteção como as *firewalls*, os antivírus, o *antispyware*, etc. para que não bloqueiem o acesso do agente ao sistema nem as operações de mineração.

11. Ao agir do modo descrito, o agente do *Cryptojacking* poderá cometer, em concurso efetivo, crimes de burla informática, falsidade informática, acesso ilegítimo e dano relativo a programas ou outros dados informáticos

12. Na medida em que o agente do *Cryptojacking*, para obter o pagamento em criptomoedas sempre que consiga validar operações com criptomoedas antes dos demais mineradores, pratica crimes, os pagamentos que tiver efetivamente recebido como contrapartida da mineração de criptomoedas nessas circustâncias são passíveis de confisco de vantagens "clássico" nos termos do artigo 110.º, n.º 1, al. b), do Código Penal.

13. Para além disso, caso seja condenado pela prática de crimes de dano relativo a programas ou outros dados informáticos (como tenderá a suceder) e/ou de acesso ilegítimo (desde que a sua conduta seja subsumível a alguma das situações mencionadas no artigo 1.º, n.º 1, al. m), da Lei n.º 5/2002) e estejam verificados os demais pressupostos legais do confisco "alargado", o património do agente do *Cryptojacking* que não seja congruente com os seus rendimentos lícitos (após a dedução das suas despesas) será alvo de confisco "alargado" de vantagens provenientes da prática de crimes, nos termos do artigo 7.º da Lei n.º 5/2002.

XII. Bibliografia

Albuquerque, Paulo Pinto de – Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos Humanos, 5.ª Edição, Universidade Católica Editora, Lisboa, 2022.

Andrade, Manuel da Costa – Consentimento e Acordo em Direito Penal, Coimbra Editora, Coimbra, 1991.

Andrade, Manuel da Costa – "Art. 212º", *in* Comentário Conimbricense do Código Penal Parte Especial, Tomo II, pp. 202 e ss., Coimbra Editora, Coimbra, 1999.

Antunes, Mário/Rodrigues, Baltazar – Introdução à Cibersegurança, A Internet, os aspetos legais e a análise digital forense, FCA, Lisboa, 2018.

Ascensão, José de Oliveira – "Criminalidade informática", *in* Direito da Sociedade da Informação, Volume II, pp. 203 e ss., Coimbra Editora, Coimbra, 2001.

Borges, Francisco – "Perda alargada de bens: alguns problemas de constitucionalidade", *in* Estudos em homenagem ao Prof. Doutor Manuel da Costa Andrade, Volume I, Direito Penal, pp. 215 e ss., Universidade de Coimbra, Coimbra, 2017.

Bravo, Rogério – O Crime de Acesso Ilegítimo na Lei da Criminalidade Informática e na CiberConvenção, *in www.academia.edu/2039178/O_Crime_de_Acesso_Ilegi_timo_na_Lei_da_Criminal*

Idade_Informa_tica_e_na_CiberConvencao (consultado em 30/06/2021).

Carvalho, Américo Taipa de – Direito Penal, Parte Geral, Questões fundamentais, Teoria geral do crime, 3.ª Edição, Universidade Católica Editora, Porto, 2016.

Cordeiro, António Menezes – Tratado de Direito Civil Português, I, Parte Geral, Tomo II, Coisas, 2.ª Edição, Almedina, Coimbra, 2002.

Correia, João Conde – Da Proibição do Confisco à Perda Alargada, INCM, Lisboa, 2012.

Costa, A.M. Almeida – "Art. 217º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, pp. 274 e ss., Coimbra Editora, Coimbra, 1999.

Costa, A.M. Almeida – "Art. 221º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, pp. 328 e ss., Coimbra Editora, Coimbra, 1999.

Costa, José Francisco de Faria – "Algumas reflexões sobre o estatuto dogmático do chamado "Direito penal informático"", *in* Direito Penal da Comunicação, Alguns escritos, pp. 103 e ss., Coimbra Editora, Coimbra, 1998.

Costa, José Francisco de Faria– "Art. 203º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, pp. 24 e ss., Coimbra Editora, Coimbra, 1999.

Costa, José Francisco de Faria/Moniz, Helena – "Algumas reflexões sobre a criminalidade informática em Portugal", *in* Boletim da Faculdade de Direito da Universidade de Coimbra, Volume LXXIII (1997), pp. 297 e ss., Universidade de Coimbra, Coimbra, 1997.

Dias, Jorge de Figueiredo – Direito Penal Português, Parte Geral II, As Consequências Jurídicas do Crime, Editorial Notícias, Lisboa, 1993.

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

Erez, Halime – "Das Schürfen von Bitcoins unter heimlicher Nutzung fremder Computer", *in* Kriminalpolitische Zeitschrift, 2020, pp. 1 e ss., *in https://kripoz.de/wp-content/uploads/2021/03/erez-das-schuerfen-von-bitcoins-unter-heimlicher-nutzung-fremder-computer.pdf* (consultado em 29/06/2021).

Europol – Internet Organised Crime Threat Assessment 2018, *in www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018* (consultado em 21/06/2021).

Europol – Internet Organised Crime Threat Assessment 2019, *in https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019* (consultado em 21/06/2021).

Europol – Internet Organised Crime Threat Assessment 2020, *in https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020* (consultado em 21/06/2021).

Europol – Internet Organised Crime Threat Assessment 2021, *in https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2021* (consultado em 05/09/2023).

Europol – Internet Organised Crime Threat Assessment 2023, *in https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2023* (consultado em 12/10/2023).

Godinho, Jorge – "Brandos costumes? O confisco penal com base na inversão do ónus da prova", *in Liber Discipulorum* para Jorge de Figueiredo Dias, pp. 1315 e ss., Coimbra Editora, Coimbra, 2003.

Gonçalves, Manuel Lopes Maia – Código Penal Anotado e Comentado, 12.ª Edição, Almedina, Coimbra, 1998.

Heine, Sonja – "Bitcoins und Botnetze – Strafbarkeit und Vermögenabschöpfung bei illegalem Bitcoin-Mining", *in* Neue Zeitschrift für Strafrecht, 2016, pp. 441 e ss., C. H. Beck'sche Verlagsbuchhandlung, Munique e Frankfurt, 2016.

Leal-Henriques, Manuel/Simas Santos, Manuel – Código Penal Anotado, Volume III, Parte Especial, 4.ª Edição, Editora Rei dos Livros, Lisboa, 2016.

Maddison, John – Is Cryptojacking Replacing Ransomware as the Next Big Threat?, *in https://www.fortinet.com/blog/industry-trends/is-cryptojacking-replacing-ransomware-as-the-next-big-threat-* (consultado em 21/06/2021).

Marques, Garcia/Martins, Lourenço – Direito da Informática, 2.ª Edição Refundida e Actualizada, Almedina, Coimbra, 2006.

Martins, Lourenço – "Criminalidade informática", *in* Direito da Sociedade da Informação, Volume IV, pp. 9 e ss., Coimbra Editora, Coimbra, 2003.

Nadeau, Michael – What is cryptojacking? How to prevent, detect, and recover from it, *in https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html* (consultado em 21/06/2021).

Nunes, Duarte Rodrigues – "Admissibilidade da inversão do ónus da prova no confisco "alargado" de vantagens provenientes da prática de crimes", *in* Julgar Online, *in http://julgar.pt/admissibilidade-da-inversao-do-onus-da-prova-no-confisco-*

alargado-de-vantagens-provenientes-da-pratica-de-crimes/ (consultado em 18/09/2020).

Nunes, Duarte Rodrigues – "Sobre a admissibilidade do confisco civil *in rem* de vantagens do crime", *in* Anatomia do Crime, n.º 6, pp. 177-205, Almedina, Coimbra, 2017.

Nunes, Duarte Rodrigues – "O crime de dano relativo a programas ou outros dados informáticos", *in* Revista do Ministério Público, n.º 153, pp. 141 e ss., Lisboa, 2018.

Nunes, Duarte Rodrigues – O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, Gestlegal, Coimbra, 2019.

Nunes, Duarte Rodrigues – Os crimes previstos na Lei do Cibercrime, Gestlegal, Coimbra, 2020.

Nunes, Duarte Rodrigues – Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, Gestlegal, Coimbra, 2021.

Nunes, Duarte Rodrigues – "Reflexões sobre as alterações às disposições penais materiais da Lei do Cibercrime", *in* Privacy and Data Protection Magazine, n.º 5, pp. 11 e ss., Universidade Europeia, Lisboa, 2022, *in https://www.europeia.pt/resources/media/documents/Revista_Privacy_Data_Protection_Magazine_N5.pdf* (consultado em 01/09/2023).

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

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

Pereira, Joel Timóteo Ramos – Compêndio Jurídico da Sociedade da Informação, Quid Juris, Lisboa, 2004.

Rocha, Manuel António Lopes – "A lei da criminalidade informática (Lei n.º 109/91 de 17 de Agosto). Génese e técnica legislativa", *in* Cadernos de Ciência de

Legislação, n.º 8 (Outubro-Dezembro 1993), pp. 65 e ss., Instituto Nacional da Administração, Lisboa, 1993.

Rodrigues, Benjamim Silva – Da Prova Penal, Tomo IV, Da Prova Electrónico-Digital e da Criminalidade Informático-Digital (Contributo para a Fundamentação de um Modelo Dinâmico-Reversivo de Ciência Forense Digital em sede de Investigação da Cyber-Criminalidade Informático-Digital e à Luz do Novíssimo Regime da Lei do Cibercrime Portuguesa), Rei dos Livros, Lisboa, 2011.

Sherer, James A./McLellan, Melinda L./Fedeles, Emily R./Sterling, Nichole L. – "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, pp. 1 e ss., *in https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (consultado em 14/06/2021).

Simmler, Monika /Selman, Sine /Burgmeister, Daniel – "Beschlagnahme von Kryptowährungen", *in* Aktuelle Juristische Praxis - Pratique Juridique Actuelle, n.º 8/2018, pp. 963 e ss., Dike Verlag, Zurique e St. Gallen, 2018.

Venâncio, Pedro Dias – Lições de Direito do Cibercrime. E da tutela penal de dados pessoais, Editora d'Ideias, Coimbra, 2022.

Venâncio, Pedro Dias – Lei do Cibercrime Anotada e Comentada, Atualizada pela Lei n.º 79/2021, de 24 de novembro, Editora d'Ideias, Coimbra, 2023.

Verdelho, Pedro – "Cibercrime", *in* Direito da Sociedade da Informação, Volume IV, pp. 347 e ss., Coimbra Editora, Coimbra, 2003.

Verdelho, Pedro – "A Convenção sobre o Cibercrime do Conselho da Europa – Repercussões na Lei portuguesa", *in* Direito da Sociedade da Informação, Volume VI, pp. 257 e ss., Coimbra Editora, Coimbra, 2006.

Verdelho, Pedro – "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, pp 505 e ss., Universidade Católica Editora, Lisboa, 2010.

Jurisprudência

Portugal

Tribunal Constitucional

Acórdão n.º 392/2015, *in www.tribunalconstitucional.pt*.

Acórdão n.º 476/2015, *in www.tribunalconstitucional.pt*.

Acórdão n.º 498/2019, *in www.tribunalconstitucional.pt*.

Supremo Tribunal de Justiça

Acórdão de 10 de janeiro de 2001 (Proc. 00P3101), *in www.dgsi.pt.*

Acórdão de 14 de julho de 2004 (Proc. 04P3287), *in www.dgsi.pt.*

Acórdão de 12 de julho de 2006 (Proc. 06P2032), *in www.dgsi.pt.*

Acórdão de 20 de setembro de 2006 (Proc. 06P1942), *in www.dgsi.pt.*

Acórdão de 5 de novembro de 2008 (Proc. 08P2817), *in www.dgsi.pt.*

Acórdão de 20 de outubro de 2010 (Proc. 78/07.6JAFAR.E2.S1), *in www.dgsi.pt.*

Acórdão de 12 de setembro de 2012 (Proc. 1008/11.6JFLSB-L1.S1), *in www.dgsi.pt.*

Acórdão de 1 de abril de 2020 (Proc. 643/18.6PTLSB.L1.S1), *in www.dgsi.pt.*

Tribunal da Relação de Coimbra

Acórdão de 25 de janeiro de 2006 (Processo 3980/05), *in www.dgsi.pt.*

Acórdão de 15 de março de 2006 (Processo 2421/05), *in www.dgsi.pt.*

Acórdão de 17 de fevereiro de 2016 (Proc. 2119/11.TALRA.C2), *in www.dgsi.pt.*

Tribunal da Relação de Évora

Acórdão de 12 de setembro de 2017 (Proc. 151/15.7GAVRS.E1), *in www.dgsi.pt*.

Acórdão de 10 de março de 2020 (Proc. 322/16.9GBCCH.E1), *in www.dgsi.pt*.

Acórdão de 22 de setembro de 2020 (Proc. 547/15.4GBCCH.E1), *in www.dgsi.pt*.

Acórdão de 23 de fevereiro de 2021 (Proc. 413/18.1T9VRS.E1), *in www.dgsi.pt*.

Tribunal da Relação de Guimarães

Acórdão de 20 de fevereiro de 2018 (Proc. 1111/16.6T9BCL.G1), *in www.dgsi.pt.*

Acórdão de 23 de janeiro de 2020 (Proc. 373/16.3T9BCL.G1), *in www.dgsi.pt.*

Tribunal da Relação de Lisboa

Acórdão de 15 de dezembro de 2009 (Proc. 4251/07.7TDLSB.L1-5), *in www.dgsi.pt.*

Acórdão de 22 de março de 2011 (Proc. 4252/07.7TDLSB.L1-5), *in www.dgsi.pt.*

Acórdão de 27 de março de 2014 (Processo 463/07.3TAALM-A.L2-9), *in www.dgsi.pt.*

Acórdão de 25 de novembro de 2015 (Proc. 47/11.1TOLSB.L1-3), *in www.dgsi.pt.*

Acórdão de 7 de março de 2018 (Proc. 5481/11.4TDLSB.L1-3), *in www.dgsi.pt.*

Acórdão de 11 de abril de 2018 (Proc. 108/09.7XCLSB-3), *in www.dgsi.pt.*

Tribunal da Relação do Porto

Acórdão de 23 de maio de 1990 (Proc. 0123980), *in www.dgsi.pt.*

Acórdão de 14 de abril de 2004 (Proc. 0346424), *in www.dgsi.pt.*

Acórdão de 29 de abril de 2009 (Proc. 0847824), *in www.dgsi.pt.*

Acórdão de 15 de julho de 2009 (Proc. 0816124), *in www.dgsi.pt.*

Acórdão de 29 de setembro de 2010 (Proc. 683/08.3TDPRT-A.P1), *in www.dgsi.pt.*

Acórdão de 8 de janeiro de 2014 (Proc. 1170/09.8JAPRT.P2), *in www.dgsi.pt.*

Acórdão de 11 de junho de 2014 (Proc. 1653/12.2JAPRT-A.P1), *in www.dgsi.pt.*

Acórdão de 3 de fevereiro de 2016 (Proc. 482/10.2SJPRT.P1), *in www.dgsi.pt.*

Acórdão de 16 de março de 2016 (Proc. 2376/14.3TDPRT-D.P1), *in www.dgsi.pt.*

Acórdão de 24 de janeiro de 2018 (Proc. 343/15.9T9ESP.P1), *in www.dgsi.pt.*

Acórdão de 15 de fevereiro de 2023 (Proc. 417/17.1T9ETR.P1), ***in www.dgsi.pt.***

Alemanha

Bundesgerichtshof

Sentença de 21 de julho de 2015, *in https://www.hrr-strafrecht.de/hrr/1/15/1-16-15.php* (consultado em 21/04/2021).

Sentença de 27 de julho de 2017, *in https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=2017-7-27&nr=82664&pos=2&anz=29* (consultado em 21/04/2021).

Da Disciplina da Segurança ma Proteção de Dados, Aplicada ao Poder Local[1]

MANUEL DAVID MASSENO[2]

1 Este texto foi sobretudo construído a partir das aulas lecionadas ao *Mestrado em Engenharia Informática* do Instituto Politécnico de Beja, desde 2010, e ao *Curso de Pós-Graduação Avançada em Direito da Proteção de Dados* do Centro de Investigação em Direito Privado da Faculdade de Direito da Universidade de Lisboa, desde 2020.

2 Professor Adjunto e Encarregado da Proteção de Dados do Instituto Politécnico de Beja. É Membro convidado do PDPC - Centro de estudos e análise da privacidade e proteção de dados da Universidade Europeia, de Lisboa e integra a EDEN – Rede de Especialistas em Proteção de Dados da Europol – a Agência da União Europeia de Cooperação Policial.

SUMÁRIO: 1. Um ponto de partida, a segurança dos dados pessoais; 2. Uma omissão… voluntária, as regras de segurança; 2.1. Os referenciais possíveis para uma densificação; 2.2. as normas no domínio da cibersegurança; 3. as "medidas técnicas e organizativas adequadas"; 3.1. um critério básico para o tratamento, a "minimização"; 3.2. uma medida… arriscada, a "anonimização"; 3.3. uma medida menos eficaz, a "pseudonimização"; 3.4. a saída que ficou por assumir, a "cifragem"; 4. Quando a segurança falha, a "violação de dados pessoais"; 4.1. o procedimento interno; 4.2. a notificação à CNPD e a comunicação aos titulares dos dados; 4.3. as outras comunicações legalmente devidas; Referências.

1. Um ponto de partida, a segurança dos dados pessoais

Do *Regulamento Geral sobre a Proteção de Dados* da UE – União Europeia, o *RGPD*[3] consta um dever de "segurança no tratamento" para o respetivo responsável e/ou o subcontratante. O qual está, desde logo, subjacente a um dos Princípios relativos ao tratamento de dados pessoais, o da «integridade e confidencialidade», pois os dados devem ser "Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas" (Art.º 5.º n.º 1 f))[4].

O que em especial se concretiza na previsão, em cujos termos, "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 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 […]" (Art.º 32.º n.º 1).

Especificando a regra, segundo a qual, "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

3 Por extenso, Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>, aplicável desde o dia 25 de maio de 2018. Salvo quando expressamente indicado, todos os preceitos referidos são do *RGPD*.

4 O presente trabalho consiste numa pré-publicação de um capítulo destinado ao livro sobre privacidade e proteção de dados a ser editado pelo Município de Lisboa, sob a Coordenação da Doutora Cristina Gouveia Caldeira. Por essa razão, privilegiámos ao máximo a transcrição de excertos dos textos originais, sobretudo se de natureza legislativa, relativamente a paráfrases, de modo a facilitar a identificação e o entendimento das Fontes, ao não ser espectável que todos os leitores tenham conhecimentos aprofundados em matéria de Direito da Proteção de Dados. Pelos mesmos motivos, abstive-me de enquadrar o texto com um aparato doutrinal, apenas indicando no final os Comentários e os Manuais entretanto publicados em Portugal. Este texto beneficiou ainda da revisão feita pelo Eng.º Jorge Gomes da Silva, da Câmara Municipal de Lisboa.

conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades." (Art.º 24.º n.º 1)[5].

A serem efetivadas "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 decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis [Consequentemente,] o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento [*i.e.*, *by Design* e *by Default*] […] as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados." (Art.º 25.º n.º 1)[6].

Sempre tendo na devida consideração que "Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas 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. […]" (Art.º 35.º n.º 1), podendo inclusive exigir uma "consulta prévia" à CNPD – Comissão Nacional de Proteção de Dados "[…] quando a avaliação de impacto sobre a proteção de dados […] indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco." (Art.º 36.º).

---

5 O que é explicado no *Considerando* (83) do Regulamento: "A fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a cifragem. Essas medidas deverão assegurar um nível de segurança adequado, nomeadamente a confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função dos riscos 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 pessoais, tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a danos físicos, materiais ou imateriais.".

6 A este propósito, são especialmente de atender *as Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados desde a Conceção e por Defeito* (Versão 2.0), de 20 de outubro de 2020, do CEPD – Comité Europeu para Proteção de Dados <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_pt>.

Consequentemente, "O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo [Princípio da] («responsabilidade»)." [*proactiva*[7], ou *accountability*] (Art.º 5.º n.º 2).

2. Uma omissão… voluntária, as regras de segurança

É necessário ter presente que do *RGPD* não consta a previsão de serem aprovadas quaisquer normas de segurança vinculativas, cuja observância seria auditada pelas Autoridades nacionais[8]. Apenas são enunciados padrões genéricos, as, denominadas, "medidas técnicas e organizativas adequadas", a serem determinados em função de critérios casuísticos, resultantes de análises de risco (Art.ºs 25.º n.ºs 1 e 2 e 32.º n.º 1), ou, como referimos, estando preenchidos os correspondentes pressupostos de avaliações de impacto (Art.º 35.º).

---

7 Como a designa a versão em língua espanhola do *RGPD*, de modo a distingui-la das responsabilidades civil (Art.º 82.º), contraordenacional (Art.º 83.º) e, ainda, penal (Art.º 84.º, esta em termos de abertura aos Estados-membros da UE, a qual foi aproveitada por Portugal com os Art.ºs 46.º a 54.º da Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados <https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982>, habitualmente designada como "Lei de Execução", dando seguimento a uma via aberta pela Lei n.º 3/73, de 5 de abril, aprova várias medidas respeitantes à proteção da intimidade da vida privada <https://diariodarepublica.pt/dr/detalhe/lei/3-1973-675640>, a qual esteve na origem da criminalização da "Devassa por meio da informática" (Art.º 193.º) pelo *Código Penal* de 1985, o qual foi, muito recentemente, revogado e substituído pela "Devassa através de meio de comunicação social, da Internet ou de outros meios de difusão pública generalizada", por força da Lei n.º 26/2023, de 30 de maio <https://diariodarepublica.pt/dr/detalhe/lei/26-2023-213706993>.

8 No que se afasta do regime determinado pela Diretiva *ePrivacy* (concretamente, do Art.º 4.º da 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 sector das comunicações eletrónicas, alterada pela Diretiva 2009/136/CE, de 25 de novembro de 2009 <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02002L0058-20091219>, transposta pelo Art.º 3.º da Lei n.º 46/2012, de 29 de agosto, alterando a Lei n.º 41/2004, de 18 de agosto <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2004-106523049>), conforme ao qual a Comissão [Europeia] está habilitada a adotar "normas técnicas de execução"; assim como no que se refere ao Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32014R0910>, o qual atribui-lhe poderes para aprovar normas em múltiplos aspetos dos regimes através de atos de execução e de atos delegados; sem esquecer o Regulamento de Execução (UE) 2018/151 da Comissão, de 30 de janeiro de 2018, que estabelece normas de execução da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho no respeitante à especificação pormenorizada dos elementos a ter em conta pelos prestadores de serviços digitais na gestão dos riscos que se colocam à segurança das redes e dos sistemas de informação, bem como à especificação pormenorizada dos parâmetros para determinar se o impacto de um incidente é substancial <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R0151>.

Com efeito, o Regulamento limita-se enunciar que tais medidas devem "[…] assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado: […] 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; [dispondo ainda de] d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento." (Art.º 32.º n.º 1).

Aliás, mesmo ao remeter para a adoção de esquemas autorregulatórios, como os códigos de conduta (Art.os 40.º e 41.º)[9] ou a certificação (Art.os 42.º e 43.º)[10], evidenciou também que, se o seu acatamento "[…] pode ser utilizado como elemento para demonstrar o cumprimento das obrigações […]" (Art.º 32.º n.º 3), o mesmo não exime de eventuais responsabilidades, só as graduando (Art.º 83.º n.º 2 d)), e só no referente à responsabilidade contraordenacional. Embora, o mesmo critério possa também relevar para a determinação judicial das responsabilidades civil e penal, modulando a culpa.

Apenas assim não ocorre, quando, com base numa regra excecional habilitante do Regulamento (Art.º 9.º n.º 4), a nossa *Lei de Execução* determina que "as medidas e os requisitos técnicos mínimos de segurança inerentes ao tratamento de ["dados de saúde" e de "dados genéticos", "categorias especiais de dados", ou dados sensíveis, definidos no Art.º 4.º 15) e 13), respetivamente] são aprovados por portaria dos membros do Governo responsáveis pelas áreas da saúde e da justiça […]" (Art.º 29.º n.º 7)[11]. Embora não sejam os destinatários mais principais desta previsão, os Municípios e as

---

9 Sobre a função destes, temos as *Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679* (Versão 2.0), de 4 de junho de 2019, do CEPD <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_pt.pdf>.

10 A cujo propósito, o CEPD aprovou as *Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento* (Versão 3.0), de 4 de junho de 2019 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf>.

11 O tratamento destas categorias especiais de dados é também regido pela Lei n.º 12/2005, de 26 de janeiro, sobre informação genética pessoal e informação de saúde <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2005-106603593>, regulamentada pelo Decreto-Lei n.º 131/2014, de 29 de agosto <https://diariodarepublica.pt/dr/detalhe/decreto-lei/131-2014-56384883>, assim como pela Lei n.º 95/2019, de 4 de setembro, a *Lei de Bases da Saúde* <https://diariodarepublica.pt/dr/detalhe/lei/95-2019-124417108>; no entanto, estes diplomas não preveem regras sobre a segurança dos dados e a referida portaria ainda não foi publicada, passados 4 anos sobre a entrada em vigor da *Lei de Execução*.

Freguesias, atendendo às respetivas atribuições, estarão também abrangidos por estas regras[12].

2.1. Os referenciais possíveis para uma densificação

Ainda que apenas vinculantes para a Administração direta do Estado, e de um modo reflexo para a indireta, as normas técnicas detalhadas constantes da Resolução do Conselho de Ministros n.º 41/2018, de 28 de março[13], dando andamento à respetiva adequação ao *RGPD*, podem servir como parâmetros. Aliás, os Municípios e as Freguesias deveriam ter recebido estas normas através de atos próprios, ficando alinhadas com o Estado. Pelo menos, sempre que a respetiva escala comporte meios operativos suscetíveis de as implementar efetivamente.

Do mesmo modo, as novas normas técnicas *ISO/IEC 27001:2022* (Sistemas de gestão da segurança da informação) e *ISO/IEC 27002:2022* (Segurança da informação – cibersegurança – privacidade), devidamente complementadas pela norma *ISO/IEC 27701:2019* (Técnicas de segurança - Extensão das normas ISO/IEC 27001 e da ISO/IEC 27002 para gestão da proteção de privacidade – orientações e diretrizes)[14], podem desempenhar esse mesmo papel de referência, sobretudo se no âmbito de procedimentos de certificação. Embora, nunca devamos esquecer que o seu exato cumprimento não exime os responsáveis pelo tratamento das respetivas responsabilidades, mormente das de natureza civil ou criminal, a serem sempre determinadas por decisões dos tribunais e não pela CNPD.

---

12 O tratamento destas categorias especiais de dados é também regido pela Lei n.º 12/2005, de 26 de janeiro, tal como pela Lei n.º 26/2016, de 22 de agosto, sobre informação genética pessoal e informação de saúde <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2005-106603593> e <https://diariodarepublica.pt/dr/detalhe/lei/26-2016-75177807>, regulamentada pelo Decreto-Lei n.º 131/2014, de 29 de agosto <https://diariodarepublica.pt/dr/detalhe/decreto-lei/131-2014-56384883>, assim como pela Lei n.º 95/2019, de 4 de setembro, a *Lei de Bases da Saúde* <https://diariodarepublica.pt/dr/detalhe/lei/95-2019-124417108>; no entanto, estes diplomas não preveem regras sobre a segurança dos dados e a referida portaria ainda não foi publicada, passados 4 anos sobre a entrada em vigor da *Lei de Execução*.

13 Com efeito, a Resolução do Conselho de Ministros n.º 41/2018, de 28 de março, define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais <https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/41-2018-114937034>, só é vinculativa para a Administração direta, sendo apenas recomendada para a indireta e para o setor empresarial do Estado.

14 Para mais informações a propósito destas normas e acesso, pago, às mesmas, vejam-se as seguintes páginas da ISO – a Organização Internacional de Normalização: <https://www.iso.org/standard/27001>, <https://www.iso.org/standard/75652.html> e <https://www.iso.org/standard/71670.html>.

Quanto a estas questões, cabe ainda referir a muito recente aprovação, pela CNPD, da Diretriz/2023/1, de 10 de janeiro, sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais. Esta, tem por base a sua atribuição quanto a "Promove[r] a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações nos termos do presente regulamento" (Art.º 57.º n.º 1 d)), e na qual a nossa Autoridade enumera um conjunto genérico de boas práticas. No entanto, em linha com o antes explicitado, tais medidas não têm um caráter vinculativo… salvo para a própria CNPD ao avaliar a adequação das ações dos responsáveis pelo tratamento e dos subcontratantes (Art.os 32.º a 34.º e 83.º n.os 2 d) e 4 a)), por força do Princípio da boa-fé, ao qual está vinculada enquanto autoridade administrativa independente[15]. Por outras palavras, não de trata de uma "diretriz", em qualquer aceção do termo, nem poderia jamais relevar em atenção ao seu conteúdo, o qual muito pouco ou nada acrescenta ao já previsto pelo *RGPD*.

2.2. As normas no domínio da cibersegurança

Por outro lado, embora não devendo ser confundidas com as pertinentes ao nosso objeto, temos as regras aplicáveis à segurança do ciberespaço. Porém, as mesmas, relevando para a segurança dos sistemas informáticos, permitem também limitar os riscos e os danos relativamente aos conteúdos qualificáveis enquanto dados pessoais.

Assim, enquanto não dispusermos de um "sistema europeu de certificação" aplicável[16], relevarão os diversos regimes relativos à aprovação de normas em matéria de cibersegurança, por via legislativa ou regulamentar nacional. Designadamente, o *Regime Jurídico da Segurança no Ciberespaço*[17], transpondo a *Diretiva* [*NIS*]*SRI* [1][18],

---

15 Nos termos dos Art.os 10.º e 2.º n.º 4 a) do *Código do Procedimento Administrativo*, aprovado pelo Decreto-Lei n.º 4/2015, de 7 de janeiro <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2015-105602322>, aplicável por força do disposto no Art.º 4.º n.º 1 da *Lei de Execução*.

16 Conforme ao previsto, sobretudo, nos Art.os 51.º e 52.º do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (*Regulamento Cibersegurança*) <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32019R0881>.

17 Lei n.º 46/2018, de 13 de agosto <https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384>.

18 A Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União < https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016L1148>, a qual deverá ser atualizada até 17 de outubro de 2024, por força do Art.º 41.º n.º 1 da Diretiva (UE) 2022/2555 do Parlamento Europeu e do

prevê a definição de requisitos de segurança, através de "legislação própria" (Art.º 12.º n.º 1).

No entanto, é necessário ter na devida conta que, "Os requisitos de segurança são definidos de forma a permitir a utilização de normas e especificações técnicas internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação […]" (Art.º 12.º n.º 3), o que nos remete, implicitamente, para as normas ISO/IEC e não para outras, escolhidas arbitrária ou discricionariamente pelo Governo ou pela Administração Pública[19].

3. As "medidas técnicas e organizativas adequadas"[20]

Sendo certo que no *RGPD* apenas estão, explicitamente, previstas a "pseudonimização e a cifragem dos dados pessoais" (Art.º 32.º n.º 1 a)), cumpre ampliar o nosso campo de análise, sempre sem sair do próprio Regulamento. O que faremos em seguida.

Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva NIS / SRI 2) <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022L2555>.

19 O que não teve as devidas consequências por força da "abertura" constante com o Decreto-Lei n.º 65/2021, de 30 de julho <https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988>, o qual regulamentou o *Regime Jurídico da Segurança do Ciberespaço*, designadamente no que se refere aos conteúdos do *Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança* <https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf>, assim como do QNRCS – *Quadro Nacional de Referência para a Cibersegurança* <https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf>, especificado através do *Quadro de Avaliação de Capacidades de Cibersegurança* <https://www.cncs.gov.pt/docs/cncs-quadrodeavaliacao.pdf>, todos aprovados pelo Centro Nacional de Cibersegurança com base nos poderes regulamentares previsto no Art.º 10.º n.º 10 do antes referido Decreto-Lei, os quais, porventura, estarão mais próximos do *Cybersecurity Framework* do NIST – *National Institute of Standards and Technology*, dos Estados Unidos da América <https://www.nist.gov/cybersecurity>, questões estas sobre as quais não nos teremos por extravasarem manifestamente o nosso objeto, embora não as devêssemos omitir.

20 A este propósito e apenas enquanto referencial de boas práticas, a ENISA – Agência da União Europeia para a Cibersegurança publicou, logo em dezembro de 2017, um *Handbook on Security of Personal Data Processing* <https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing>; no mesmo e em termos sucintos, ainda que relativamente detalhados, enunciou os principais riscos e medidas a serem efetivadas em cada âmbito das organizações, não distinguindo entre os Setores Público e Privado; entretanto, em início de 2022, a ENISA avançou para uma perspetivação mais transversal das questões e das medidas técnicas e organizativas, em especial no que se refere às PET – Tecnologias de Reforço da Privacidade, com uma publicação sobre *Data Protection Engineering* <https://www.enisa.europa.eu/publications/data-protection-engineering>.

3.1. Um critério básico para o tratamento, a "minimização"

Assim e em primeiro lugar, embora tenda a ser pouco referida neste contexto, a minimização está subjacente a toda a disciplina. Inclusive, sendo qualificada como um Princípio, o da «minimização dos dados», os quais devem ser "Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados" (Art.º 5.º n.º 1 c)).

O que ocorre também na sua dimensão temporal, ainda que a mesma tenha sido autonomizada no Princípio da «limitação da conservação», devendo ser "Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados […]" (Art.º 5.º n.º 1 e))[21].

Aliás, a conexão entre a Segurança e estes Princípios é posta pelo Legislador em termos explícitos, ao preconizar que "[…] o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas […] destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização." (Art.º 25.º n.º 1)[22].

Regra depois especificada a propósito das várias dimensões antes enunciadas, determinando que "O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, [igualmente] por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares." (Art.º 25.º n.º 2).

---

21 Como esclareceu recentemente o TJUE – Tribunal de Justiça da União Europeia, no seu Acórdão de 20 de outubro de 2022, proferido no Processo C-77/21 - *Digi* <https://curia.europa.eu/juris/liste.jsf?num=C-77/21>.

22 Como também resulta, explicitamente, do *Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados desde a Conceção e por Defeito*, do CEPD, cit.; tendo também interesse as considerações constantes das *Diretrizes 2/2019 sobre o tratamento de dados pessoais ao abrigo do artigo 6.º, n.º 1, alínea b), do RGPD no contexto da prestação de serviços em linha aos titulares dos dados* (Versão 2.0), de 16 de outubro <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_pt.pdf>, igualmente do CEPD.

Aliás, o mesmo ocorre a propósito das "regras vinculativas aplicáveis às empresas" nas transferências de dados pessoais para países terceiros ou organizações internacionais (Art.º 47.º n.º 2 d)) ou do "[…] tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos […]" (Art.º 89.º n.º 1).

Em qualquer caso, é evidente a redução dos riscos e das correspondentes responsabilidades, incluindo os ligados à Segurança, se estes Princípios forem estritamente observados.

3.2. Uma medida… arriscada, a "anonimização"[23]

Quanto a esta, o critério é o da não associação, originária ou provocada, a identificadores. Com efeito, cumpre recordar que "[…] é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular" (Art.º 4.º 1))[24].

Porém, o *RGPD* não considera a anonimização como uma medida destinada a garantir a segurança dos dados pessoais, inclusive em termos explícitos. Consequentemente, "[…] Os princípios da proteção de dados [melhor dizendo, o regime jurídico na sua integridade] não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não

---

23 Quanto a esta, bem como às PET passíveis de constituir uma alternativa à anonimização, mesmo se menos eficaz, tem um especial interesse o estudo da ENISA sobre *Data Protection Engineering*, antes indicado, assim como o da OCDE – Organização para a Cooperação e Desenvolvimento Económico, já de 2023, sobre *Emerging privacy-enhancing technologies. Current regulatory and policy approaches* <https://www.oecd.org/publications/emerging-privacy-enhancing-technologies-bf121be4-en.htm>.

24 Incluindo os quase-identificadores e os metadados [isto é, os dados sobre dados], até porque "As pessoas singulares podem ser associadas a identificadores por via eletrónica [e] Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares.", nos termos do *Considerando* (30) do *RGPD* e ficou patente nos fundamentos do Acórdão de 19 de outubro de 2016, Processo C-582/14, *Breyer*, do TJUE <https://curia.europa.eu/juris/liste.jsf?num=C-582/14>.

seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação." (*Considerando* (26), *in fine*)" [25].

A este respeito, é ainda mais explícito o *Regulamento sobre os dados não pessoais*[26], o qual, além de distinguir "dados pessoais" de "dados não pessoais" e de restringir a sua aplicação a estes, incluindo as situações em que ambos "estejam indissociavelmente ligados", reitera a imperatividade dos regimes de proteção dos dados pessoais (Art.os 2.º n.º 2 e 3.º n.º 1)). No entanto e simultaneamente, evidencia como "A internet das coisas, a inteligência artificial e a aprendizagem automática, que estão em expansão, representam grandes fontes de dados não pessoais, por exemplo, em consequência da sua utilização em processos automatizados de produção industrial. Exemplos concretos de dados não pessoais incluem conjuntos de dados agregados e anonimizados utilizados para a análise de grandes volumes de dados [e termina concluindo que] Se os progressos tecnológicos permitirem transformar dados anonimizados em dados pessoais, esses dados devem ser tratados como dados pessoais, e o Regulamento (UE) 2016/679 deve ser aplicado em conformidade." (*Considerando* (9)).

O que ocorre com a disponibilização, cada vez mais ampla, de ferramentas de IA – Inteligência Artificial agindo sobre megadados [*Big Data*], como tem sido também mostrado institucionalmente[27], incluindo as ferramentas tecnológicas à disposição de "terceiros", na aceção do Art.º 4.º 10)[28].

---

25 Enquanto, a Comissão Europeia, nas suas *Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados não pessoais na União Europeia* (COM(2019) 250 final, de 29 de maio), reiterou que "se determinados dados não pessoais puderem ser associados a uma pessoa de qualquer forma, tornando-os direta ou indiretamente identificáveis, devem ser considerados dados pessoais [designadamente] quando a evolução da tecnologia e da análise de dados torna possível a conversão de dados anonimizados em dados pessoais" <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52019DC0250>, dando seguimento ao teor deste *Considerando*.

26 Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1807>.

27 Neste sentido, com uma assertividade crescente, foi-se pronunciando o Grupo de Trabalho do Artigo 29.º - GT 29 (Atual CEPD), no *Parecer n.º 7/2003*, de 12 de dezembro, *sobre a reutilização de informações do setor público e a proteção dos dados pessoais - Estabelecer um equilíbrio* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp83_pt.pdf>, seguido do *Parecer n.º 6/2013*, de 5 de junho, *sobre dados abertos e reutilização de informações do setor público (ISP)* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_pt.pdf>, e sobretudo, no *Parecer n.º 5/2014*, de 10 de abril, *sobre as técnicas de anonimização* <https://ec.europa.eu/justice/article-29/documentation/opinion-

Assim, sempre que a tecnologia permitir uma identificação, ou reidentificação, ainda que potencial, pois o critério é de ser uma pessoa "identificável" (Art.º 4.º 1)), serão de aplicar os regimes constantes do *RGPD* e o "responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo ([conforme ao Princípio da] «responsabilidade»)" (Art.º 5.º n.º 2, retomado no 24.º n.º 1), cabendo-lhe os riscos de desenvolvimento que resultem do tratamento de tais dados.

O que, no mínimo, impõe reavaliações cíclicas dos riscos inerentes a cada procedimento de anonimização, por parte dos responsáveis pelo tratamento, até com sucessivas avaliações de impacto, designadamente quando estiverem em causa "novas tecnologias", em especial as resultantes do desenvolvimento da IA (Art.º 35.º n.º 1).

Por isso mesmo, a nova *Diretiva relativa aos dados abertos e à reutilização de informações do setor público*[29] procura efetivar a robustez das anonimizações nos seus âmbitos de aplicação, começando por defini-la como "o processo de transformar documentos em documentos anónimos que não digam respeito a uma pessoa singular identificada ou identificável, ou o processo de tornar anónimos os dados pessoais, por forma a que a pessoa em causa não seja ou deixe de ser identificável." (Art.º 2.º 7))[30] [31].

---

recommendation/files/2014/wp216_pt.pdf>; mais recentemente, a AEPD - Autoridade Europeia para a Proteção de Dados e a *Agencia Española de Protección de Datos* produziram um documento conjunto sobre os *10 misunderstandings related to anonymisation*, no qual intentam mostrar tanto as vantagens quanto as limitações desta técnica <https://edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en>, estando o mesmo apenas disponível nas línguas inglesa e castelhana.

28 Ou seja, "a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais"; como resulta também do Acórdão proferido pelo TJUE no Processo T-557/20 - CUR/AEPD, de 26 de abril de 2023 <https://curia.europa.eu/juris/liste.jsf?language=pt&td=ALL&num=T-557/20>.

29 Por extenso, a Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informações do setor público <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32019L1024>; para cujo texto final em muito contribuiu o Parecer n.º 5/2018, sobre a proposta de reformulação da Diretiva relativa à reutilização de Informações do Setor Público (ISP), de 10 de julho, da AEPD (Autoridade Europeia para a Proteção de Dados), enfatizando a importância da anonimização neste domínio, o qual só está disponível na íntegra em língua inglesa <https://edps.europa.eu/sites/edp/files/publication/18-07-11_psi_directive_opinion_en.pdf>, embora tenha sido publicada uma síntese em português <https://edps.europa.eu/sites/default/files/publication/18-07-10_psi_directive_opinion_summary_pt.pdf>.

30 Como enuncia o respetivo *Considerando* (52), "[…] a reutilização de dados pessoais só é admissível se for respeitado o princípio da limitação da finalidade estabelecido no artigo 5.º, n.º 1, alínea b, e no artigo 6.º, do Regulamento (UE) 2016/679 [o *RGPD*]. Por «informações anónimas» entende-se quaisquer informações que não digam respeito a uma pessoa singular identificada ou identificável, ou que se refiram a dados pessoais tornados anónimos, por forma a que a pessoa em causa não seja ou deixe de ser identificável. A anonimização das informações é uma forma de conciliar o interesse em tornar as informações do setor público tão reutilizáveis quanto possível com as obrigações decorrentes do direito

Por sua vez, o novo *Regulamento Governação dos Dados* reforça o papel da anonimização, sempre a propósito da "reutilização de determinadas categorias de dados protegidos detidos por organismos do setor público", para lá dos abrangidos pela Diretiva (UE) 2019/1024[32]. Para tanto e além de sublinhar os riscos envolvidos[33], prevê que "os organismos do setor público asseguram, em conformidade com o direito da União e nacional, que a natureza protegida dos dados seja preservada [para o que,] Podem [melhor dizendo, devem] estabelecer os seguintes requisitos: a) O acesso para fins de reutilização de dados só deve ser concedido se o organismo do setor público ou o organismo competente, na sequência de um pedido de reutilização, tiver assegurado que os dados: i) foram anonimizados, no caso dos dados pessoais" (Art.º 5.º).

---

em matéria de proteção de dados, mas acarreta custos. É conveniente considerar esses custos como um dos elementos que contribuem para o cálculo do custo marginal de divulgação, na aceção da presente diretiva".

31 Esta Diretiva foi transposta pela Lei n.º 68/2021, de 26 de agosto, que também aprovou os princípios gerais em matéria de dados abertos, alterando a Lei n.º 26/2016, de 22 de agosto, a qual foi republicada <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2021-170221049>, também definindo a «anonimização» como "o processo de transformar informações, dados ou documentos, qualquer que seja a sua forma ou formato, de modo a que não possam revelar pessoa singular identificada ou identificável neles referida, ou o processo de tornar anónimos os dados pessoais, por forma a que a pessoa em causa não seja ou deixe de ser identificável" (Art.º 3.º n.º 1 h)) e restringindo fortemente a reutilização dos documentos nominativos não anonimizados, além de prever a cobrança de taxas relativas a tais operações (Art.os 19.º n.º 11, 20.º c), 23.º-A n.º 1 e 14.º n.º 1 c)).

32 O 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 (*Regulamento Governação de Dados*) <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022R0868>, no qual a "«Reutilização» [é definida como] a utilização, por pessoas singulares ou coletivas, de dados detidos por organismos do setor público, realizada para fins comerciais ou não comerciais que não correspondem à finalidade inicial da missão de serviço público para a qual os dados foram produzidos, excetuando o intercâmbio de dados entre organismos do setor público exclusivamente no desempenho das suas missões de serviço público." (Art.º 2.º 2)); sendo uma disciplina também resultante do contributo do Parecer conjunto 3/2021 do CEPD e da AEPD sobre a proposta de Regulamento do Parlamento Europeu e do Conselho relativo à governação de dados (Regulamento Governação de Dados), de 11 de março <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_pt>, produzido durante o correspondente processo legislativo.

33 Assim, os *Considerandos* (7) e (8) e (9), respetivamente, dão conta que "Existem técnicas que permitem análises em bases de dados que contêm dados pessoais, tais como a anonimização, a privacidade diferencial, a generalização, a supressão e a aleatorização, a utilização de dados sintéticos ou similares e de outros métodos avançados de preservação da privacidade que poderão contribuir para um tratamento de dados mais favorável à privacidade. Os Estados-Membros deverão prestar apoio aos organismos do setor público para que utilizem da melhor forma essas técnicas e, consequentemente, disponibilizem para partilha o máximo possível de dados. [Em qualquer caso,] A reidentificação dos titulares dos dados a partir de conjuntos de dados anonimizados deverá ser proibida. Tal proibição deverá aplicar-se sem prejuízo da possibilidade de realizar investigação sobre técnicas de anonimização, em especial para garantir a segurança da informação, melhorar as técnicas de anonimização existentes e contribuir para a robustez geral da anonimização, em conformidade com o Regulamento (UE) 2016/679.".

Adicionalmente, "[…] O organismo do setor público reserva-se o direito de verificar o processo, os meios e quaisquer resultados do tratamento de dados efetuado pelo reutilizador para preservar a integridade da proteção dos dados e reserva-se o direito de proibir a utilização de resultados que contenham informações que comprometam os direitos e interesses de terceiros. […]" e "[…] Os reutilizadores ficam proibidos de reidentificar qualquer titular dos dados a quem os dados digam respeito e devem tomar medidas técnicas e operacionais para prevenir a reidentificação e para notificar ao organismo do setor público qualquer violação de dados que resulte na reidentificação dos titulares dos dados em causa. […]" (Art.º 5.º n.os 4 e 5).

Para terminar, cumpre não esquecer que a própria anonimização é uma das "operações tratamento", sendo apenas lícita se estiver presente algum dos fundamentos previstos e for realizada através das "[…] medidas técnicas adequadas […] destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento […]", no contexto da proteção de dados desde a conceção, incluindo avaliações de impacto prévias, sempre que necessário (Art.os 4.º 2), 6.º, 9.º, 25.º n.º 1 e 35.º n.º 1 do *RGPD, designadamente*).

3.3. Uma medida menos eficaz, a "pseudonimização"[34]

Neste caso, temos uma definição normativa, consistindo no: "[…] tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;" (Art.º 4.º 5)).

E, além de ser, reiteradamente, sugerida pelo Regulamento em sede de *Considerandos*[35] e surgir qualificada como constituindo uma "[…] medida técnica

34 A propósito da operacionalização desta, ainda que centrado num dos setores no qual é mais comum, até necessariamente, o da saúde, a ENISA publicou o estudo *Deploying Pseudonymisation Techniques*, em março de 2022 <https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques>.
35 Assim, nos *Considerandos* (28), (29), (75), (78), (85) ou (156), designadamente nos dois primeiros temos que "A aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento e os seus subcontratantes a cumprir as suas obrigações de proteção de dados. A introdução explícita da «pseudonimização» no presente regulamento

adequada para assegurar um nível de segurança adequado ao risco […]" (Art.º 32.º n.º 1 a)), constitui "o exemplo" de entre as "[…] medidas técnicas […] adequadas […] destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento […]", no contexto da proteção de dados desde a conceção (Art.º 25.º n.º 1), sendo ainda a sua especificação remetida para os "códigos de conduta" (Art.º 40.º n.º 2 d)).

Mas, "o problema" está em a reidentificação dos titulares dos dados ser ainda mais fácil tecnicamente que com a anonimização. Neste caso, a mesma poderá resultar não só com base nas analíticas de *Big Data*, mas também por outras vias, como as correlações internas aos registos, a notícias de jornal, ao acesso a dados de tráfego ou a registos de operações de cartões de crédito, bem como pela reversão dos pseudónimos através de força bruta computacional, com ou sem a utilização de ferramentas de IA[36].

Daí, a preocupação manifesta do Legislador com os riscos inerentes à "inversão não autorizada da pseudonimização"[37]. O que exige, ou torna muito aconselhável, uma pseudonimização forte, incluindo a dos quase-identificadores, já próxima das técnicas de cifragem.

Porém, a pseudonimização pode constituir a única medida técnica disponível, sobretudo quando for inviável a anonimização dos dados, como ocorre com os arquivos,

---

não se destina a excluir eventuais outras medidas de proteção de dados." e "A fim de criar incentivos para aplicar a pseudonimização durante o tratamento de dados pessoais, deverá ser possível tomar medidas de pseudonimização, permitindo-se simultaneamente uma análise geral, no âmbito do mesmo responsável pelo tratamento quando este tiver tomado as medidas técnicas e organizativas necessárias para assegurar, relativamente ao tratamento em questão, a aplicação do presente regulamento e a conservação em separado das informações adicionais que permitem atribuir os dados pessoais a um titular de dados específico. O responsável pelo tratamento que tratar os dados pessoais deverá indicar as pessoas autorizadas no âmbito do mesmo responsável pelo tratamento".

36 Aliás, estas limitações da pseudonimização já constavam, amplamente, do *Parecer n.º 5/2014*, do GT 29, *sobre as técnicas de anonimização*, antes referido.

37 Especificamente, ao alertar para o facto de "[…] Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. [e] Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. […]", tal como enuncia o *Considerando* (26).

uma realidade de especial relevância para as Autarquias Locais[38]. O mesmo ocorre quanto à "reutilização de determinadas categorias de dados protegidos detidos por organismos do setor público", no *Regulamento Governação dos Dados*, o qual admite também o recurso à pseudonimização[39], embora com cautelas[40].

Por último, como clarificou o Tribunal de Justiça[41], é preciso acentuar que os dados não são univocamente anonimizados ou pseudonimizados, dependendo sempre das informações licitamente à disposição do responsável pelo tratamento ou de um terceiro. O mesmo podendo afirmar-se a propósito do subcontratante.

---

38 Neste caso e como resulta do *RGPD*, "O tratamento […] está sujeito a garantias adequadas, nos termos do presente regulamento, para os direitos e liberdades do titular dos dados. Essas garantias asseguram a adoção de medidas técnicas e organizativas a fim de assegurar, nomeadamente, o respeito do princípio da minimização dos dados. Essas medidas podem incluir a pseudonimização, desde que os fins visados possam ser atingidos desse modo. Sempre que esses fins possam ser atingidos por novos tratamentos que não permitam, ou já não permitam, a identificação dos titulares dos dados, os referidos fins são atingidos desse modo." (Art.º 89.º n.º 1).

39 Especificamente, no *Considerando* (15) é explicitado que "[…] Nos casos em que o fornecimento de dados anonimizados ou alterados não responda às necessidades do reutilizador, sob reserva de terem sido cumpridos todos os requisitos para a realização de uma avaliação de impacto em matéria de proteção de dados e a consulta da autoridade de controlo, nos termos dos artigos 35.º e 36.º do Regulamento (UE) 2016/679 [o *RGPD*], e os riscos para os direitos e interesses dos titulares dos dados tenham sido considerados mínimos, poderá ser permitida a reutilização dos dados [mas, apenas] nas instalações ou de forma remota num ambiente de tratamento seguro. Tal poderá consistir num mecanismo adequado para a reutilização de dados pseudonimizados. As análises de dados realizadas nesses ambientes de tratamento seguros deverão ser supervisionadas pelo organismo do setor público, a fim de proteger os direitos e interesses de terceiros. […]".

40 Efetivamente e ainda nos termos do *Considerando* (15), "[…] Em especial, os dados pessoais só deverão ser transmitidos a terceiros para reutilização se existir uma base jurídica ao abrigo do direito de proteção de dados que permita essa transmissão. Os dados não pessoais só deverão ser transmitidos se não houver motivos para crer que a combinação de conjuntos de dados não pessoais conduziria à identificação dos titulares dos dados. O mesmo se deverá aplicar aos dados pseudonimizados que mantêm o seu estatuto de dados pessoais. Em caso de reidentificação dos titulares dos dados, a obrigação de notificar essa violação de dados ao organismo do setor público deverá aplicar-se, para além da obrigação de notificar essa violação de dados a uma autoridade de controlo e ao titular dos dados em conformidade com o Regulamento (UE) 2016/679. […]".

41 No recentíssimo Acórdão *CUR/AEPD*, o qual levou até ao limite as considerações já constantes do Acórdão *Breyer*, ambos já referidos.

3.4. A saída que ficou por assumir, a "cifragem"[42]

Antes de mais, cabe acentuar como esta só é referida pelo Regulamento, sem sequer a definir e sempre a par da pseudonimização, a propósito dos tratamentos que não tenham por base o consentimento dos titulares dos dados ou disposições de natureza legislativa limitadoras dos seus direitos e liberdades fundamentais (Art.º 6.º n.º 4 e)) e da segurança no tratamento (Art.º 32.º n.º 1 a)).

Aliás, por si só, apenas surge a propósito da isenção de responsabilidades no caso de ocorrerem incidentes de segurança, sempre que "O responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem." (Art.º 34.º n.º 3 a)).

Embora, devamos acentuar o facto de a "cifragem dos dados pessoais" (Art.º 32.º n.º 1 a)), só por si, não ser bastante para afastar as responsabilidades no respeitante às consequências de incidentes de segurança, por apenas garantir a confidencialidade dos dados, não as respetivas integridade e disponibilidade, nomeadamente quando a cifragem resulta de uma ação maliciosa de terceiros, como nos ataques de *ransomware*, ou os dados forem apagados ou ficarem inacessíveis devido a algum caso fortuito.

Daí, o caráter cumulativo das medidas de segurança previstas, *i.e.*, "A capacidade de assegurar [não só] a confidencialidade, [mas também a] integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;", "A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico", e, ainda, a implementação de "Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento." (Art.º 32.º n.º 1, b), c) e d))

---

42 Sobre esta e logo em novembro de 2013, durante o processo legislativo conducente à adoção do *RGPD*, a ENISA publicou um estudo sobre as *Recommended cryptographic measures - Securing personal data* <https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data>, enquanto os desafios de médio prazo são enfrentados *no Post-Quantum Cryptography: Current state and quantum mitigation* <https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation?v2=1>, de maio de 2021, depois complementado pelo *Post-Quantum Cryptography - Integration study* <https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study?v2=1>, de outubro de 2022.

Ainda assim, a cifragem é aconselhável perante grandes riscos, designadamente perante o "Tratamento de categorias especiais de dados pessoais" (Art.º 9.º), mormente se for identificada como uma medida apropriada na sequência de avaliações de impacto (Art.º 35.º).

Porém, é necessário ter presente as distintas perspetivas das Instituições e das agências da União Europeia perante a cifragem, sobretudo se forte, pelas suas implicações em termos de segurança e de combate à criminalidade organizada e ao terrorismo[43].

Embora, em coerência com a Cultura da UE, os processos legislativos têm resultado em compromissos, como mostram o *Código Europeu das Comunicações Eletrónicas*[44], e a *Diretiva* [*NIS*/] *SRI 2*, enquanto exemplos recentes.

---

43 Em termos muito sintéticos, podemos salientar como o PE – Parlamento Europeu, o CEPD, a AEPD, a FRA – Agência Europeia para os Direitos Fundamentais e ainda a ENISA – Agência da União Europeia para a Cibersegurança a defendem, desde logo, com a *Resolução sobre a luta contra a cibercriminalidade*, do PE, de 3 de outubro de 2017 (2017/2068(INI) <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52017IP0366>, seguida pela *Declaração sobre a cifragem e o seu impacto na proteção dos indivíduos relativamente ao tratamento dos seus dados pessoais na UE*, ainda do GT 29, de 11 de abril de 2018 <https://ec.europa.eu/newsroom/article29/items/622229/en>, os Relatórios sobre Direitos Fundamentais, da FRA, sobretudo de 2017 e de 2018 <http://fra.europa.eu/pt>, o *Parecer sobre Cifragem – Uma cifragem forte garante a nossa identidade digital*, da ENISA, de dezembro de 2016 <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption>, e a *Declaração Conjunta sobre uma investigação criminal lícita que respeite a proteção dos dados no século XXI*, da Europol – Agência de Polícia da União Europeia e da ENISA, de 20 de maio de 2016, apesar das reservas da Europol <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection>; no outro polo tem estado o Conselho, com a maioria dos Estados-Membros, e também a Europol, concretizadas na Resolução do Conselho sobre a *Encriptação – Segurança através da encriptação e segurança apesar da encriptação*, de 24 de novembro de 2020 <https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/pt/pdf>, e, com um ênfase crescente, nas IOCTA – Avaliações sobre o Crime Organizado na Internet da Europol, desde 2016 <https://www.europol.europa.eu/publications-events/main-reports/iocta-report>; enquanto a Comissão tem tido uma posição ambivalente, embora pendendo para a do Conselho, como mostram a Proposta de Regulamento relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas – *ePrivacy*), (COM(2017) 10 final), de 10 de janeiro de 2017 <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52017PC0010>, a Comunicação Conjunta da Comissão e da Alta Representante da União para os Negócios Estrangeiros e Política de Segurança - *Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE* (JOIN(2017) 450 final), de 13 de setembro de 2017 <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52017JC0450>, e a Comunicação sobre a *Estratégia da UE para a União da Segurança* (COM(2020) 605 final), de 24 de julho de 2020 <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52020DC0605>, ou ainda a Comunicação Conjunta da Comissão e do Alto Representante da União para os Negócios Estrangeiros e Política de Segurança - *Estratégia de Cibersegurança da UE para a Década Digital* (JOIN(2020) 18 final), de 16 de dezembro de 2020 <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52020JC0018>.

44 Estabelecido pela Diretiva (UE) 2018/1972, de 11 de dezembro de 2018 <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018L1972>, como resulta do respetivo Art.º

Em Portugal, esta questão estará *resolvida pela Carta Portuguesa de Direitos Humanos na Era Digital*[45], em cujos termos, "Todos têm 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." (Art.º 8.º n.º 1). Embora se trate de um direito dos titulares dos dados, no mínimo estará presente um dever de não interferência por parte dos responsáveis pelo tratamento, senão mesmo de predisporem os meios técnicos necessários para o efetivar. Além de o *Código Europeu das Comunicações Eletrónicas* e a nova *Lei das Comunicações Eletrónicas*[46], que o transpôs, terem alargado o respetivo âmbito aos serviços OTT (*Over-the-top*) de comunicação bidirecional, isto é, às mensagens de texto e de voz e às chamadas de voz e de vídeo, designadamente no âmbito de redes sociais[47], mesmo que não impliquem a atribuição pública de números conforme aos planos de numeração nacionais e internacional, como exigia a legislação anterior.

40.º n.º 1 e, sobretudo, dos *Considerandos* (96) e (97), a qual foi transposta pela Lei n.º 16/2022, de 16 de agosto, que aprova a *Lei das Comunicações Eletrónicas*, transpondo as Diretivas 98/84/CE, 2002/77/CE e (UE) 2018/1972, alterando as Leis n.os 41/2004, de 18 de agosto e 99/2009, de 4 de setembro, e os Decretos-Leis n.os 151-A/2000, de 20 de julho, e 24/2014, de 14 de fevereiro, e revogando a Lei n.º 5/2004, de 10 de fevereiro, e a Portaria n.º 791/98, de 22 de setembro <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2022-187527517>, relevando para o efeito o disposto no Art.º 59.º n.º 1.

45 Aprovada pela Lei n.º 27/2021, de 17 de maio <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2021-164870244>.

46 Especificamente, o Art.º 2.º 5) do *Código* define como "«Serviço de comunicações interpessoais», o serviço oferecido, em geral mediante remuneração, que permite o intercâmbio interpessoal direto e interativo de informações através de redes de comunicações eletrónicas entre um número finito de pessoas, através do qual as pessoas que participam ou dão início à comunicação determinam o(s) seu(s) destinatário(s) e não inclui serviços que permitem a comunicação interpessoal e interativa que funcionem de modo acessório e que estejam intrinsecamente ligados a outro serviço", assim explicitando o seu âmbito de aplicação, enunciado no Art.º 1.º n.º 1, enquanto a nossa Lei o faz nos Art.os 1.º e 3.º n.º 1 tt), igualmente a propósito do «Serviço de comunicações interpessoais».

47 Como explica o *Considerando* (15) do *Código Europeu das Comunicações Eletrónicas*, "Os serviços utilizados para fins de comunicações, e os meios técnicos usados para prestar esses serviços, evoluíram consideravelmente. Os utilizadores finais trocam cada vez mais a tradicional telefonia vocal, as mensagens de texto (SMS) e os serviços de envio de correio eletrónico por serviços em linha equivalentes em termos de funcionamento, tais como os serviços de voz em IP (VoIP), os serviços de mensagens e os serviços de correio eletrónico baseados na Web (webmail). Para garantir que os utilizadores finais e os seus direitos são eficazmente protegidos e beneficiam da mesma proteção quando utilizam serviços funcionalmente equivalentes, a definição, orientada para o futuro, do conceito de «serviços de comunicações eletrónicas» não deverá basear-se meramente em parâmetros técnicos, mas antes numa abordagem funcional. O âmbito da regulação necessária deverá ser adequado aos seus objetivos de interesse público. Embora o «envio de sinais» continue a ser um importante parâmetro para determinar os serviços abrangidos pelo âmbito de aplicação da presente diretiva, a definição deverá abranger também os outros serviços que permitem a comunicação. Do ponto de vista do utilizador final é irrelevante se é o fornecedor a enviar ele próprio os sinais ou se a comunicação é efetuada através de um serviço de acesso à Internet, […]".

4. Quando a segurança falha, a "violação de dados pessoais"[48]

Antes de tudo o mais, é indispensável evidenciar como, no âmbito do género "incidentes de segurança", o Regulamento ocupa-se apenas de uma espécie, a "«Violação de dados pessoais»: [a qual consiste em] uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (Art.º 4.º 12))[49].

Ora, esta não deve ser confundida, de todo, com a "violação dos direitos" dos titulares dos dados (Art.º 79.º n.º 1) ou com a "violação do [presente] regulamento" (Art.os 77.º n.º 1, 79.º n.º 1, 82.º n.º 1, 83.º ou 84.º), isto é, com quaisquer falhas, no que respeita à sua responsabilidade "proativa", por parte do responsável pelo tratamento dos dados[50].

Aliás, como enunciou repetidamente o CEPD, as situações de destruição, de dano, de perda ou de tratamento não autorizado ou ilícito podem ser enquadradas numa tipologia, consistente na "violação de confidencialidade", na "violação de integridade" ou na "violação de disponibilidade" dos dados, sempre pressupondo atos maliciosos ou casos fortuitos, tanto de origem externa quanto interna.

---

48 Sobre estas questões, é indispensável levar em consideração o disposto nas *Guidelines 9/2022 on personal data breach notification under GDPR* (Versão 2.0), de 28 de março de 2023 [ainda sem uma versão em língua portuguesa] <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_pt>, que sucederam ao *Parecer 03/2014*, de 25 de março, *relativo à notificação da violação de dados pessoais* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_pt.pdf>, e às *Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679*, de 3 de outubro de 2017 / 6 de fevereiro de 2018 <https://ec.europa.eu/newsroom/article29/items/612052/en> ambos ainda do GT 29; entretanto, esclarecidas pelas *Orientações sobre exemplos da notificação de uma violação de dados pessoais* (Versão 2.0), adotadas em 14 de dezembro de 2021 <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_pt>, estas já do CEPD.

49 Porque, "Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo [!?] ou usurpação da 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 significativa das pessoas singulares. […]", como conta do *Considerando* (85).

50 Como ficou demonstrado pelo teor da Deliberação/2021/1569, de 21 de dezembro, da CNPD, a propósito de múltiplos incumprimentos do *RGPD* por parte do Município de Lisboa, entre os quais não esteve a falta de notificação do ocorrido à Comissão, porque não ocorreu qualquer "violação de dados pessoais", contrariamente ao que muitos "comentadores" se apressaram a dizer à Comunicação Social <https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121953>.

Cumpre ainda acrescentar, quanto aos atos maliciosos, inclusive praticados por terceiros, que estaremos ainda perante um tratamento de dados, em sentido próprio, isto é, "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (Art.º 4.º 2)), cuja ilicitude não afasta a aplicação dos princípios e regras constantes do Regulamento. Incorrendo os seus autores nas inerentes responsabilidades, incluindo a responsabilidade civil (Art.º 82.º) e a contraordenacional (Art.º 83.º)[51], pois são qualificáveis como "responsáveis pelo tratamento", por "determina[rem] as finalidades e os meios de tratamento de dados pessoais" (Art.º 4.º 7)).

4.1. O procedimento interno

Em todos os casos, o "responsável pelo tratamento documenta quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à autoridade de controlo verificar o cumprimento do disposto no presente artigo." (Art.º 33.º n.º 5)[52].

Do mesmo modo, o responsável pelo tratamento, ou o subcontratante, deve adotar medidas para reparar os efeitos da violação de dados e "[…] inclusive, se for caso disso […] para atenuar os seus eventuais efeitos negativos" (Art.º 33.º n.º 3 d)).

---

51 Além da responsabilidade penal resultante do, eventual, preenchimento das previsões típicas correspondentes aos crimes de "Acesso indevido" (Art.º 47.º), de "Desvio de dados" (Art.º 48.º), de "Viciação ou destruição de dados" (Art.º 49.º) e ou de "Inserção de dados falsos" (Art.º 50.º), todos da *Lei de Execução*.

52 O que não corresponde apenas a uma especificação do dever geral de registo de todas as operações de tratamento, Art.º 30.º e é explicado pelo *Considerando* (82), "A fim de comprovar a observância do presente regulamento, o responsável pelo tratamento ou o subcontratante deverá conservar registos de atividades de tratamento sob a sua responsabilidade. Os responsáveis pelo tratamento e subcontratantes deverão ser obrigados a cooperar com a autoridade de controlo e a facultar-lhe esses registos, a pedido, para fiscalização dessas operações de tratamento.", pois as operações de tratamento em causa, incluindo "[…] a limitação, o apagamento ou a destruição;" (Art.º 4.º 2)), podem ser imputáveis a terceiros.

O que supõe uma análise dos riscos para "[…] os direitos e liberdades das pessoas singulares. […]" (Art.º 33.º n.º 1), de modo a poder determinar, e se necessário demonstrar, a desnecessidade de notificar a violação de dados à CNPD, quando os mesmos forem nulos ou extremamente reduzidos[53].

Na análise em questão, deve ser imediatamente envolvido o Encarregado da Proteção de Dados (Art.os 38.º n.º 1 e 39.º n.º 1 a) e b) do *RGPD* e Art.º 11.º b) da *Lei de Execução*), o qual terá "[…] em devida consideração os riscos associados […]" (Art.º 39.º n.º 2), desde uma posição de autonomia técnica reforçada (Art.os 38.º n.º 3 do *RGPD* e 9.º n.º 2 da *Lei de Execução*) e atendendo à previsão consistente em ser o "Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento […]" (Art.º 39.º n.º 1 e))[54] [55].

Para a mesma, podem servir de referência os critérios de exclusão da comunicação ao titular dos dados (Art.º 34.º n.º 3 a) e b)), com as devidas adaptações resultantes dos graus de risco, além de não ultrapassar o prazo de notificação à Autoridade, salvo se justificadamente (Art.º 33.º n.º 1). Contudo, esta análise não deve ser confundida com

---

53 Como enuncia o *Considerando* (75), ainda que em termos gerais e prévios a qualquer "violação de dados pessoais", "O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados."; consequentemente, "A probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento de dados. Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado", conforme ao *Considerando* (76).

54 Neste sentido, de um modo explícito, embora sem a aprofundar a questão, as *Orientações sobre os encarregados da proteção de dados (EPD)*, de 13 de dezembro de 2016, com revisão e última redação adotada em 5 de abril de 2017, do GT 29 <https://ec.europa.eu/newsroom/article29/items/612048>.

55 Embora a tal não estejam obrigados, será também aconselhável estabelecer um diálogo a este respeito com o responsável de segurança, obrigatoriamente nomeado por todas as Autarquias Locais, nos termos e para os efeitos previstos no Art.º 5.º do Decreto-Lei n.º 65/2021, de 30 de julho, independentemente de se verificarem os pressupostos constantes do Art.º 15.º do *Regime Jurídico da Segurança do Ciberespaço* e explicitados nos Art.os 11.º a 17.º do Decreto-Lei antes referido.

uma avaliação de impacto sobre a proteção de dados, inclusive atendendo ao momento, aos pressupostos e aos critérios previstos para a mesma (Art.º 35.º)[56].

4.2. A notificação à CNPD e a comunicação aos titulares dos dados

No entanto, se da violação de dados pessoais for suscetível de resultar num risco [mesmo pequeno] para os direitos e liberdades das pessoas singulares, "[…] o responsável pelo tratamento notifica desse facto a autoridade de controlo competente […], sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma […]" (Art.º 33.º n.º 1). No caso de a mesma ter sido identificada por um subcontratante, este deve notificar, melhor dizendo informar, o responsável pelo tratamento, "[…] sem demora injustificada após ter conhecimento […]" da mesma (Art.º 33.º n.º 2), ao caber apenas a este a análise dos riscos envolvidos e a correspondente obrigação de notificar a CNPD.

Da notificação devem constar, "pelo menos [uma descrição da] natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa [, bem como,] o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações [, uma descrição das] consequências prováveis da violação de dados pessoais [e outra das] medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos;" (Art.º 33.º n.º 3). Podendo a mesma ser faseada, quando tal seja justificável, objetivamente (Art.º 33.º n.º 4).

---

56 A este propósito, o *Considerando* (84) enuncia que "A fim de promover o cumprimento do presente regulamento nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco. Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento. […]"; sendo também de sublinhar a relevância das *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679*, de 4 de abril de 2017, revistas e adotadas pela última vez em 4 de outubro de 2017, ainda do GT 29 <https://ec.europa.eu/newsroom/article29/items/611236/en>.

Por seu turno, se "[…] a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada." (Art.º 34.º n.º 1), por iniciativa própria ou por exigência da CNPD (Art.º 34.º n.º 4).

Todavia, esta comunicação não é exigida ao responsável pelo tratamento, inclusivamente pelos altos custos reputacionais eventualmente envolvidos ou para evitar uma perceção de insegurança pública excessiva, se este "[…] tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem;" ou "[…] tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados […] já não é suscetível de se concretizar." (Art.º 34.º n.º 3 a) e b)).

Distinta e eventualmente mais gravosa para o responsável pelo tratamento é a decorrente da desproporcionalidade, ou da inviabilidade material, de comunicar a violação a todos os titulares dos dados cujos direitos e liberdades tenham ficado em risco com a violação, caso em que "[…] é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz." (Art.º 34.º n.º 3 c)).

4.3. As outras comunicações legalmente devidas

No que se refere às violações de dados pessoais em sistemas informáticos no Poder Local, à notificação à CNPD junta-se o dever de o fazer ao "Centro Nacional de Cibersegurança [quanto aos] incidentes com um impacto relevante na segurança das redes e dos sistemas de informação […]" (Art.º 15.º n.º 1 do *Regime Jurídico da*

Segurança do Ciberespaço). Os pressupostos e os procedimentos desta notificação, constantes deste preceito, são depois detalhados no Decreto-Lei n.º 65/2021[57].

Consequentemente, de acordo com a *Diretiva* [*NIS/*] *SRI*[58] e com o *Regime Jurídico da Segurança do Ciberespaço* (Art.os 12.º e 13.º), estamos perante uma duplicação de deveres de notificar.

Daí também a previsão legal de uma cooperação, ou pelo menos de um diálogo, entre as respetivas autoridades, no nosso caso, entre o Centro Nacional de Cibersegurança e a CNPD, designadamente reportando entre si os incidentes de segurança dos quais tiverem conhecimento. Embora não esteja legalmente previsto qualquer alinhamento regulatório ou de procedimentos[59], até em atenção ao Primado do *RGPD* e à independência garantida por este a cada Autoridade competente (Art.os 51.º a 58.º)[60].

---

57 Especificamente, nos Art.os 11.º a 16.º, relevando também e em especial o *Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança* e o *Quadro de Avaliação de Capacidades de Cibersegurança*, já referidos, bem como e ainda, o Regulamento n.º 183/2022, de 21 de fevereiro, do Centro Nacional de Cibersegurança, o qual aprovou *a Instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes* <https://www.cncs.gov.pt/docs/regulamento-183-2022.pdf>.

58 Nos Art.os 2.º n.º 1 e 15.º n.º 4, tal como clarifica o *Considerando* (63), "Os dados pessoais ficam em muitos casos comprometidos em consequência de incidentes. Neste contexto, as autoridades competentes e as autoridades encarregadas da proteção dos dados deverão cooperar e trocar informações sobre todas as questões pertinentes para combater as eventuais violações de dados pessoais resultantes de incidentes.".

59 Explicitando o Art.º 3.º n.os 3 a) e c) do Decreto-Lei n.º 65/2021 que "O cumprimento dos requisitos de segurança e das obrigações de notificação de incidentes previstos no Regime Jurídico da Segurança do Ciberespaço e no presente decreto-lei não prejudica: a) O cumprimento dos requisitos específicos de segurança e das obrigações específicas de notificação de incidentes nos termos definidos pelas autoridades competentes, nomeadamente […] pela Comissão Nacional de Proteção de Dados (CNPD) […]", não estando esta entre "As entidades referidas no n.º 1 do artigo anterior [as quais] podem estabelecer formas de colaboração com vista ao cumprimento das obrigações em matéria de requisitos de segurança e de notificação de incidentes previstos no Regime Jurídico da Segurança do Ciberespaço, e no presente decreto-lei, numa lógica de partilha de recursos, desde que seja assegurada a efetiva operacionalização das mesmas em cada entidade", o que é confirmado pelo disposto no Art.º 2.º n.º 7 do Decreto-Lei em cujos termos "O disposto na presente lei não prejudica o cumprimento da legislação aplicável em matéria: a) De proteção de dados pessoais, designadamente o disposto no Regulamento (UE) n.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados)".

60 E assim continuará com a *Diretiva* [*NIS/*] *SRI 2*, a partir de 18 de outubro de 2024, como prevê o respetivo Art.º 31.º n.º 2, "Quando tratarem de incidentes que tenham originado violações de dados pessoais, as autoridades competentes devem trabalhar em estreita cooperação com as autoridades de supervisão nos termos do Regulamento (UE) 2016/679, sem prejuízo das competências e funções que incumbem às autoridades de supervisão nos termos desse regulamento", porque, como explica *Considerando* (108), "Os dados pessoais ficam amiúde expostos em consequência de incidentes. Nesse contexto, as entidades competentes deverão cooperar e trocar informações sobre todas as questões pertinentes com as autoridades referidas no Regulamento (UE) 2016/679 […]".

Por último, não deve ser esquecido o dever de denunciar ao Ministério Público os "[…] crimes de que tomarem conhecimento no exercício das suas funções e por causa delas;" que incumbe aos funcionários das Autarquias Locais[61], designadamente dos previstos e punidos pela *Lei de Execução*.

61 Por força do previsto no Art.º 242.º n.º 1 b) do *Código do Processo Penal*, aprovado pelo Decreto-Lei n.º 78/87, de 17 de fevereiro <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1987-34570075>.

Referências:

CORDEIRO, A. Barreto Menezes (Coord.). *Comentário ao Regulamento Geral sobre Proteção de Dados e à Lei n.º 58/2019*. Coimbra: Almedina, 2021, sobretudo pp. 266-279, da autoria de Francisco Rodrigues Rocha.

CORDEIRO, A. Barreto Menezes. *Direito da Proteção de Dados – À luz do RGPD e da Lei n.º 58/2019*. Coimbra: Almedina, 2020, sobretudo pp. 346-352.

MONIZ, Graça Canto. *Manual de Introdução à Proteção de Dados Pessoais*. Coimbra: Almedina, 2023, sobretudo pp. 241-258.

PINHEIRO, Alexandre Sousa (Coord.). *Comentário ao Regulamento Geral sobre Proteção de Dados*. Coimbra: Almedina, 2018, sobretudo pp. 448-457, da autoria de Alexandre Sousa Pinheiro e de Carlos Jorge Gonçalves.

A Responsabilidade Civil dos Prestadores Intermediários de Serviço da Sociedade de Informação em Relação ao Conteúdo Ilícito na União Europeia

MANUEL DA COSTA CABRAL

SUMÁRIO: 1. Introdução; 2. O enquadramento regulamentar vigente para a moderação de conteúdo ilegal; 2.1. Instrumentos jurídicos relativos à moderação de conteúdo ilegal em linha; 2.2. Regulação da moderação de determinados tipos específicos de conteúdo ilegal; 3. As decisões do TJUE e de Tribunais Nacionais; 3.1. C-236/08, C-237/08, C-238/08, de 23/03/2010 (acórdão genericamente conhecido como Google France Vs Louis Vuitton); 3.2. C-234/09, de 12/07/2011 (L'Oreal vs eBay); 3.3. STJ 10-Dez.-2020 (Ferreira Lopes), proc. n.º 44/18.6YHLSB.L1.S2; 3.4. Decisão 7708/19 Reti Televisive Italiane SpA v Yahoo! Inc; 4. O Novo enquadramento regulamentar; 4.1. As limitações do enquadramento atual, em particular da Diretiva 2000 / 31 / CE; 4.2. A "reforma do espaço digital"; 4.3. A noção de conteúdo ilegal ao abrigo do novo Regulamento; 4.4. Os regimes de responsabilidade ao abrigo do Regulamento dos serviços digitais; 4.4.1. Responsabilidade dos prestadores de serviços intermediários; 4.4.2. Investigações voluntárias por iniciativa própria; 4.5. Obrigações de moderação de conteúdo ilícito aplicáveis aos prestadores; 4.5.1. Obrigações aplicáveis a todos os prestadores de serviços intermediários; 4.5.2. Obrigações adicionais aplicáveis aos prestadores de armazenagem em servidor; 4.5.3. Obrigações adicionais aplicáveis aos fornecedores das plataformas em linha; 4.5.4. Obrigações adicionais aplicáveis aos fornecedores de Plataformas em linha de muito grande dimensão e de motores de pesquisa em linha de muito grande dimensão no que se refere à gestão de riscos sistémicos; 5. Considerações finais; 5.1. Reflexões sobre o novo regime de responsabilidade; 5.2. Reflexões sobre as novas obrigações de moderação de conteúdo ilícito; 6. Conclusões; 7. Bibliografia

RESUMO:

O presente artigo aborda a responsabilidade dos intermediários em relação aos conteúdos ilegais na União Europeia. A responsabilidade dos intermediários é uma das questões mais controversas no contexto dos debates mundiais sobre a governação da Internet. A União Europeia tem tentado abordar a questão da responsabilidade dos intermediários desde, pelo menos, 2000, ano em que foi publicada a Diretiva relativa ao comércio eletrónico. Além disso, uma variedade de iniciativas legislativas de âmbito obrigatório e não obrigatório da UE podem também ter implicações na responsabilidade. Vinte e dois anos depois, o Regulamento dos Serviços Digitais (RSA) está prestes a entrar em vigor. Neste sentido, é nosso objetivo analisar os pontos comuns

entre a Diretiva sobre o Comércio Eletrónico e o RSA, bem como as principais inovações deste novo regulamento da UE.

Por último, apresentamos as nossas reflexões sobre o regime de responsabilidade previsto no RSA.

ABSTRACT:

This paper addresses the liability of intermediaries in relation to illegal content in the European Union. The liability of intermediaries is one of the most controversial issues in the context of worldwide Internet Governance discussions. The European Union has been trying to address the liability of intermediaries since at least 2000, when the Directive *on electronic commerce was published. Additionally, a number of mandatory and non-mandatory EU legal initiatives may also have implications on the liability. Twenty-two years later the Digital Services Act (DSA) is about to enter in force. This paper will analyse the commonalities between the Directive on electronic commerce and the DSA and the main innovations of this new EU Regulation.*

Finally, the paper will present reflections concerning the liability regime prescribed in the DSA.

1. Introdução

Na origem da Internet esteve o projeto Arpanet, criado no início dos anos 60, no âmbito de uma investigação norte-americana ligada ao setor da defesa, a ARPA. Porém, cedo os ideais de auto-regulação[1] [2]ou mesmo libertários[3] foram ganhando peso e moldando o crescimento da Internet.

O ciberliberatismo plasmado na "Declaração de Independência do Ciberespaço", de 1996 redigida por John Perry Barlow, influenciou decisivamente a forma como a Internet se foi desenvolvendo e ainda se sente nos nossos dias. A ideia de um espaço cibernético global que se desenvolve em torno da liberdade de expressão, de informação ou de comércio, ao arrepio de interferências dos Governos, não deixa de ter um caráter sedutor. No entanto, hoje de acordo com a União Internacional de Telecomunicações 4,9 mil milhões de pessoas estão conectadas à Internet, o que corresponde a 63% da população mundial[4]. Por seu turno, o Banco Mundial indica-nos que a economia digital representa já 15,5% do PIB Mundial e o seu ritmo de crescimento, nos últimos 15 anos, tem sido duas vezes e meia superior ao crescimento do PIB Mundial[5]. A importância social, cultural, económica e política da Internet foi progressivamente suscitando interrogações sobre o melhor modelo de Governação da Internet[6]. Neste contexto, a responsabilidade civil dos prestadores intermediários de serviço da sociedade de informação é dos temas mais controversos, não apenas na Europa, mas a nível global.

---

1 Rosa, A. M. (1998). Internet: uma história. P.24

2 Machuco Rosa demonstra a importância dos ideais de auto-regulação a partir da obra de Norbert Wiener, "Cybernética: Ou Controle e Comunicação no Animal e na Máquina", de 1948, obra na qual é apresentada a ideologia comunicativa, que "a pouco e pouco, viria a tornar-se dominante em algumas comunidades *on-line"* (Rosa, A.M (1998). Op. Cit.). A ideologia comunicativa parte da premissa que a fala é o caráter humano mais importante, e que existe uma "tendência irresistível para a comunicação". "As máquinas deverão desempenhar um papel central para a remoção de obstáculos à comunicação, e graças às novas máquinas poderemos "participar numa corrente contínua de influência que nos chegam do mundo exterior".

3 Rosa, A. M. (1998). Op. Cit. P. 68

4 Measuring digital development, Facts and Figures 2021, International Telecommunication Union, disponível em https://www.itu.int/itu-d/reports/statistics/facts-figures-2021/

5 Sítio do Banco Mundial, "Digital Development" https://www.worldbank.org/en/topic/digitaldevelopment/overview

6 O conceito de Governação da Internet aqui entendido tal como entendido no ponto 34 da Agenda de Tunes para a Sociedade de Informação: "o desenvolvimento e aplicação de princípios, normas, regras e procedimentos de tomada de decisão, que moldam a evolução e o uso da Internet, por parte dos Governos, setor privado e sociedade civil, no âmbito das suas competências". Tunis Agenda for the Information Society, 2005, disponível em https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

A União Europeia tem vindo frequentemente a ser precursora na definição de um quadro regulamentar sobre esta matéria. Sublinhamos, neste percurso, a importância da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000 relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (Diretiva do Comercio Eletrónico), e da "reforma do espaço digital" apresentada pela Comissão Europeia em dezembro de 2020 e que consistiu, na prática, na apresentação de duas propostas para dois novos Regulamentos: O Regulamento dos Mercados Digitais e do Regulamento dos Serviços Digitais.

O Regulamento dos Serviços Digitais, em particular, apresenta um novo regime de responsabilidade para os prestadores intermediários, que substituirá o regime previsto na Diretiva de Comércio Eletrónico. Veremos que em ambos os casos o legislador comunitário deu prevalência, porventura ainda inspirado pela Declaração de Barlow, à isenção, por defeito, da responsabilidade dos prestadores intermediários. No entanto, esta reforma adiciona um conjunto de medidas aplicáveis a estes prestadores que terão seguramente impacto nas condições necessárias para que a referida isenção de responsabilidade se aplique. Dado o caráter inovador desta reforma estamos em crer que o mesmo terá impacto na União Europeia, e poderá inspirar legisladores noutras latitudes.

O presente trabalho focar-se-á na responsabilidade civil dos prestadores intermediários de serviço da sociedade de informação para a remoção do conteúdo ilícito na União Europeia. Deixar-se-á, assim, de lado a responsabilidade face a conteúdo lesivo ou informações incompatíveis com os termos e condições dos serviços, que à luz do Regulamento dos serviços digitais também poderão ser alvo de políticas de moderação.

Neste contexto, o trabalho seguirá a seguinte estrutura.

Após esta Introdução, o Capítulo 2 abordará o anterior enquadramento regulamentar aplicável à moderação de conteúdo ilegal. Veremos que o *aquis* comunitário compreendia instrumentos jurídicos relativos à moderação de conteúdo ilegal em linha e instrumentos relativos à moderação de determinados tipos específicos de conteúdo ilegal. Iremos identificar, assim, um conjunto de atos legislativos relevantes para essa moderação.

De seguida, no Capítulo 3 abordaremos a jurisprudência resultante deste enquadramento legislativo. Para o efeito, analisaremos dois acórdãos do Tribunal de Justiça da União Europeia e também dois acórdãos dos Tribunais Superiores de Portugal e Itália. De notar que a jurisprudência sobre a responsabilidade dos prestadores intermediários tanto a nível comunitário, como nacional é abundante, pelo que a escolha destes quatro casos se deveu fundamentalmente a critérios de originalidade e relevância dos argumentos invocados e de diferentes pontos de vista defendidos.

No Capítulo 4 iremos referir a já mencionada "reforma do espaço digital", em particular o Regulamento dos Serviços Digitais.

No Capítulo 5 analisaremos as mais impactantes disposições do novo Regulamento suscitam, à luz do objetivo geral do mesmo.

Por fim, o Capítulo 6 contem as conclusões do trabalho.

2. O anterior enquadramento regulamentar para a moderação de conteúdo ilegal

Neste capítulo iremos analisar diversos instrumentos jurídicos, vinculativos e não vinculativos, que foram incluídos no *acquis* comunitário ao longo dos anos visando o combate / moderação do conteúdo ilegal em linha.

Em termos gerais, podemos agrupar tais instrumentos em duas categorias: instrumentos jurídicos relativos à moderação de conteúdo ilegal em linha; instrumentos jurídicos para a moderação de determinados tipos específicos de conteúdo ilegal.

É com base nesta categorização que o presente capítulo se desenvolve.

2.1.Instrumentos jurídicos relativos à moderação de conteúdo ilegal em linha

Instrumentos jurídicos vinculativos

A Diretiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000 relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio electrónico», Doravante DCE) foi, ao longo de vinte anos, a peça basilar do atual

regime da responsabilidade civil dos prestadores de serviço da sociedade de informação na União Europeia. Lembra-nos Sousa e Silva[7] que "quando esta Diretiva foi aprovada não conhecíamos o Facebook, o Youtube, o Whatsapp, o Flickr ou o Uber, e a Netflix e a HBO ainda não ofereciam serviços de streaming". É, de facto, surpreendente que numa área tão dinâmica e basilar das nossas sociedades e economias, a DCE tenha sido a base jurídica para endereçar a questão da responsabilidade das plataformas eletrónicas durante tantos anos, ou como diria Streel[8], o pilar do nosso Mercado Interno.

Importa, assim, debruçamo-nos sobre esta Diretiva, que no ordenamento jurídico nacional foi transposta pelo Decreto-Lei n.º 7/2004, de 7 de janeiro.

Nos considerandos da Diretiva eram invocados os fundamentos deste ato legislativo, sendo referido que o "desenvolvimento dos serviços da sociedade da informação na Comunidade é entravado por um certo número de obstáculos legais ao bom funcionamento do mercado interno (…). Esses obstáculos advêm da divergência das legislações, bem como da insegurança jurídica dos regimes nacionais aplicáveis a esses serviços (….)"[9]. Assim, é considerado que "estes obstáculos devem ser abolidos, através da coordenação de determinadas legislações nacionais e da clarificação, a nível comunitário, de certos conceitos legais, na medida do necessário ao bom funcionamento do mercado interno (…)[10].

Pretendia-se, pois, "garantir a segurança jurídica e a confiança do consumidor"[11] e "criar um enquadramento legal destinado a assegurar a livre circulação dos serviços da sociedade da informação entre os Estados-Membros"[12].

Um ponto prévio relevante, diz respeito à definição de «serviços da sociedade da informação», que é apresentada na DCE por referência ao artigo 1.°, n.º 2, da Diretiva 98/34/CE, de 22 de Junho de 1998[13], que compreendia "qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido

7 Sousa e Silva, N. , *Responsabilidade na Internet: o Ato dos Serviços Digitais garante a liberdade de expressão*, de 10-Fev.-2021
8 de Streel, A., & Husovec, M. (2020). The e-commerce Directive as the cornerstone of the Internal Market. *Available at SSRN 3637961*.
9 Considerando 5 da DCE
10 Considerando 6 da DCE
11 Considerando 7 da DCE
12 Considerando 8 da DCE
13 Diretiva 98/34/CE, de 22 de Junho de 1998, relativa a um procedimento de informação no domínio das normas e regulamentações técnicas, conforme alterada pela Diretiva 98/48/CE, de 20 de Julho de 1998

individual de um destinatário de serviços"[14]. Nos termos do art. 2.º b) da Diretiva 2000/31/CE era considerado "prestador de serviços" "qualquer pessoa, singular ou colectiva, que preste um serviço do âmbito da sociedade da informação". Conforme nos diz Menezes Leitão[15] a definição de prestador de serviço é "propositadamente abrangente, permitindo nela incluir não apenas as operadoras, mas também os próprios cibernautas" que podem circunstancialmente prestar este tipo de serviço.

Esta Diretiva consagrava três níveis de responsabilidade dos prestadores intermediários de serviços, consoante se tratem de prestadores de serviço de simples transporte[16], de armazenagem temporária[17] ou armazenagem em servidor[18].

O princípio geral era o de não responsabilização. Com efeito, estipulava-se, que "os Estados-Membros velarão para que a responsabilidade do prestador do serviço não possa ser invocada". No entanto, eram estabelecidas condições para que este princípio geral se concretize.

Assim, no caso do prestador de serviços de armazenagem em servidor a respetiva responsabilidade não podia ser invocada caso a sua atividade seja "puramente técnica, automática e de natureza passiva", implicando não tenha "conhecimento da informação transmitida ou armazenada, nem o controlo desta" (considerando 42 da DCE). Adicionalmente, a não responsabilização do prestador estava salvaguardada, caso o mesmo venha a ter conhecimento de uma ilicitude, mas "atue com diligência no sentido

---

14 No artigo 1.°, n.º 2, da Diretiva 98/34, na sua versão alterada pela Diretiva 98/48, mais estabelece que se entende por:
"- à distância": um serviço prestado sem que as partes estejam simultaneamente presentes,
- "por via eletrónica": um serviço enviado desde a origem e recebido no destino através de instrumentos eletrónicos de processamento (incluindo a compressão digital) e de armazenamento de dados, que é inteiramente transmitido, encaminhado e recebido por cabo, rádio, meios óticos ou outros meios eletromagnéticos,
- "mediante pedido individual de um destinatário de serviços": um serviço fornecido por transmissão de dados mediante pedido individual

15 Leitão, L. M. (2002). A responsabilidade civil na Internet. *Direito da Sociedade da Informação, 3*, 147-167.

16 O n.1 do art.º 12º da DCE estabelece que o simples transporte consiste na prestação "de um serviço da sociedade da informação que consista na transmissão, através de uma rede de comunicações, de informações prestadas pelo destinatário do serviço ou em facultar o acesso a uma rede de comunicações"

17 Caso em que se procede a uma "armazenagem automática, intermédia e temporária dessa informação, efetuada apenas com o objetivo de tornar mais eficaz a transmissão posterior da informação a pedido de outros destinatários do serviço" (n.1 do art.º 13º da DCE)

18 O n.1 do art.º 14º da DCE estabelece que a armazenagem em servidor consiste na "prestação de um serviço da sociedade da informação que consista no armazenamento de informações prestadas por um destinatário do serviço"

de retirar ou impossibilitar o acesso às informações" (alínea b) do nº1 do Artigo 14º da DCE).

No caso do prestador de serviços da sociedade de informação, que consistissem no simples transporte ou armazenagem temporária ("caching"), a sua responsabilidade não podia ser invocada quando estes são inteiramente alheios à informação transmitida, o que exige, designadamente, que não alterassem a informação que transmitem (considerando 43 e alínea a) e nº 1 dos Artigos 12º e 13º da DCE). Pelo contrário, as isenções de responsabilidade não eram aplicáveis sempre que se desse o caso de um prestador colaborar "deliberadamente com um dos destinatários do serviço prestado, com o intuito de praticar atos ilegais" (considerando 44 da DCE).

De notar que este regime de responsabilidade benevolente do ponto de vista dos intermediários poderia conduzir a um desequilíbrio face ao enquadramento vigente no *off-line*. Na realidade, no caso português, devemos ter em conta o Artigo 30.º do Decreto-Lei 330/90, de 23 de Outubro (Código da publicidade) relativo à Responsabilidade civil estabelece no seu n.1 que "os anunciantes, os profissionais, as agências de publicidade e quaisquer outras entidades que exerçam a atividade publicitária, bem como os titulares dos suportes publicitários utilizados ou os respetivos concessionários, respondem civil e solidariamente, nos termos gerais, pelos prejuízos causados a terceiros em resultado da difusão de mensagens publicitárias ilícitas". Surgia, assim, uma possível disparidade de tratamento entre os titulares de suportes publicitários tradicionais (tipicamente órgãos de comunicação social) e os prestadores de serviços em linha.

Instrumentos jurídicos não vinculativos

Neste ponto, importa referenciar dois instrumentos da autoria da Comissão Europeia que tiveram o propósito de intensificar a luta contra os conteúdos ilegais em linha: Por um lado, a Comunicação da Comissão COM/2017/0555 final "Combater os conteúdos ilegais em linha Rumo a uma responsabilidade reforçada das plataformas em linha"; e, por outro lado, a Recomendação (UE) 2018/334 da Comissão, de 1 de março de 2018, sobre medidas destinadas a combater eficazmente os conteúdos ilegais em linha.

Vejamos cada um deles em maior detalhe.

No que respeita à Comunicação COM/2017/0555, esta surgiu primordialmente para dar resposta à "crescente presença de material terrorista em linha e a propagação desse tipo de conteúdos constituem uma séria ameaça à segurança e à dignidade das vítimas". Adiantava-se, aliás, que a comunicação visava "igualmente clarificar as responsabilidades das plataformas quando tomam medidas proativas para detetar, remover ou impossibilitar o acesso a conteúdos ilegais (as chamadas medidas do «Bom Samaritano»)".

A Comunicação previa, assim, um conjunto de mecanismos a ser aplicados (voluntariamente) pelos prestadores intermediários para endereçar conteúdos ilegais, como sejam, as notificações pelos utilizadores, os sinalizadores de confiança, os mecanismos de resolução extrajudicial, bem como medidas proativas a serem desenvolvidas pelos prestadores. Relativamente a estas últimas, esclarecia-se que a sua adoção não implicaria necessariamente a perda de isenção de responsabilidade das plataformas em linha, prevista no artigo 14.º da Diretiva sobre o comércio eletrónico.

Esta comunicação é relevante por si, mas também pelo facto de que diversas medidas nela previstas viriam a ser plasmadas na proposta de Regulamento dos serviços digitais, que viria a ser apresentada em 2020 (ver a este propósito Capítulo 0 - O Novo enquadramento **regulamentar**).

No que à Recomendação (EU) 2018/334 diz respeito, pretendeu-se igualmente endereçar a questão da moderação do conteúdo ilegal. Medidas que constavam na Comunicação COM/2017/0555, como a apresentação e tratamento de notificações, sinalizadores de confiança ou medidas proativas, surgem agora sistematizadas sob a forma de recomendação, emprestando-lhes assim um carater mais formal, ainda que a sua adoção permanecesse voluntária.

2.2. Regulação da moderação de determinados tipos específicos de conteúdo ilegal

Para além dos referidos instrumentos jurídicos, que são transversais conforme descritos no ponto anterior, existe um conjunto de outras normas de carater setorial ou que endereçam apenas um tipo de conteúdo ilegal.

São algumas dessas normas que serão referidas neste ponto.

Diretiva 2010/13/EU, de 10 de março, relativa a Serviços de Comunicação Social Audiovisual, tal como alterada pela Diretiva 2018/1808, de 14 de novembro

A Diretiva 2018/1808 (*Serviços de Comunicação Social Audiovisual*) introduz a definição de "Serviço de plataforma de partilha de vídeos", cuja principal finalidade consiste "na oferta ao público em geral de programas ou de vídeos gerados pelos utilizadores, ou de ambos (…)"[13]. Na própria definição deste serviço se esclarece que o prestador do mesmo não tem responsabilidade sobre os conteúdos. [19]

Ainda assim, o Artigo 28º - B estabelece medidas para que os fornecedores de plataformas de partilha de vídeos protejam os menores e público em geral do acesso a conteúdo ilegal (ex. conteúdo suscetível de prejudicar o desenvolvimento físico, mental ou moral de menores; conteúdos cuja divulgação constitua uma atividade que seja uma infração penal nos termos do direito da União, a como o incitamento público à prática de infrações terroristas, infrações relativas à pornografia infantil, e infrações de caráter racista e xenófobo).

Diretiva (UE) 2019/790, de 17 de abril de 2019, relativa aos direitos de autor e direitos conexos no mercado único digital e que altera as Diretivas 96/9/CE e 2001/29/CE

A Diretiva (UE) 2019/790, de 17 de abril de 2019, relativa aos direitos de autor e direitos conexos no mercado único digital, apresenta disposições que se aplicam aos prestadores de serviços de partilha de conteúdos em linha.[20]

19 Artigo 1(1aa) da Diretiva de 2018/1808

20 Prestador de serviços de partilha de conteúdos em linha é definido na Diretiva *2019/790* como *"*um prestador de um serviço da sociedade da informação que tem como principal objetivo ou um dos seus principais objetivos armazenar e facilitar o acesso do público a uma quantidade significativa de obras ou

O n. 1 do Artigo 17º da Diretiva, dispõe que os prestadores de serviços de partilha de conteúdos em linha devem obter uma autorização dos titulares de direitos de autor, "através da celebração de um acordo de concessão de licenças, a fim de comunicar ao público ou de colocar à disposição do público obras ou outro material protegido". O n.º 4 do mesmo Artigo, prevê ainda que "caso não seja concedida nenhuma autorização, os prestadores de serviços de partilha de conteúdos em linha são responsáveis por atos não autorizados de comunicação ao público".

Neste caso concreto, parece, assim, estabelecer-se um regime de responsabilidade mais severo para estes prestadores de serviços de partilha de conteúdos em linha, uma vez que se admite a responsabilização de um prestador de serviço de partilha de conteúdo, caso o mesmo não tenham a necessária licença.

Diplomas relativos ao combate ao terrorismo

Neste ponto, importa reter a Diretiva 2017/541, de 15 de março[21], relativa à luta contra o terrorismo e o Regulamento 2021/784, de 29 de abril[22], relativo ao combate à difusão de conteúdos terroristas em linha.

No que respeita à Diretiva 2017/541, de 15 de março, destaque para o Artigo 21º que estabelece medidas contra os conteúdos em linha de incitamento público à prática de infrações terroristas e que visa assegurar a sua supressão imediata.

Quanto Regulamento 2021/784, de 29 de abril, importa assinalar o seu Considerando 7) que esclarece que "nenhuma das medidas adotadas pelo prestador de serviços de alojamento virtual em conformidade com o presente regulamento, inclusive medidas específicas, deverá, em si mesma, implicar que esse prestador de serviços perca o benefício da isenção de responsabilidade prevista" na DCE.

Por conseguinte, o regime de responsabilidade dos prestadores de serviços de alojamento virtual não é afetado por este Regulamento. Ainda assim, este Diploma

---

outro material protegido por direitos de autor carregados pelos seus utilizadores, que organiza e promove com fins lucrativos" (nº. 6 do Artigo 2º).

21 Diretiva 2017/541, de 15 de março disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32017L0541 (consultado em agosto de 2022)

22 Regulamento 2021/784, de 29 de abril disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32021R0784 (consultado em agosto de 2022)

introduz algumas medidas para supressão imediata de conteúdo terrorista em linha, que terão de ser aplicadas pelos prestadores de serviço.

Diretiva 2011/93 de 13 de dezembro[23]*, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil*

A Diretiva 2011/93 no seu Artigo 25º estabelece "a supressão imediata das páginas eletrónicas que contenham ou difundam pornografia infantil sediadas no seu território.

À semelhança dos Diplomas relativos ao combate ao terrorismo, o disposto na Diretiva 2011/93 de 13 de dezembro não altera o regime de responsabilidade dos prestadores intermediários.

Código de conduta para a luta contra os discursos ilegais de incitação ao ódio em linha[24]

Finalmente, importa referimos o "Código de conduta para a luta contra os discursos ilegais de incitação ao ódio em linha", de 2016, que inclui orientações, não vinculativas, para a remoção de conteúdo ilegal de discurso de ódio na Internet, por parte das empresas de tecnologias de informação.

O Código de conduta sublinha a importância da cooperação entre diversos atores, em particular das organizações da sociedade civil para travar a luta contra discursos de incitamento ao ódio.

3. As decisões do TJUE e de Tribunais Nacionais

Neste ponto, iremos abordar jurisprudência, comunitária e nacional, que emprestaram relevantes contributos sobre o tema do presente trabalho. Naturalmente, que os acórdãos identificados abordam outras matérias relevantes, nomeadamente sobre

23 *Diretiva 2011/93 de 13 de dezembro* disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32011L0093 (consultado em agosto de 2022)
24 C*ódigo de conduta para a luta contra os discursos ilegais de incitação ao ódio em linha* disponíveis em https://ec.europa.eu/newsroom/just/document.cfm?doc_id=42867 (consultado em agosto de 2022)

a definição de marcas comunitárias e os direitos dos respetivos detentores. Ainda assim, focaremos a nossa análise nos pontos relativos à responsabilidade civil dos prestadores intermediários de serviço da sociedade de informação, por ser este o objeto deste trabalho.

Pela sua relevância e pertinência, analisaremos quatro acórdãos. Dois do Tribunal de Justiça da União Europeia (TJUE) e dois de Tribunais nacionais superiores, a saber:

- C-236/08, C-237/08, C-238/08, de 23/03/2010 (acórdãos genericamente conhecidos como Google France Vs Louis Vuitton)[25]
- C-234/09, de 12/07/2011 (L'Oreal vs eBay)[26]
- STJ 10-Dez.-2020 (Ferreira Lopes), proc. n.º 44/18.6YHLSB.L1.S2[27]
- Decisão 7708/19 Reti Televisive Italiane SpA v Yahoo! Inc e decisão 7709/19 Reti Televisive Italiane SpA v Yahoo! Inc

A abordagem destes acórdãos impõe, em primeiro lugar, que identifiquemos as partes (AA e RR). De seguida, descreveremos sumariamente o caso. Em 3º lugar, especificaremos as questões prejudiciais / pedidos da Autora. Por fim, precisaremos o sentido das decisões e respetiva fundamentação.

3.1. C-236/08, C-237/08, C-238/08, de 23/03/2010 (acórdão genericamente conhecido como Google France Vs Louis Vuitton)

Identificação dos autores e réus

Os AA são titulares de marcas (Louis Vuitton Malletier, Viaticu, Luteciel e CNRRH) contra a Google.

---

25 Acórdão disponível em https://curia.europa.eu/juris/document/document.jsf;jsessionid=7365F603A1158F27A14FCF4D7DF0A4C5?text=&docid=83961&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1299900

26 Acórdão disponível em https://curia.europa.eu/juris/document/document.jsf?docid=107261&doclang=PT

27 Acórdão disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/2afd1063f5a2ff88802586580072fab4?OpenDocument

Descrição sumária do caso

Neste ponto, focar-nos-emos naquele que teve a Louis Vuitton como parte, atendendo à sua maior visibilidade.

A Google presta o serviço de motor de busca, de forma gratuita, e fornece, adicionalmente, um serviço de referenciação, o Google Adwords, que é pago pelos anunciantes. Este serviço permite que os clientes da Google exponham anúncios publicitários, quando determinados termos (palavras chave) são usados.

A publicidade é remunerada de acordo com um determinado algoritmo da Google e a ordem pela qual os anúncios são apresentados depende do preço pago pelo anunciante, a qualidade do anúncio (sendo a mesma aferida pela Google), entre outros parâmetros.

Os anunciantes podem usar palavras-chave genéricas, mas também podem ser usadas palavras-chave que coincidam com marcas (Ex: Vuitton). É assim frequente que se usem as próprias marcas como palavras-chave, mas também marcas de outros.

No caso, estava em causa o facto de alguns anunciantes usarem indevidamente marcas da Vuitton como palavras-chave e ainda divulgarem os seus anúncios, complementando tais marcas Vuitton com palavras como "imitação", "cópia". Como consequência, a Vuitton intentou uma ação nos Tribunais nacionais de França contra a Google, a fim de obter, designadamente, a declaração de que esta tinha violado os seus direitos de marca.

No dia 4 de Fevereiro de 2005, o Tribunal de Grande Instância de Paris condenou a Google por contrafação das marcas da Vuitton. Desta decisão, houve recurso para o *Cour d'Appel* de Paris, que confirmou a decisão do Tribunal de Grande Instância de Paris

No entanto, a Google interpôs recurso sobre este último acórdão.

No seguimento deste recurso o *Cour de Cassation* suspendeu a instância e submeteu ao Tribunal de Justiça três questões prejudiciais que de seguida se nomeiam.

Questões prejudiciais

«1) Devem os artigos 5.°, n.º 1, alíneas a) e b), da [Diretiva 89/104] e 9.°, n.º 1, alíneas a) e b), do Regulamento [n.º 40/94] ser interpretados no sentido de que o prestador de um serviço remunerado [de referenciamento] na Internet no caso a Google, que põe à disposição dos anunciantes palavras chave que reproduzem ou imitam marcas registadas e organiza, através do referenciamento, faz um uso destas marcas que o seu titular está habilitado a proibir?

2) Na hipótese de as marcas gozarem de [prestígio], pode o titular opor se a tal uso, com base nos artigos 5. °, n.º 2, da Diretiva [89/104] e 9.°, n.º 1, alínea c), do Regulamento [n.° 40/94]?

3) Na hipótese de tal uso não constituir um uso suscetível de ser proibido pelo titular da marca, em aplicação da Diretiva [89/104] e do Regulamento [n.º 40/94], pode o prestador do serviço remunerado [de referenciamento] na Internet ser considerado um fornecedor de um serviço da sociedade da informação, que consiste em armazenar informações fornecidas pelo destinatário do serviço, na aceção do artigo 14.° da Diretiva 2000/31 […], de modo que [não pode incorrer em] responsabilidade antes de ter sido informado, pelo titular da marca, do uso ilícito do sinal por parte do anunciante?»

Os pedidos de decisão prejudicial tiveram, assim, por objeto a interpretação de três disposições:

- Artigo 5.° (Direitos conferidos pela marca)[28], n.ºs 1 e 2, da Primeira Diretiva 89/104/CEE do Conselho, de 21 de Dezembro de 1988, que harmoniza as legislações dos Estados Membros em matéria de marcas (JO 1989, L 40, p. 1)[29].

28 Artigo 5.º
Direitos conferidos pela marca
1. A marca registada confere ao seu titular um direito exclusivo. O titular fica habilitado a proibir que um terceiro, sem o seu consentimento, faça uso na vida comercial:
a) De qualquer sinal idêntico à marca para produtos ou serviços idênticos àqueles para os quais a marca foi registada;
b) De um sinal relativamente ao qual, devido à sua identidade ou semelhança com a marca e devido à identidade ou semelhança dos produtos ou serviços a que a marca e o sinal se destinam, exista, no espírito do público, um risco de confusão que compreenda o risco de associação entre o sinal e a marca.

- Artigo 9.° (Direito conferido pela marca comunitária)[30], n.º 1, do Regulamento (CE) n.º 40/94 do Conselho, de 20 de Dezembro de 1993, sobre a marca comunitária (JO 1994, L 11, p. 1), e

- Artigo 14.° (Armazenagem em servidor)[31] da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») (JO L 178, p. 1).

---

2. Qualquer Estado-membro poderá também estipular que o titular fique habilitado a proibir que terceiros façam uso, na vida comercial, sem o seu consentimento, de qualquer sinal idêntico ou semelhante à marca para produtos ou serviços que não sejam semelhantes àqueles para os quais a marca foi registada, sempre que esta goze de prestígio no Estado-membro e que o uso desse sinal, sem justo motivo, tire partido indevido do carácter distintivo ou do prestígio da marca ou os prejudique.

29 A Diretiva 89/104 foi revogada pela Diretiva 2008/95/CE do Parlamento Europeu e do Conselho, de 22 de Outubro de 2008, que aproxima as legislações dos Estados Membros em matéria de marcas (versão codificada) (JO L 299, p. 25), que entrou em vigor em 28 de Novembro de 2008. No entanto, atendendo à data dos factos, os litígios nos processos principais continuam a ser regidos pela Directiva 89/104.)

30 Artigo 9º do Regulamento (CE) n.º 40/94 do Conselho, de 20 de Dezembro de 1993

Direito conferido pela marca comunitária

1. A marca comunitária confere ao seu titular um direito exclusivo. O titular fica habilitado a proibir um terceiro de utilizar, sem o seu consentimento, na vida comercial:

a) Um sinal idêntico à marca comunitária para produtos ou serviços idênticos àqueles para os quais esta foi registada;

b) Um sinal que, pela sua identidade ou semelhança com a marca comunitária e pela identidade ou semelhança dos produtos ou serviços abrangidos pela marca comunitária e pelo sinal, provoque o risco de confusão no espírito do público; o risco de confusão compreende o risco de associação entre o sinal e a marca;

c) Um sinal idêntico ou similar à marca comunitária, para produtos ou serviços que não sejam similares àqueles para os quais a marca comunitária foi registada, sempre que esta goze de prestígio na Comunidade e que o uso do sinal sem justo motivo tire partido indevido do carácter distintivo ou do prestígio da marca comunitária ou lhe cause prejuízo.

31 Artigo 14º da «Diretiva sobre o comércio eletrónico»

Armazenagem em servidor

1. Em caso de prestação de um serviço da sociedade da informação que consista no armazenamento de informações prestadas por um destinatário do serviço, os Estados-Membros velarão por que a responsabilidade do prestador do serviço não possa ser invocada no que respeita à informação armazenada a pedido de um destinatário do serviço, desde que:

a) O prestador não tenha conhecimento efectivo da actividade ou informação ilegal e, no que se refere a uma acção de indemnização por perdas e danos, não tenha conhecimento de factos ou de circunstâncias que evidenciam a actividade ou informação ilegal, ou

b) O prestador, a partir do momento em que tenha conhecimento da ilicitude, actue com diligência no sentido de retirar ou impossibilitar o acesso às informações.

2. O n.o 1 não é aplicável nos casos em que o destinatário do serviço actue sob autoridade ou controlo do prestador.

3. O disposto no presente artigo não afecta a faculdade de um tribunal ou autoridade administrativa, de acordo com os sistemas legais dos Estados-Membros, exigir do prestador que previna ou ponha termo a uma infracção, nem afecta a faculdade de os Estados-Membros estabelecerem disposições para a remoção ou impossibilitação do acesso à informação.

Sentido da decisão e fundamentação

A responsabilidade do prestador do serviço de referenciação é um dos pontos-chave do acórdão, tendo dado origem a ampla discussão e análise.

Na realidade, o TJUE debruçou-se, pois, sobre a responsabilidade da Google pela violação de marca registada por parte dos seus clientes anunciantes que usam marcas registradas para produtos ou serviços, prejudicando a função das marcas, através da seleção de palavras-chave. O Tribunal considerou que o serviço de referenciamento na Internet (e não o serviço de motor de busca) constitui um serviço da sociedade da informação (parágrafo 110 do acórdão), que consiste no armazenamento de informações fornecidas pelo anunciante, de modo que esse serviço se enquadra na «armazenagem em servidor», na aceção do artigo 14º da Diretiva 2000/31. Consequentemente, no entender do Tribunal, a Google não pode ser considerada responsável antes de ele próprio ter sido informado do comportamento ilícito do referido anunciante.

O argumento invocado pela Louis Vuitton, segundo o qual a sua marca estaria a ser usada pela Google atendendo a que o serviço de referenciação era pago, não foi acolhido pelo Tribunal (parágrafo 116).

O Tribunal deliberou ainda que o intermediário de informação pode ser responsabilizado por infrações legais efetivamente cometidas por outros, caso se verifiquem certos pressupostos. Assim, no caso em que a atividade do intermediário não for de carácter meramente técnico, automático e natureza passiva, ou seja, sempre que o prestador possuir conhecimento ou controle das informações divulgadas (parágrafo 113) a isenção de responsabilidade não se aplica. No sentido inverso, a partir do momento em que o provedor adquira conhecimento da ilicitude das informações divulgadas através dos seus serviços deve imediatamente remover ou bloquear o acesso às mesmas, sob pena de poder vir a ser responsabilizado.

Resulta, assim, que foi assumido pelo TJUE que não se pode concluir que um intermediário tenha adquirido conhecimento ativo das informações que armazenou, apenas por ter havido concordância entre a palavra-chave selecionada e o termo de pesquisa introduzido por um internauta (parágrafo 117).

Com a decisão do TJUE, a responsabilidade da Google pelo uso, por parte dos seus clientes, de palavras-chave que infringem marcas registadas, foi descartada, pelo menos como regra geral, uma vez que se considerou que a Google não participava ativamente da seleção de palavras-chave.

De salientar que esta decisão do TJUE, teve por base a opinião do Advogado-Geral português Miguel Poiares Maduro, apresentada a 22 de setembro de 2009[32]. As opiniões dos Advogados-Gerais não são vinculativas, mas podem influenciar decisivamente as decisões do TJUE.

A opinião de Poiares Maduro merece-nos atenção, embora a mesma tenha sido inteiramente seguida pelo TJUE. O Advogado-Geral considerou que o serviço *Adwords* se enquadra na definição do serviço da sociedade de informação (parágrafo 134 da opinião). Considerou ainda que o *AdWords* cumpre os "requisitos para estar abrangido pelo conceito de armazenagem em servidor, tal como é definido no Artigo 14º da Diretiva 2000/31" (parágrafo 138). No entanto, Poiares Maduro foi da opinião que a isenção de responsabilidade prevista no Artigo 14º da DCE não deveria ser aplicável ao *AdWords* (parágrafo 141).

Para fundamentar esta posição, o jurista distingue o serviço de motor de busca tradicional do Google com o serviço Adwords. Enquanto naquele caso, a Google presta um serviço de forma neutra porque "não tem interesse em chamar a atenção dos internautas para um sítio em especial" (parágrafo 144), neste último caso, "o AdWords deixa de ser um veículo neutro de informação: a Google tem um interesse direto em que os internautas cliquem nos links para os anúncios (ao contrário do que acontece com os resultados naturais apresentados pelo motor de busca)" (parágrafo 145).

A distinção apresentada por Miguel Poiares Maduro entre o que se pode considerar um serviço prestado de forma neutra ou de forma ativa parece-nos um contributo relevante para a discussão das circunstâncias que deverão estar presentes para que os prestadores intermediários beneficiem de uma isenção de responsabilidade dos intermediários. No entanto, esta opinião acabou por não ser refletida, neste ponto, na decisão do TJUE.

---

32 Conclusões do Advogado-Geral Miguel Poiares Maduro, apresentadas em 22 de setembro de 2009, disponíveis em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A62008CC0236

3.2. C-234/09, de 12/07/2011 (L'Oreal vs eBay)

Identificação dos autores e réus

O Caso C-234/09 opôs a L'Oreal à eBay.

A L'Oréal é uma empresa que produz e comercializa perfumes, cosméticos e produtos para o cabelo, sendo titular de marcas comunitárias. No Reino Unido, detém várias marcas nacionais (parágrafo 26 do acórdão do TJUE referente ao caso C-234/09). A eBay "explora um sítio de comércio eletrónico no qual são apresentados anúncios de produtos colocados à venda por pessoas inscritas para este efeito que criaram uma conta de vendedor na eBay. A eBay cobra uma percentagem sobre as transações realizadas" (parágrafo 28).

A eBay permite vendas através de um modelo de leilão em que os compradores potenciais poderão licitar os objetos propostos pelos vendedores, mas também permite a venda de objetos a um preço fixo, através do sistema de «compra imediata». Adicionalmente, os vendedores podem criar «lojas 'online'» nos sítios da eBay, que apresentam todos os produtos que um vendedor tem para venda num determinado momento (parágrafo 29).

Descrição sumária do caso

Conforme é referido no parágrafo 34 do acórdão, por carta de 22 de maio de 2007, a L'Oréal transmitiu à eBay a sua preocupação relativamente à existência de transações em grande escala nos sítios Internet europeus da eBay que violavam os seus direitos de propriedade intelectual, e solicitou ao prestador a adoção de medidas para resolver esta situação. Não tendo visto as suas pretensões satisfeitas, a "L'Oréal intentou diversas ações contra a eBay em diferentes Estados-Membros, incluindo a ação intentada na High Court of Justice (England & Wales), Chancery Division" (parágrafo 35).

Na ação interposta pela L'Oréal, a empresa francesa peticiona que o Tribunal considere a eBay responsável pelas vendas de objetos efetuadas no sítio www.ebay.co.uk, porque estas violariam direitos conferidos à L'Oréal. Em particular, foram identificadas pela L'Oréal diversas vendas, sendo que algumas dessas vendas

correspondiam a produtos contrafeitos. Foram também identificadas vendas de produtos que não se destinavam a ser comercializadas no Espaço Económico Europeu.

Além disso, o eBay anunciava a venda destes produtos através do serviço *Adwords* da Google. Tais anúncios eram visíveis caso fossem usadas algumas palavras-passe que correspondessem a marcas pertencentes à L'Oréal[33].

No acórdão de 22 de maio de 2009, a *High Court of Justice* concluiu que o processo não poderia ser decidido, na medida em que, previamente, diversas questões de direito deveriam ser necessariamente interpretadas pelo TJUE (parágrafo 45 do acórdão do TJUE). A *High Court of Justice* não deixou de tecer considerações sobre o caso. Com efeito, reconheceu-se que a eBay dispunha de mecanismos de filtragem para detetar e remover mercadorias que violavam os direitos de propriedade intelectual e foi igualmente sublinhado que este prestador poderia adotar medidas mais restritivas para resolver o problema generalizado dessas violações.

Questões prejudiciais

No seu acórdão, a *High Court of Justice* identificou dez questões prejudiciais (que estão elencadas no parágrafo 50 do acórdão do TJUE). Dentro destas questões, importa salientar três com especial pertinência para o nosso tema:

Em primeiro lugar, é questionado se por via da Diretiva 89/104 e do Regulamento 40/94, o titular da marca terá o direito de impedir a realização de vendas não autorizadas dos seus produtos registados, nos sítios de comércio eletrónico.

É igualmente questionado se o titular da marca tem o direito de impedir que o prestador do sítio de comércio eletrónico divulgue, numa secção de *links* patrocinados, anúncios a produtos que fazem uso da sua marca registada.

Por fim, é questionado se a atividade do prestador do sítio de comércio eletrónico se enquadra no âmbito do artigo 14º da Diretiva do Comércio Eletrónico (isto é, se é

33 Entre as palavras-passe usadas pela eBay para anunciar estas vendas foram referidas termos como: "*Shu Uemura"*, marca nacional da L'Oréal; «matrix hair», que invoca a marca nacional *Matrix* também da L'Oréal,

enquadrável no âmbito do serviço de armazenagem e servidor) e até que ponto tal prestador pode der responsabilizado no âmbito dessa disposição.

Sentido da decisão e fundamentação

Iremos focar, novamente, a nossa análise nas decisões do TJUE que digam respeito à responsabilidade do prestador do sítio de comércio eletrónico, neste caso o eBay.

Em primeiro lugar, o TJ abordou a questão de saber se o serviço prestado pelo eBay poderá caber no conceito de «serviço da sociedade da informação», que consta do artigo 2.°, alínea a), da Diretiva 2000/31 por remissão para o artigo 1.°, n.° 2, da Directiva 98/34/CE do Parlamento Europeu e do Conselho, de 22 de Junho de 1998 (ver a este propósito Capítulo 2 - O anterior enquadramento regulamentar). Na sua douta decisão o Tribunal considerou que "é óbvio que a exploração de um sítio de comércio eletrónico pode reunir" todos os elementos que definem um serviço da sociedade da informação, atendendo a que os serviços prestados pelo eBay são "serviços prestados à distância, por via eletrónica de processamento e de armazenamento de dados, mediante pedido individual de um destinatário de serviços e, normalmente, mediante remuneração".

Mais importante, no que diz respeito às responsabilidades legais do eBay, o Tribunal discutiu se o prestador pode invocar a isenção de responsabilidade prevista na Diretiva da UE 2000/31. Neste âmbito, esclareceu que o serviço prestado pelo prestador de um sítio de comércio eletrónico, engloba o armazenamento das informações que lhe são transmitidas pelos seus clientes vendedores, pelo que o mesmo se enquadra no Artigo 14º da Diretiva 2000/31 (parágrafos 110 e 111).

Salientou-se, porém, que esse facto não seria suficiente para a não assunção de responsabilidades por parte do prestador. Na realidade, para que tal se verifique é necessário ainda que sejam satisfeitas uma das seguintes condições (parágrafos 118 e seguintes):

a) o prestador não tem conhecimento real da atividade ou informação ilícita; ou

b) o prestador, ao obter tal conhecimento ou conhecimento, age de forma expedita para remover ou impedir o acesso às informações".

O Tribunal esclareceu ainda que tal isenção de responsabilidade não se aplica quando "prestador do serviço, em vez de se limitar a uma prestação neutra, através de um processamento puramente técnico e automático dos dados fornecidos pelos seus clientes, desempenha um papel ativo suscetível de lhe facultar um conhecimento ou um controlo destes dados" (parágrafo 113)[34].

O Tribunal considerou que o eBay geralmente processava dados inseridos pelos seus clientes/vendedores, e que, em alguns casos, o eBay fornecia assistência para otimizar ou promover determinadas ofertas para venda (parágrafo 114). Assim sendo, considerou o Tribunal que o prestador em questão não poderia invocar a isenção de responsabilidade prevista no artigo 14.o, n.o 1, da Diretiva 2000/31 (parágrafo 116).

O Tribunal concluiu que caberia ao órgão jurisdicional de reenvio, isto é, ao *High Court of Justice* do Reino Unido, examinar se o eBay desempenhou um papel no processamento dos dados relacionados à venda dos produtos da L'Oréal.

Parece-nos que esta decisão constitui uma evolução face ao acórdão Google France Vs Vuitton, ao ser mais exigente na avaliação do que se considera ser uma avaliação meramente técnica por parte do prestador, o que terá implicações na assunção de responsabilidade.

Após a abordagem de dois acórdãos do TJUE, iremos analisar dois acórdãos de Tribunais Superiores de dois Estados-Membros, no caso, Portugal e Itália.

34 Neste ponto, o TJUE faz uma referência ao caso Google France Vs Louis Vuitton, que foi objeto de análise no ponto 0 do presente trabalho.

3.3. STJ 10-Dez.-2020 (Ferreira Lopes), proc. n.º 44/18.6YHLSB.L1.S2[35]

Identificação dos autores e réus

A ação foi interposta no Tribunal da Propriedade Intelectual pelo Modelo Continente Hipermercados, S.A., contra a Eviano Digital, SL, sociedade de direito espanhol, "que se dedica à criação e desenvolvimento, alojamento, assessoria, gestão e exploração de páginas web, plataformas de formação e páginas de venda online e gestão de cobrança e pagamentos por conta dos seus clientes.

Descrição sumária do caso

Conforme consta do acórdão proferido pelo STJ, no dia 11 de Março de 2014, com efeitos retractivos a Dezembro de 2013, a Eviano Digital celebrou com uma sociedade registada em Hong Kong, a West Pacific International, um acordo escrito, ao abrigo do qual a Eviano Digital forneceria os serviços web hosting e e-mail dos endereços eletrónicos web, assim como os serviços de faturação e cobrança do cliente, de diversos sítios, incluindo do sítio www.persolo1euro.com

Por esses serviços, a Eviano Digital reteria, por forma de compensação, 5% do valor total rececionado na sua conta bancária, em relação aos pagamentos efetuados pelos clientes finais, tendo também a obrigação de transferir os restantes 95% do valor total recebido para a West Pacific". Ficou ainda a constar do contrato que a West Pacific seria "responsável por todo e qualquer conteúdo colocado nos endereços eletrónicos, armazenados no servidor contratado, assumindo a obrigação que nenhum dos conteúdos dos endereços eletrónicos conteria elementos contrário à Lei, moral ou ordem pública".

O acórdão do STJ refere ainda que nas condições gerais do sítio porso1euro.com consta a indicação que "a empresa Eviano Digital S.L atua como prestadora de serviços de intermediação. Não obstante, tanto o gerenciamento de conteúdo acima e edição da website são de exclusiva responsabilidade da Sociedade West Pacific International". Mais se informava no mesmo sítio que os utilizadores para poderem usufruir de todas as

35 Acórdão disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/2afd1063f5a2ff88802586580072fab4?OpenDocument

vantagens do porso1euro.com, deveriam despender 24,90€ mensalmente, extensível e sem compromisso de duração.

Indica o acórdão que, em setembro de 2014, na página de internet www.porso1euro.com, cujo domínio está registado em nome da Eviano Digital SL, acedia-se a uma promoção de "por só 1 € aproveite 50€ nas suas compras no continente" e ainda o logótipo e o nome CONTINENTE, apesar de a Modelo Continente Hipermercados nunca ter autorizado a Eviano Digital. a efectuar qualquer promoção ou publicidade ligada à marca CONTINENTE, nem a usar os sinais CONTINENTE.

Pedido da Autora

Face à situação descrita, a Modelo Continente veio pedir a condenação da Eviano Digital a:

1. "Abster-se de anunciar ou publicitar qualquer produto ou serviço, designadamente descontos e outras vantagens económicas, bem como utilizar por qualquer meio e para qualquer finalidade os sinais distintivos Continente e outros semelhantes;

2. Abster-se de emitir quaisquer tipos de vales de descontos ou outros documentos semelhantes, para serem utilizados nos estabelecimentos comerciais da Autora;

3. A pagar à Autora uma indemnização por perdas e danos, em valor a fixar pelo tribunal, com recurso à equidade, nos termos previstos no nº 5 do art.º. 338 do C.P.I,, que compreenda, designadamente as despesas em que a Autora incorreu para a defesa dos seus direitos de propriedade industrial;

4. A pagar uma sanção pecuniária compulsória, a dividir em partes iguais entre a Autora e o Estado, no valor diário de €500,00, posterior ao trânsito em julgado

da decisão da acção, em que a Ré não cumprir algumas das injunções que forem decretadas".

A ação foi declarada procedente, no Tribunal de 1ª Instância, e confirmada no Tribunal da Relação de Lisboa. Ainda assim, a Ré interpôs revista excecional. Na revista excecional, a Ré discorre entre outras matérias sobre o conceito de prestador intermediário de serviços em rede, e em particular ao definido no artigo 4.º, n.º 5 do Decreto-Lei n.º 7/2004[36] e o seu regime de responsabilidade e eventual isenção ao abrigo dos artigos 9.º e seguintes do mesmo diploma normativo.

Sentido da decisão e respetiva fundamentação.

O Supremo Tribunal de Justiça revogou, contudo, as decisões precedentes relativas ao Processo n.º 44/18.6YHLSB.L1.S2.

O STJ deliberou que "devem ser qualificados como "prestadores intermediários de serviços em rede", as pessoas, singulares ou coletivas, que intervindo de forma autónoma, permanente e organizada, criam e disponibilizam os meios técnicos para que um determinado conteúdo circule na internet".

Adicionalmente, o acórdão refere que "o art.º. 12º do DL 07/2004 declara que os prestadores intermediários de serviços em rede não estão sujeitos a um dever de vigilância sobre as informações que transmitem e armazenam, consagrando-se nesse diploma, um regime específico de responsabilidade dessas entidades pelo desempenho dessa atividade".

Sofia Lopes Agostinho[37] chama-nos à atenção que em termos nacionais, "foi apenas a 10 de dezembro de 2020 que foi esboçada uma definição jurisprudencial" para a figura dos prestadores intermediários de serviços em rede. E nesta decisão, o STJ veio desresponsabilizar, pelos motivos já referidos, a Eviano Digital SL, "pelo uso, no seu

36 Conforme anteriormente notado, o Decreto-Lei n.º 7/2004 transpõe para a ordem jurídica nacional a Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno

37 Agostinho, Sofia Lopes, *A responsabilidade das plataformas digitais pela segurança dos consumidores – A propósito do Ac. do STJ, de 10/12/2020*, de 18-Fev.-2021

sítio na internet, dos sinais distintivos de que a Autora é titular, sem as devidas autorizações necessárias para efeitos legais".

Sublinhe-se ainda o entendimento de Sofia Lopes Agostinha no que respeita a este acórdão, segundo o qual "impressiona, contudo, que o Tribunal não tenha analisado, para resolução desta questão, o que já muito foi discutido a nível europeu e, nomeadamente, pelo Tribunal de Justiça da União Europeia (TJUE)".

Salvo melhor opinião parece-nos que o STJ poderia considerar com outra profundidade, se as condições para a invocação da irresponsabilidade do prestador intermediário estariam satisfeitas.

3.4. Decisão 7708/19 Reti Televisive Italiane SpA v Yahoo! Inc[38]

Importa agora analisar a Decisão do Supremo Tribunal Italiano 7708/19 Reti Televisive Italiane SpA, doravante designada **RTI,** contra a Yahoo! Inc, doravante designada Yahoo, e a decisão 7709/19 RTI v Yahoo.

O acórdão 7708/19, de 19 de março de 2019, diz respeito a uma disputa sobre o serviço de partilha de vídeos em linha da Yahoo. No mesmo dia, o Supremo Tribunal Italiano proferiu o acórdão 7709/19, envolvendo as mesmas entidades, a respeito do serviço de motor de busca da Yahoo. Por se considerar que o acórdão 7708/19 tem mais relevância para o tema do presente trabalho iremos centrar a nossa análise essencialmente neste caso.

O caso importa porque aborda matérias como as circunstâncias em que há irresponsabilidade dos prestadores intermediários e as situações em que os mesmos podem alegar o desconhecimento do armazenamento de conteúdos ilegais nos seus serviços.

Identificação dos autores e réus

Conforme referido, o caso opôs a **RTI**, e a Yahoo, doravante designada Yahoo.

38 Acórdão da La Corte Suprema di Cassazione de Itália disponível em https://iusletter.com/wp-content/uploads/Cass.-Sez.-I-Civ.-19-marzo-2019-n.-7708.pdf

A RTI é um canal de televisão privada, do grupo Mediaset, de Silvio Berlusconi, enquanto que a Yahoo é um prestador de serviços em linha, disponibilizando um serviço de partilha de vídeos em linha, que está na origem deste processo.

Descrição sumária do caso

O caso prende-se com a partilha de conteúdos da RTI no serviço de partilha de vídeos da Yahoo.

Em 2011, o Tribunal de 1ª instância de Milão deliberou que a Yahoo seria responsável pelo armazenamento de conteúdo audiovisual não licenciado detido pela RTI no seu serviçi de partilhas de vídeo em linha. Em 2015, o Tribunal de recurso de Milão reverteu a decisão da 1ª instância e considerou que a Yahoo, sendo um prestador intermediário, se qualificava para beneficiar do estatuto previsto no Artigo 14º da Diretiva de Comércio eletrónico, não podendo por isso ser responsável pelos conteúdos armazenados nos seus serviços (O tribunal atribui assim à Yahoo a proteção ao abrigo de "porto seguro" – "*safe harbour"*).

Pedidos da Autora

RTI contestou a decisão do Tribunal de recurso de Milão para o Supremo Tribunal, reclamando que a Yahoo seria responsável pela partilha indevida de conteúdo detido por aquele operador de radiodifusão televisiva, alegando, nomeadamente que a Yahoo não teria desempenhado um papel meramente passivo na difusão de tal conteúdo.

Decisões e respetiva fundamentação.

A importância deste acórdão está desde logo na distinção mais objetiva entre uma intervenção passiva e uma intervenção ativa do prestador intermediário.

Assim considerou o Tribunal que um prestador de "armazenagem em servidor" assume um papel ativo, não sendo por isso abrangido pelo regime de irresponsabilidade

previsto no Artigo 14º da Diretiva de Comércio Eletrónico[39], sempre que presta um serviço que não seja meramente técnico, automático, passivo.

Para Corte Suprema di Cassazione os elementos adequados para aferir se a intervenção do prestador intermediário é meramente passiva ou não, passam por aferir se este desenvolveu, "a título de exemplo e **não necessariamente todas co-presentes - as atividades de filtragem, seleção, indexação, organização, catalogação, agregação, avaliação, utilização, modificação, extração ou promoção dos conteúdos, operadas através de uma gestão empresarial do serviço**, **bem como a adoção de uma técnica de avaliação comportamental dos utilizadores para aumentar a sua lealdade**: conduta que tem, essencialmente, o efeito de complementar e enriquecer de forma não passiva a utilização de conteúdos por utilizadores indeterminados"[40] (sublinhado nosso).

A Corte Suprema di Cassazione teve assim uma perspetiva restritiva do que se pode considerar uma intervenção passiva dos prestadores intermediários, reforçando desse modo a possibilidade de os mesmos virem a ser responsabilizados pelos conteúdos que armazenam e divulgam através dos serviços que prestam.

Outro ponto relevante do acórdão prende-se com o esclarecimento do que se entende ser a tomada de conhecimento por parte do prestador intermediário. Também aqui a *Corte Suprema* teve uma interpretação não coincidente com as pretensões da Yahoo e demais prestadores intermediários. Diz-nos o acórdão:

> "No caso da responsabilidade do prestador de serviços da sociedade da informação, (…) o conhecimento da irregularidade de outra pessoa, como elemento constitutivo da responsabilidade do próprio prestador, coincide com a existência de uma

39 A Diretiva do Comércio Eletrónico foi transporta para o ordenamento jurídico italiano pelo D.Lgs. n. 70 del 2003, disponível em https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-04-09;70

40 Traduzido do acórdão original em italiano: "Gli elementi idonei a delineare la figura o "indici di interferenza", da accertare in concreto ad opera del giudice del merito, sono – a titolo esemplificativo e non necessariamente tutte compresenti – le attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti, operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione: condotte che abbiano, in sostanza, l'effetto di completare ed arricchire in modo non passivo la fruizione dei contenuti da parte di utenti indeterminati."

comunicação para esse efeito feita pelo terceiro cujo direito é alegadamente violado"[41].

Bastará assim que sejam apresentadas denúncias sobre a existência de um conteúdo ilegal para que se considere que o prestador intermediário obteve conhecimento sobre o mesmo. O Tribunal foi ainda mais longe ao considerar que bastará que as denúncias sejam feitas verbalmente para que se considere que o prestador intermediário teve conhecimento das situações denunciadas, ainda que, nesses casos, seja mais desafiante provar que tais denúncias tenham ocorrido[42].

O Tribunal é ainda claro ao determinar que assim que o prestador intermediário tome conhecimento dos factos ele seria responsável pelos danos causados. Ficou igualmente expresso que os prestadores teriam a obrigação de partilhar com as autoridades judiciárias e administrativas eventuais atos ilícitos com o intuito de identificar, mas também de prevenir tais atos.

Da confrontação dos acórdãos do TJUE e dos Supremos Tribunais de Portugal e de Itália parece, assim, transparecer diferentes abordagens ao conceito da responsabilidade civil dos prestadores. Desta disparidade, poder-se-á inferir uma certa insegurança jurídica resultante do atual enquadramento legislativo e das diferentes interpretações que resultam do mesmo.

4. O Novo enquadramento regulamentar

No presente capítulo, analisaremos algumas das limitações identificadas no atual quadro regulamentar, em particular na DCE, e seguidamente debruçar-nos-emos sobre o que foi apresentada como a "reforma do espaço digital" aquando da apresentação pela Comissão Europeia das propostas para dois novos Regulamentos: O Regulamento dos Serviços Digitais e o Regulamento dos Mercados digitais.

---

41 Traduzido do acórdão original em italiano: "Nel caso della responsabilità del prestatore dei servizi della società dell'informazione, dunque, con riguardo all'interpretazione ed applicazione del D.Lgs. n. 70 del 2003, art. 16, comma 1, lett. a), la conoscenza dell'altrui illecito, quale elemento costitutivo della responsabilità del prestatore stesso, coincide con l'esistenza di una comunicazione in tal senso operata dal terzo, il cui diritto si assuma leso".

42 Do acórdão orginal: "Infine, in assenza dell'attuazione di una modalità di comunicazione scritta e formale al provider, la prova della conoscenza in capo al medesimo, gravante sul titolare del diritto leso, potrà essere data con ogni mezzo, restando in tal caso più ardua però la dimostrazione di tale elemento".

Em particular, analisaremos as disposições contidas no Regulamento dos serviços digitais que impactam direta ou indiretamente na assunção de responsabilidade dos prestadores intermediários

4.1. As limitações do enquadramento atual, em particular da Diretiva 2000 / 31 / CE

Tendo presente os objetivos que estiveram da base do atual enquadramento regulamentar e que foram elencadas no capítulo 2 – "O anterior enquadramento regulamentar para a moderação de conteúdo ilegal"[43], importa analisar em que medida é que tais objetivos foram ou não atingidos.

Anja Hoffmann & Alessandro Gasparotti[44] apresentam-nos uma relevante análise sobre esse tema, indicando que a DCE deixa diversos conceitos expostos a uma incerteza jurídica.

Em particular, entendem que o conceito de tomada de "conhecimento" (referido, nomeadamente, no considerando 42 da DCE) que é primordial para a assunção ou não de responsabilidades pelo prestador intermediário é pouco claro, podendo dar origem a interpretações múltiplas[45].

Também a aferição das circunstâncias concretas em que se considera que a atividade dos prestadores assume um caracter "puramente técnico, automático e de natureza passiva" padece de incerteza. A fronteira que separa uma atividade passiva / neutra (situação em que não se imputa responsabilidade ao prestador) de uma atividade do prestador ativa (situação em que tal responsabilidade passa a ser imputável ao prestador intermediário) é assim ténue e de certa forma discricionária.

---

43 Recorde-se que nos Considerando da DCE referia-se que importava abolir obstáculos ao desenvolvimento dos serviços da sociedade da informação, como sejam os obstáculos legais ao bom funcionamento do mercado interno resultantes da divergência das legislações, bem como da insegurança jurídica dos regimes nacionais aplicáveis a esses serviços. Pretendia-se, pois, "garantir a segurança jurídica e a confiança do consumidor" e "criar um enquadramento legal destinado a assegurar a livre circulação dos serviços da sociedade da informação entre os Estados-Membros".

44 Anja Hoffmann & Alessandro Gasparotti (2020), Liability for illegal content online: Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a "Digital Services Act", March 2020.

45 Para aquilo que se considera ser a tomada de conhecimento do prestador, bastará que este tenha conhecimento que determinado conteúdo exista, ou necessitam de ter conhecimento que o mesmo é ilegal?

Acresce que, caso prestador de armazenagem, seja em servidor, seja temporária, venha a ter conhecimento de uma ilicitude, mas atue com diligência no sentido de retirar ou impossibilitar o acesso às informações consideradas ilegais, fica igualmente isento de responsabilidade. Questiona-se, neste ponto, o que se pode considerar uma atuação diligente, atendendo a que não são definidos prazos, para a retirada do conteúdo, que permitam graduar objetivamente a diligência do prestador. A acrescer a incerteza há ainda a sublinhar regimes distintos para a notificação de ilicitudes consoante o tipo de ilícito em causa (proteção de marcas registadas, ou propaganda terrorista).

As diferentes abordagens ao conceito da responsabilidade civil dos prestadores seguidas nos acórdãos dos do TJUE e Supremos Tribunais nacionais, que vimos no capítulo anterior, parece reforçar a ideia da incerteza invocada pelos autores citados.

Outra insuficiência apontada prende-se com o facto de não ser estabelecida qualquer regra para prestadores estabelecidos fora da União Europeia.

Por fim, sendo, por ventura, uma insuficiência intrínseca a qualquer disposição que pretenda estabelecer regras no ciberespaço, não deixa de ser importante referir que um vasto conjunto de tipos de prestadores surgiram ou ganharam expressão após a aprovação da Diretiva, pelo que é incerto que a mesma lhes seja aplicável. Estão neste lote de prestadores, segundo Hoffmann e Gasparotti, prestadores de computação em nuvem, redes sociais ou prestadores de serviços da economia "colaborativa" como a UBER.

4.2.A "reforma do espaço digital"

A 15 de dezembro de 2020, Margrethe Vestager, vice-presidente da Comissão europeia e Thierry Breton, comissário responsável pelo Mercado Interno, anunciaram uma proposta visando "reforma ambiciosa do espaço digital". Esta reforma concretizar-se-ia através de dois diplomas: o Regulamento dos serviços digitais (*Digital services Act*) e o Regulamento mercados digitais (*Digital markets Act*). No comunicado de imprensa publicado nesse mesmo dia, intitulado "Uma Europa preparada para a era

digital: Comissão propõe novas regras para as plataformas digitais"[46], Margrethe Vestager é citada para referir que "as duas propostas têm o mesmo objetivo: garantir que, enquanto utilizadores, temos acesso a uma vasta escolha de produtos e serviços seguros em linha, e que as empresas que operam na Europa podem competir livremente e de forma equitativa em linha, tal como fazem fora de linha. (…) Porque o que é ilegal fora de linha é igualmente ilegal em linha.»

Uma importante ilação que se extrai desta citação é o facto de parecer que a Comissão Europeia pretenderia fazer convergir as regras existentes para o mundo "fora de linha" com as do mundo "em linha", o que representaria uma importante evolução, nomeadamente em face do que foi descrito no Capítulo 2 do presente trabalho.

Analisando os objetivos particulares de cada um destes instrumentos, no mesmo comunicado pode ler-se que com o "Regulamento dos mercados digitais" se estabelecer "regras harmonizadas que definem e proíbem práticas desleais", por parte de "plataformas detentoras do controlo de acesso que atuam como «guardiãs digitais» do mercado interno" que podem "impedir ou retardar a chegada ao consumidor de serviços valiosos e inovadores dos seus utilizadores empresariais e concorrentes".

No que respeita Regulamento dos serviços digitais pretendia-se, segundo o mesmo comunicado "reequilibrar os direitos e responsabilidades dos utilizadores, das plataformas intermediárias e das autoridades públicas, com base nos valores europeus (…)." O Regulamento visa assim criar um conjunto de regras e princípios relativas à forma como os prestadores intermediários participam na publicações e divulgação de conteúdo *on-line* e qual a respetiva responsabilidade sobre tal conteúdo.

A questão da responsabilidade dos intermediários é, pois, central novo Regulamento dos serviços digitais.

Com a entrada em vigor do Regulamento[47], a DCE será revogada. Atendendo à natureza do Regulamentos, de aplicação vinculativa e direta nos ordenamentos jurídicos

---

46 Comunicado de imprensa "Uma Europa preparada para a era digital: Comissão propõe novas regras para as plataformas digitais", de 15 de dezembro de 2020, disponível em https://ec.europa.eu/commission/presscorner/detail/pt/ip_20_2347

47 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), disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2065

nacionais, a entrada em vigor do Regulamento dos serviços digitais implicará igualmente a revogação das disposições que transpõem para o ordenamento jurídico nacional a DCE.

4.3. A noção de conteúdo ilegal ao abrigo do novo Regulamento

Importa esclarecer o que se entende por conteúdo ilegal no âmbito do Regulamento dos serviços digitais.

A este propósito, atente-se o Considerando 12 do Regulamento indica que o conceito de conteúdo ilegal "deverá ser entendido como referindo-se a informações que, independentemente da forma que assumam, nos termos da lei aplicável, são ilegais, como os discursos ilegais de incitação ao ódio ou os conteúdos terroristas e os conteúdos discriminatórios ilícitos, ou que as regras aplicáveis tornam ilegais, tendo em conta o facto de estarem relacionadas com atividades ilegais. São exemplos ilustrativos dessas atividades a partilha de imagens pedopornográficas, a partilha não consensual ilícita de imagens privadas, a perseguição em linha, a venda de produtos não conformes ou contrafeitos, a venda de produtos ou a prestação de serviços em violação do direito em matéria de defesa dos consumidores, a utilização não autorizada de material protegido por direitos de autor, a oferta ilegal de serviços de alojamento ou a venda ilegal de animais vivos". O legislador esclarece ainda que o "conceito de «conteúdos ilegais» deve refletir em sentido lato as normas existentes no ambiente fora de linha". Vemos, portanto, neste ponto uma concretização prática do princípio formulado pela Vice-Presidente Verstager na apresentação da relevante proposta legislativa "Porque o que é ilegal fora de linha é igualmente ilegal em linha" (ver ponto 4.2 - A "reforma do espaço digital" do presente artigo).

Refira-se, ainda, que o Regulamento prevê igualmente a moderação de conteúdos caso os termos e condições dos prestadores não sejam respeitados. Sobre essa matéria, porém, não trataremos no presente trabalho, por não fazer parte do seu escopo.

Feito este esclarecimento, importa abordar os regimes de responsabilidade previstos.

4.4. Os regimes de responsabilidade ao abrigo do Regulamento dos serviços digitais

As categorias de intermediários em linha previstas no Regulamento assemelham-se a um conjunto de *matrioskas* russas[48], significando que cada categoria de intermediário abrange um maior número de prestadores face à categoria imediatamente posterior. De Streel identifica quatro categorias de intermediários às quais se aplicam regras / obrigações crescentemente exigentes:

a) A maior das *matrioskas* deste conjunto corresponde ao prestador de "Serviço intermediário", que de acordo com o Artigo 3º do Regulamento abrange os prestadores de "simples transporte"[49] (alínea g) i)), de "armazenagem temporária" (alínea g) ii))[50] e de "alojamento virtual" (alínea g) iii))[51][52]

b) Prestador de serviço de "alojamento virtual", que consiste na "armazenagem de informações prestadas por um destinatário do serviço a pedido do mesmo". Esta *matrioska* inclui serviços como os de computação em nuvem ou de alojamento na web[53];

c) Fornecedor de plataforma em linha, que se refere a um "um prestador de um serviço de armazenagem em servidor que, a pedido de um destinatário do serviço, armazene e divulgue informações ao público" (Artigo 3º, alínea i)). Esta categoria inclui serviços como as redes sociais e os mercados em linha[54].

d) Por fim, os fornecedores de plataformas em linha de muito grande dimensão, que correspondem a "plataformas em linha que atingem um número médio mensal de destinatários ativos do serviço na União igual ou superior a 45 milhões" (n. 1 do Artigo 33º do Regulamento). De notar que no decorrer do processo legislativo, foi introduzida a definição do motor de pesquisa em linha[55].

---

48 De Streel, A., & Ledger, M. (2021). Regulating the moderation of illegal online content. In *Unravelling the Digital Services Act package* (pp. 20-39). European Audiovisual Observatory.
49 "mere conduit" na versão inglesa do Regulamento
50 "caching" na versão inglesa do Regulamento
51 "hosting" na versão inglesa do Regulamento
52 Na Tradução oficial do Regulamento dos serviços digitais, o termo "hosting" é traduzido para "alojamento virtual", enquanto que na DCE era usado o termo "armazenagem em servidor"
53 Considerando 13 do Regulamento
54 Considerando 13 do Regulamento
55 «Motor de pesquisa em linha» é definido no Artigo 2º alínea ?): um serviço digital que permite aos utilizadores fazer pesquisas para consultar, em princípio, todos os sítios na Internet, ou sítios Internet

Concomitantemente, surge a figura do motor de pesquisa em linha de muito grande dimensão (ou seja, motores que atingem mais de 45 milhões de destinatários por mês). As obrigações aplicáveis aos fornecedores de plataformas em linha de muito grande dimensão são igualmente aplicáveis aos fornecedores de motores de pesquisa em linha de muito grande dimensão e são tratados no Capítulo III, Secção 5 do Regulamento, isto é, Artigos 33º e seguintes.

4.4.1. Responsabilidade dos prestadores de serviços intermediários

O princípio geral de não responsabilização dos prestadores intermediários que já se verificava na DCE, mantém-se neste Regulamento dos Serviços Digitais, sendo igualmente identificadas condições para que cada uma destes prestadores beneficie dessa ausência de responsabilização.

Neste no Regulamento, a responsabilidade dos prestadores de serviço intermediário está prevista nos Artigos 4º, 5º e 6º do Regulamento, e respeitam, respetivamente a prestadores de simples transporte, armazenagem temporária e alojamento virtual. Importa, assim, realçar que a redação destas disposições resulta de uma transcrição praticamente integral dos Artigos 12º, 13º e 14º da DCE.

Assinala-se igualmente o Considerando 18, o qual esclarece que "As isenções de responsabilidade estabelecidas no presente regulamento não serão aplicáveis nos casos em que, em vez de se limitar a prestar os serviços de forma neutra, através de um tratamento meramente técnico e automático das informações prestadas pelo destinatário do serviço, o prestador de serviços intermediários desempenhe um papel ativo que lhe permita ter conhecimento ou controlo dessas informações". A redação deste Considerando terá sido uma decorrência de acórdãos do TJUE como o Google France Vs Vuitton ou Ebay Vs L'Óreal, que vimos anteriormente[56].

---

numa determinada língua, com base numa pesquisa sobre qualquer assunto, sob a forma de uma palavra-chave, comando de voz, frase ou outros dados, e que fornece resultados em qualquer formato nos quais pode ser encontrada informação relacionada com o tipo de conteúdo solicitado;

56 Kuczerawy, A. (2021). The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act, disponível em https://www.law.kuleuven.be/citip/blog/the-good-samaritan-that-wasnt/

4.4.2. Investigações voluntárias por iniciativa própria

Na análise das disposições do Regulamento dos serviços digitais, importa referir o seu Artigo 7º, que se aplica a todos os prestadores intermediários. Dispõe este Artigo que os prestadores não poderão 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".

Esta cláusula terá sido inspirada no designado princípio de "bom samaritano", que foi originalmente introduzido da legislação norte-americana[57].

Ainda que a interpretação deste Artigo 7º do Regulamento seja desafiante[58], o mesmo parece traduzir um incentivo a que os prestadores intermediários adotem iniciativas voluntárias para a deteção de conteúdo ilegal ou lesivo[59].

4.5 Obrigações de moderação de conteúdo ilícito aplicáveis aos prestadores

Embora a redação das disposições em que a matéria de responsabilidade dos intermediários é diretamente endereçada pouco se tenha alterado, não podemos deixar de mencionar um conjunto de novas obrigações que indiretamente se relacionam com essa mesma responsabilidade. Na realidade, algumas das novas regras introduzidas procuram introduzir uma maior transparência às ações dos prestadores para a remoção do conteúdo ilegal e agilizar os procedimentos que se relacionam com a tomada de conhecimento, por parte dos intermediários, da existência de determinado conteúdo ilegal.

Analisemos, pois, algumas dessas novas obrigações que nos parecem particularmente relevantes.

---

57 O princípio do "bom samaritano" encontra-se plasmado na Secção 230 (c) do *Communications Act* de 1934, alterado pelo *Telecommunications Act* de 1996. Ver Barata, J. (2021). The Digital Services Act and social
media power to regulate speech: obligations, liabilities and safeguards. In *Unravelling the Digital Services Act package* (pp. 5-19). European Audiovisual Observatory.
58 Barata, J., op. cit. (2021), p. 13
59 Kuczerawy, A., op. cit. (2021).

4.5.1. Obrigações aplicáveis a todos os prestadores de serviços intermediários.

O Capítulo III do Regulamento dos serviços digitais assume o título "Obrigações de devida diligência para um ambiente em linha transparente e seguro". No nosso entender é este Capítulo que contém as disposições mais inovadoras do Regulamento e que, ainda que de forma indireta, se relacionam com a questão da responsabilidade dos intermediários.

No que respeita às obrigações aplicáveis a todos os prestadores de serviços intermediários, importa destacar a necessidade de os "termos e condições informações sobre quaisquer restrições que imponham em relação à utilização do seu serviço no que diz respeito às informações prestadas pelos destinatários do serviço", nomeadamente "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." (n.º 1 do Artigo 14º do Regulamento).

Todos os prestadores intermediários ficam também obrigados a "disponibilizar ao público, num formato legível (…), pelo menos uma vez por ano, relatórios claros, facilmente compreensíveis sobre qualquer atividade de moderação de conteúdos em que tenham participado durante o período pertinente" (n. 1 do Artigo 15º do Regulamento). Fica, assim, instituída uma obrigação de reporte público por parte destes prestadores intermediários, relativamente às suas ações de moderação de conteúdos, que não deixará de ter implicações na forma como essa moderação é conduzida pelos intermediários.

4.5.2. Obrigações adicionais aplicáveis aos prestadores de armazenagem em servidor

Avançando para a *matrioska* seguinte, a os prestadores de alojamento virtual, verifica-se que é imposta uma obrigação que se relaciona com a assunção de responsabilidade destes prestadores. Trata-se dos "Mecanismos de notificação e ação", previsto no Artigo 16º do Regulamento.

Este mecanismo possibilitará a que qualquer cidadão ou entidade possa notificar os prestadores de armazenagem da existência de conteúdo que seja considerado ilegal.

O Regulamento elenca quais os elementos que as notificações deverão conter[60] (ex: explicação das razões pelas quais se considera determinado conteúdo ilegal) e esclarece que tais notificações "dão lugar a um conhecimento efetivo ou a um alerta para efeitos do Artigo 6º" (n.º3 do Artigo 16º do Regulamente). Ou seja, esta disposição diz-nos que uma vez que uma notificação, feita nos termos descritos, é endereçada aos prestadores de alojamento virtual, os mesmos já não estarão em condições de alegar desconhecimento desse conteúdo, pelo que, à partida, não se poderão assumir como irresponsáveis perante o mesmo.

O Artigo 16º aborda, assim, uma questão que, conforme se retratou no Capítulo 0 do presente trabalho, tem suscitado elevada incerteza jurídica: a de saber em que circunstâncias podem os prestadores de alojamento virtual alegar que desconhecem determinado conteúdo.

4.5.3. Obrigações adicionais aplicáveis aos fornecedores das plataformas em linha

No que respeita às obrigações adicionais que são aplicáveis às plataformas em linha, destaca-se a introdução de uma nova figura: a dos "sinalizadores de confiança" (Artigo 22º do Regulamento). Estas entidades serão especialmente credenciadas por parte do coordenador de serviços digitais[61] para a apresentação de notificações (semelhantes às notificações referidas no Artigo 16º). Porém, as notificações que venham a ser apresentadas por estes sinalizadores de confiança deverão ser "objeto de uma decisão sem demora indevida" (n.º 1 do Artigo 22º). O mesmo artigo define as condições que deverão ser reunidas para que uma entidade se possa constituir como "sinalizador de confiança".

Os fornecedores das plataformas em linha são ainda obrigados a estabelecer um sistema interno de tratamento de reclamações (Artigo 20º). Este sistema permitirá que

60 Segundo o Art.º 16º do Regulamento, as notificações devem incluir elementos como: a) explicação das razões pelas quais se considera determinado conteúdo ilegal; b) indicação clara da localização eletrónica exata dessas informações (endereços URL) c) nome e endereço de correio eletrónico do autor da notificação, exceto no caso de informações que envolvam determinados crimes; d) declaração que confirme a boa-fé do cidadão ou da entidade que apresenta a notificação.

61 O Considerando 75 do Regulamento refere que "Os Estados-Membros podem designar uma autoridade nacional existente e incumbi-la da função de coordenador dos serviços digitais, ou de funções específicas para supervisionar e assegurar o cumprimento do presente regulamento"

os utilizadores possam reclamar das medidas dos fornecedores das plataformas no âmbito da moderação de conteúdo, em resultado, por exemplo, de uma notificação recebida. O mesmo artigo elenca o tipo de medidas de moderação de conteúdo que podem ser alvo de reclamação pelos utilizadores[62].

O sistema de tratamento de reclamações é ainda complementado com um mecanismo de resolução extrajudicial de litígios para a arbitragem de disputas relativas a decisões de moderação de conteúdos (Artigo 21º do Regulamento).

Importa, por fim, realçar que as micro e pequenas empresas são excluídas das obrigações impostas às plataformas em linha (Artigo 19º do Regulamento).

Do exposto, parece-nos que mais uma vez estas disposições poderão ter importantes consequências na assunção de responsabilidades dos fornecedores de plataformas perante o conteúdo nelas divulgado.

4.5.4. Obrigações adicionais aplicáveis aos fornecedores de Plataformas em linha de muito grande dimensão e de motores de pesquisa em linha de muito grande dimensão no que se refere à gestão de riscos sistémicos.

Neste ponto, que se encontra no Capítulo III, Secção 5 do Regulamento, isto é, Artigos 33º e seguintes, procura-se essencialmente endereçar os riscos sistémicos para a sociedade e mesmo para a democracia (Considerando 104 do Regulamento). Os riscos sistémicos de que se falam, podem, segundo o Artigo 34º resultar da divulgação de conteúdos ilegais através dos seus serviços; de efeitos negativos reais ou previsíveis no exercício dos direitos fundamentais; efeitos negativos reais ou previsíveis no discurso cívico e nos processos eleitorais, bem como na segurança pública; de efeitos negativos reais ou previsíveis em relação à violência de género, à proteção da saúde pública, entre outros.

62 Segundo o n.1 do Artigo 17º entre as decisões dos fornecedores que são passíveis de serem reclamadas por via do "sistema interno de tratamento de reclamações" constam decisões como: remoção de informação, bloqueio do acesso à mesma ou restrição da sua visibilidade (ou a decisão de não o fazer); suspensão ou cessação da prestação do serviço, no todo ou em parte, aos destinatários (ou a decisão de não o fazer); suspensão ou encerramento da conta dos destinatários (ou a decisão de não o fazer); suspensão, cessação ou de qualquer outra restrição à capacidade de monetização de conteúdos fornecidos pelos destinatários (ou a decisão de não o fazer).

Aos fornecedores de plataformas em linha de muito grande dimensão compete não apenas a identificação, análise e avaliação diligente de "todos os riscos sistémicos na União decorrentes da conceção ou do funcionamento do seu serviço e dos seus sistemas relacionados, incluindo os sistemas algorítmicos, ou decorrentes da utilização dos seus serviços" (n.º 1 do Artigo 34º do Regulamento), mas também a adoção de "medidas de atenuação razoáveis, proporcionadas e eficazes, adaptadas aos riscos sistémicos específicos identificados" (n.º 1 do Artigo 35º do Regulamento).

5. Considerações finais

Neste capítulo apresentar-se-ão algumas considerações sobre o regime de responsabilidade dos intermediários, bem como das obrigações de moderação de conteúdo que são aplicáveis aos prestadores intermediários, em especial à luz do novo Regulamento dos Serviços digitais.

5.1. Reflexões sobre o novo regime de responsabilidade

Conforme referido, a proposta para o novo pacote legislativo, composto pelo Regulamento dos Mercados Digitais e pelo Regulamento dos Serviços Digitais, foi apresentada como a "reforma do espaço digital".

No que respeita ao Regulamento dos Serviços Digitais, embora as obrigações dos diferentes prestadores intermediários, relativas à moderação do conteúdo sejam claramente mais detalhadas, sendo definidos os mecanismos a implementar pelos diferentes tipos de prestadores, no que respeita ao regime de responsabilidade, tal como igualmente mencionado, não foram introduzidas alterações significativas.

O caminho poderia ter sido outro.

Buiten[63] sublinha que é questionável que a manutenção da dicotomia entre a intervenção passiva e intervenção ativa dos prestadores intermediários seja o caminho

63 Buiten, M. C. (2021). The Digital Services Act from Intermediary Liability to Platform Regulation. *J. Intell. Prop. Info. Tech. & Elec. Com. L., 12*, 361, disponível em https://www.ejtn.eu/PageFiles/20504/Buiten%20-%20The%20Digital%20Services%20Act.pdf

mais eficaz, atendendo à intensa moderação de conteúdo que é feita pelos diversos prestadores. Atividades como a filtragem ou otimização de conteúdo continuam a ser vistas como atividades meramente técnicas, assumindo-se que não resultam num "conhecimento" sobre o conteúdo ilegal que é alojado numa qualquer plataforma. Buiten questiona-se, ainda, se estas assunções refletem o mundo digital da atualidade, onde os prestadores, especialmente os de muito grande dimensão, recorrem exaustivamente à inteligência artificial para fins de moderação de conteúdo.

A este propósito, relembremos o Acórdão da Corte Suprema di Cassazione, de março de 2019 (analisado no ponto 3.4 do presente trabalho) elenca os elementos adequados para aferir se a intervenção do prestador intermediário é meramente passiva ou não. No Acórdão é esclarecido que "atividades de filtragem, seleção, indexação, organização, catalogação, agregação, avaliação, utilização, modificação, extração ou promoção dos conteúdos, operadas através de uma gestão empresarial do serviço, bem como a adoção de uma técnica de avaliação comportamental dos utilizadores para aumentar a sua lealdade", são suscetíveis de configurar uma intervenção que não é meramente técnica por parte dos prestadores.

Este entendimento mais lato do que se considera ser uma intervenção ativa por parte dos prestadores, plasmado pela Corte Suprema Italiana, poderia ter sido tomado em linha de conta na proposta da Comissão de dezembro de 2020 e nas posteriores revisões que o Regulamento sofreu ao longo do processo de co-decisão.

De igual modo, a opinião de Miguel Poiares Maduro no caso Google France Vs Louis Vuitton (ver ponto 0 do presente trabalho) em que é feita a distinção entre o serviço prestado de uma forma neutra (serviço de motor de busca) e um serviço prestado de forma ativa (serviço de referenciação, como o Adwords) poderia igualmente ter sido recuperada no âmbito do novo Regulamento.

Essa não foi, porém, a opção do legislador, que preferiu uma via porventura mais conservadora na definição do regime de responsabilidade dos prestadores.

Subjacente ao regime de responsabilidade dos prestadores intermediários, parece, assim, que sobrepesaram ponderações de índole económica e a avaliação dos impactos que um regime de responsabilidade mais gravoso poderia acarretar, nomeadamente para os prestadores.

Neste particular, poder-se-á nomear impactos diretos e impactos indiretos resultante do estabelecimento de determinado regime de responsabilidade e das obrigações complementares aplicáveis aos diferentes prestadores. Aqueles dizem respeito ao custo diretamente imputável à implementação de medidas como das diversas medidas de transparência, das notificações, dos sinalizadores de confiança, etc.[64].

Quanto aos impactos indiretos, ainda que se reconheça que o conhecimento sobre os mesmos é necessariamente limitado face à ausência de evidência empírica[65], parece permanecer viva a perceção, nomeadamente junto do próprio legislador, de que a assunção de um regime de responsabilidade mais robusto poderia impactar negativamente dimensões como a inovação e até mesmo o bem-estar social[66].

Atendendo ao caminho seguido, poder-se-á ainda questionar se o objetivo definido em dezembro de 2020, segundo o qual se deveria prosseguir uma maior semelhança do enquadramento jurídico aplicável ao *on-line* e *off-line*, poderá vir a ser atingido em matéria de responsabilidade de intermediários.

Um outro ângulo de análise, leva-nos até à questão da incerteza jurídica que pode resultar deste Regulamento dos serviços digitais. Relembremos as considerações de Anja Hoffmann & Alessandro Gasparotti (apresentadas no ponto 0 do trabalho) sobre as limitações do enquadramento atual, em particular da DCE. Um dos aspetos conducentes à incerteza jurídica trazida pela DCE prendia-se com a dificuldade de identificar o que constitui uma atuação "puramente técnica, automática e de natureza passiva" de uma atuação ativa por parte dos prestadores. O novo Regulamento também poderá não ser decisivo para ultrapassar essa incerteza, atendendo a que não introduz uma distinção mais objetiva para esta distinção.

Ainda no âmbito da impossível incerteza jurídica, Busch[67], ao abordar a responsabilidade sobre os produtos comercializados nos mercados em linha, analisa o

64 O *Impact Assessment* publicado pela Comissão em 15 de dezembro de 2020, apresenta uma avaliação detalhada dos custos diretos estimados para cada uma das medidas previstas no Regulamento dos serviços digitais. *Impact Assessment of the digital services Act – Part I – pag 50 e seguintes. Disponível em* https://digital-strategy.ec.europa.eu/pt/node/466 *(consultado em agosto de 2022)*

65 Lefouili, Y., Madio, L. (2022). The economics of platform liability. *Eur J Law Econ* **53**, 319–351. https://doi.org/10.1007/s10657-022-09728-7

66 Jeon, Doh-Shin, Yassine Lefouili, and Leonardo Madio. 2021. "Platform liability and innovation". Mimeo.

67 Busch, C. (2021). Rethinking Product Liability Rules for Online Marketplaces: A Comparative Perspective. *Available at SSRN 3897602*.

que designou como “regulação assimétrica” para diferentes categorias de prestadores intermediários, de acordo com a sua natureza e dimensão. Relembra o autor que, de acordo com o novo Regulamento, há obrigações que apenas são aplicáveis a fornecedores de Plataformas em linha de muito grande dimensão e de motores de pesquisa em linha de muito grande dimensão, enquanto que a prestadores de pequena dimensão são isentos quase por completo de obrigações.

Este modelo poderá, à partida, beneficiar estes pequenos prestadores e permitir a entrada de novos prestadores no mercado. Num entanto, numa leitura mais fina, e do ponto de vista de defesa do consumidor esta abordagem poderá trazer consequências algo perniciosas.

Desde logo, defende o autor, este modelo poderá trazer incerteza jurídica, nomeadamente, no que respeita à defesa do consumidor, porque poderá não ser claro para um consumidor inferir se está a adquirir produtos de uma plataforma de pequena dimensão que está isenta de responsabilidade ou de uma empresa de grande dimensão que se responsabiliza pelos produtos comercializados nas suas plataformas.

Apenas o tempo dirá se estes riscos de incerteza jurídica terão ou não expressão aquando da aplicação prática das disposições do Regulamento, mas consideramos que a análise do presente trabalho não seria completa se os mesmos não fossem sinalizados.

5.2. Reflexões sobre as novas obrigações de moderação de conteúdo ilícito

Se ao nível do regime de responsabilidade o cenário pouco é alterado com o novo Regulamento, o mesmo não se verifica, como vimos anteriormente, ao conjunto de obrigações que são impostas aos prestadores intermediários.

Buiten[68] considera que o Regulamento dos serviços digitais coloca os prestadores intermediários sob o foco da regulação, afastando-se do cenário da assunção de responsabilidade. Na realidade, em caso de incumprimento das obrigações previstas no Regulamento as sanções aplicáveis são essencialmente as coimas e não a perda de isenção de responsabilidade.

68 Buiten, M. C.. op. cit (2021).

Busch[69] compara mecanismos como a "notificação e ação" e os sinalizadores de confiança, que são introduzidas pelo novo Regulamento, a um "*outsourcing* regulatório" em que as responsabilidades são externalizadas para atores diversos. O autor assinala, por exemplo, que o papel de sinalizador de confiança tanto pode vir a ser desempenhado por entidade públicas, mas também por organizações não governamentais, como organizações de defesa do consumidor. Busch refere ainda este tipo de externalização é importada de outras iniciativas europeias já referidas no presente trabalho, como o Código *de* conduta para a luta contra os discursos ilegais de incitação ao ódio em linha, no qual é sublinhado a importância da cooperação de diversos atores, em particular as organizações da sociedade civil.

O autor assinala, por fim, que este tipo de abordagem pode ter resultados ambíguos. Na realidade, considera que se a mesma poderá ser aconselhável num campo tão sensível e politizado como é a luta contra o discurso de ódio, já noutras áreas, como a segurança dos produtos comercializados em linha tal externalização poderá contribuir apenas para a mitigação do papel central que os prestadores intermediários deverão assumir no que respeita à responsabilidade sobre os produtos comercializados nomeadamente nas plataformas em linha.

A questão da externalização das soluções para entidades privadas é, de resto, abordada por outros autores.

Cauffman e Goanta[70] chamam-nos à atenção para relevante papel que entidades privadas tanto na elaboração do quadro regulamentar aplicável aos intermediários, como na sua aplicação.

As autoras dão como exemplo deste relevante papel diversas disposições contidas na Secção 6 do Regulamento dos serviços digitais "Outras disposições relativas às obrigações de devida diligência", referindo que no n.º1 do Artigo 44º, é previsto que "A Comissão (…) apoia e promove a elaboração e a aplicação de norma facultativas estabelecidas pelos organismos de normalização europeus e internacionais pertinentes", nomeadamente para efeitos da "apresentação eletrónica de notificações por

69 Busch, C. (2021). Op.cit..

70 Cauffman, Caroline; GOANTA, Catalina. A new order: The Digital Services Act and consumer protection. European Journal of Risk Regulation, v. 12, n. 4, p. 758-774, 2021.

sinalizadores de confiança". Já no Artigo 45º refere-se que deve ser incentivada "a elaboração de códigos de conduta facultativos a nível da União para contribuir para a correta aplicação do presente regulamento", ou referentes à publicidade em linha (Artigo 46º), ou referente a matérias de acessibilidade (Artigo 47º). No que respeita aos protocolos de crise, de aplicação efetiva, "para enfrentar situações de crise estritamente limitadas a circunstâncias extraordinárias que afetem a segurança pública ou a saúde pública" (n. 1 do Artigo 48º), é igualmente incentivada "a participação das plataformas em linha de muito grande dimensão, dos motores de pesquisa em linha de muito grande dimensão e, quando adequado, de outras plataformas em linha ou motores de pesquisa em linha, em interação com a Comissão, na elaboração, testagem e aplicação desses protocolos de crise" (n. 2 do Artigo 48º).

As autoras chamam, por outro lado, a atenção que para descrever o papel da Comissão e do Comité Europeu dos Serviços Digitais são usadas expressões como "facilitar", "convidar", ou "ter por objetivo garantir" que parecem enfraquecer o seu papel na aplicação do Regulamento.

As autoras sublinham que a "externalização do processo de regulamentação a entidades privadas é uma tendência Global. Ainda assim, a 'privatização' da Governação da Internet não deixa de ser alvo de duras críticas sob o ponto de vista dos direitos fundamentais". As autoras apontam para questões de legitimidade que resultam desta externalização, especialmente quando o que está em causa é a própria remoção de conteúdo ilegal ou supressão do acesso ao mesmo. Chamam, por fim, à atenção para o facto de essa supressão poder ser feita sem uma autorização judicial ou de outras autoridades competentes, podendo eventuais disputas ser dirimidas através de mecanismos de resolução extrajudicial.

6. Conclusões

Conforme referido anteriormente a questão da responsabilidade dos intermediários é das mais controversas no âmbito da Governação da Internet há décadas, nas apenas na Europa.

A União Europeia em concreto tem procurado encontrar uma abordagem para este assunto há mais de 20 anos, em particular, através da DCE, que é complementada por

um conjunto de outros instrumentos jurídicos vinculativos e não vinculativos. Contudo, as tentativas para regular esta responsabilidade têm sido imperfeitas e têm dado origem a diferentes interpretações conduzindo a uma incerteza jurídica.

Em comum com a DCE, o Regulamento dos serviços digitais tem o facto de manter, por defeito, a isenção da responsabilidade dos intermediários, sendo necessário que se verifiquem algumas circunstâncias para que tal isenção se extinga. Por norma, esta isenção extinguir-se-á caso o prestador intermediário desempenhe um papel ativo que lhe permita ter conhecimento ou controlo de conteúdos ilícitos divulgados através dos serviços que presta.

Porém, o Regulamento dos serviços digitais introduz um conjunto de obrigações que irão impactar na forma como estes prestadores tomam conhecimento desses conteúdos, pelo que indiretamente, o regime de responsabilidade é impactado. Adicionalmente, o simples facto de se ter optado pela aprovação de um Regulamento, de aplicação direta, contribuirá para uma maior coerência do panorama a nível Europeu.

Alguns poderão considerar que se poderia ter ido mais longe nesta matéria e que a União Europeia poderia ter ido mais longe na aferição das responsabilidades dos intermediários, mas apenas o tempo e a prática dirão se as medidas agora introduzidas traduzir-se-ão num progresso no que à responsabilidade dos intermediários diz respeito.

7. Bibliografia

Agostinho, Sofia Lopes, A responsabilidade das plataformas digitais pela segurança dos consumidores – A propósito do Ac. do STJ, de 10/12/2020, de 18-Fev.-2021

Anja Hoffmann & Alessandro Gasparotti (2020), Liability for illegal content online: Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a "Digital Services Act", March 2020.

Barata, J. (2021). The Digital Services Act and social

Buiten, M. C. (2021). The Digital Services Act from Intermediary Liability to Platform Regulation. J. Intell. Prop. Info. Tech. & Elec. Com. L., 12, 361, disponível em https://www.ejtn.eu/PageFiles/20504/Buiten%20-%20The%20Digital%20Services%20Act.pdf

Busch, C. (2021). Rethinking Product Liability Rules for Online Marketplaces: A Comparative Perspective. Available at SSRN 3897602.

Cauffman, Caroline; GOANTA, Catalina. A new order: The Digital Services Act and consumer protection. European Journal of Risk Regulation, v. 12, n. 4, p. 758-774, 2021.

de Streel, A., & Husovec, M. (2020). The e-commerce Directive as the cornerstone of the Internal Market. Available at SSRN 3637961.

De Streel, A., & Ledger, M. (2021). Regulating the moderation of illegal online content. In Unravelling the Digital Services Act package (pp. 20-39). European Audiovisual Observatory.

Jeon, Doh-Shin, Yassine Lefouili, and Leonardo Madio. 2021. "Platform liability and innovation". Mimeo.

Kuczerawy, A. (2021). The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act, disponível em https://www.law.kuleuven.be/citip/blog/the-good-samaritan-that-wasnt/

Lefouili, Y., Madio, L. (2022). The economics of platform liability. Eur J Law Econ **53**, 319–351. https://doi.org/10.1007/s10657-022-09728-7

Leitão, L. M. (2002). A responsabilidade civil na Internet. Direito da Sociedade da Informação, 3, 147-167.

Poiares Maduro, M. (2009). Conclusões do advogado-geral. Caso Google France SARL e Google Inc. contra Louis Vuitton Malletier SA (C-236/08), Google France SARL contra Viaticum SA e Luteciel SARL (C-237/08) e Google France SARL contra Centre national de recherche en relations humaines (CNRRH) SARL e outros (C-238/08).

Rosa, A. M. (1998). Internet: uma história. P.24

Sousa e Silva, N., Responsabilidade na Internet: o Ato dos Serviços Digitais garante a liberdade de expressão, de 10-Fev.-2021

CYBERLAW

BY CIJIC

O Direito e a Inteligência Artificial:

Uma Solução ou um Problema?

VICÊNCIA SARKIS[1]

1 Doutoranda na Faculdade de Direito da Universidade de Lisboa. vicencia.sarkis@gmail.com

SUMÁRIO: Resumo; I. Introdução; II. IA e o sistema judiciário; III. A tecnologia e implicações jurídicas; IV. Conclusões; V. Bibliografia.

RESUMO:

A evolução tecnológica, onde se encontra a inteligência artificial (IA), é geradora de novos hábitos, novos paradigmas e novos benefícios adotados rapidamente pelas pessoas. Este "mundo moderno", necessita de ser ancorado na ética e na intervenção do direito através da regulamentação, na medida em que deverá existir estruturas jurídicas que tenham a possibilidade de disciplinar as criações tecnológicas a resguardar, desta forma, o bem-estar das pessoas.

A utilização pelo direito da IA poderá auxiliar os operadores jurídicos em vários aspetos, como exemplo se tem as análises contratuais, análises de auditoria, a redação de petições e até mesmo a justiça preditiva. A tecnologia, independentemente do seu modelo, visa facilitar diversas tarefas embora possa causar graves preocupações jurídicas.

Dento da ceara do direito, a IA poderá interferir nos direitos fundamentais, na concorrência, na defesa da democracia, na proteção dos consumidores, nos direitos de personalidades, na indeminização civil entre outras áreas jurídicas, podendo desta forma causar conflitos e prejuízos nestas áreas especialmente.

A metodologia deste artigo é em uma revisão bibliográfica de publicações nacionais e estrangeiras e artigos científicos e de opinião que se detiveram sobre esta temática.

Palavras-chaves: direito, inteligência artificial, tecnologia e efeitos jurídicos.

ABSTRACT:

Technological evolution, where artificial intelligence (AI) is found, generates new habits, new paradigms and new benefits quickly adopted by people. This "modern world" needs to be anchored in ethics and the intervention of law through regulation, insofar as there must be legal structures that have the possibility of disciplining technological creations to safeguard, in this way, the well-being of people.

The use of AI by law can help legal operators in several aspects, such a contractual analysis, audit analyses, writing petitions and even predictive justice. Technology, regardless of its model, aims to facilitate various tasks, although it can cause serious legal concerns.

Within the scope of law, AI may interfere with fundamental rights, competition, the defense of democracy, consumer protection, personality rights, civil compensation, among other legal areas, and may thus cause conflicts and losses in these areas, especially.

The methodology of this article is a bibliographic review of national and foreign publications and scientific and opinion articles that have focused on this theme.

Keywords: *law, artificial intelligence, technology, and legal effects.*

I. Introdução

Alguns países passaram a utilizar a IA no sistema judiciário, incluindo o aplicativo móvel *DoNotPay*[2] orientado para advogados. Também foram adotados os juízes robôs para avaliação de pequenas causas na Estônia, no Canadá utilizam mediadores robôs, de forma similar na China e na Malásia utilizam juízes de inteligência artificial. As autoridades destes países defendem a ideia de que os sistemas judiciais baseados em IA tornam as sentenças mais consistentes, evitando os atrasos nos casos em litígio de maneira mais rápida, menos dispendiosa e evitando litígios estressantes, longos e dispendiosos[3].

O desenvolvimento dos sistemas de Inteligência Artificial voltado para a utilização no sistema judiciário já possui muitas ofertas de produtos no mercado atual, como os sistemas para automatizar a deteção de mentiras, sendo utilizada as micro-expressões faciais, o sistema utiliza algoritmos de visão computacional, geralmente baseados em técnicas de aprendizagem automática[4], permitindo desta forma, através de expressões faciais, a deteção de mentiras, separando as emoções falsas das verdadeiras.

Não é mister desde já, rigorosamente definir que as novas tecnologias impactam de forma decisiva o judiciário, mas decerto que toda a sociedade está a ser alterada.

Com estas considerações preliminares ficará debuxado em termos explícitos que esta evolução tecnológica em linhas gerais é definitiva. Segundo o discurso do Papa Francisco aos Juízes do Continente Americano, o direito não é apenas a lei ou as normas, sendo uma praxe transformadora em "artificie" do direito na medida em que

---

2 Para aprofundamento do tema *Vide* **The World's First Robot Lawyer**, [Em linha]. [2022]. [Consult. 04 jan. 2023]. Disponível em WWW:<URL: https://donotpay.com/>.

3 Cfr. Agência Anadolu, **Mr. Robot takes on law&order: Malaysia tests AI in judicial system**, [Em linha]. [2022]. [Consult. 05 jan. 2023]. Disponível em WWW:<URL: https://www.dailysabah.com/life/mr-robot-takes-on-laworder-malaysia-tests-ai-in-judicial-system/news >.

4 Cfr. MONARO, Merylin, MALDERA, Stéphanie, SCARPAZZA, Cristina, SATORI, Giuseppe e NAVARIN, Nilocoló, **Detecting deception through facial expressions in a dataset of videotaped interviews: A comparison between human judges and machine learning models**, [Em linha]. [2021]. [Consult. 04 jan. 2023]. Disponível em WWW:<URL: https://www-sciencedirect-com.translate.goog/science/article/abs/pii/S0747563221003861?_x_tr_sl=auto&_x_tr_tl=pt&_x_tr_hl=pt-PT&_x_tr_pto=wapp >.

sejam confrontadas as pessoas com a realidade. Diz ainda que a imaginação jurídica deve atender às novas realidades[5].

II. IA e o sistema judiciário

A IA já faz parte da vida das pessoas, mesmo que estas não se tenham percebido ainda, sendo mesmo indispensável. Como mero exemplo antes a sociedade tomava conhecimento de conteúdo informativo através de jornais, revistas, boletins, entre outros, porém, hoje toda essa informação é através de sítios na internet. Estas plataformas utilizam a IA para exibir informação relevante para o leitor, adicionalmente existe a possibilidade de escrever opiniões e avaliações. A IA possui a cada dia mais importância nos media que pode ser considerado o quarto pilar da democracia[6]. Segundo Montesquieu, o equilíbrio dos poderes Legislativo, Executivo e Judiciário tinha como finalidade a garantia de que nenhum tivesse mais poder do que o outro.

De facto, a sociedade está a ser alterada, como a história comprova num passado não muito distante. Por exemplo, o século XIX foi o século das relações internacionais, na medida em que os Estados entenderam quanto lhes era desfavorável manter uma situação de isolamento, e assim iniciaram um movimento de congregação e concórdia. Os interesses individuais de cada Estado foram assim, subordinados aos interesses da comunidade internacional. A comunidade internacional oitocentista pode ser considerada como uma comunidade de deveres, caracterizada por assumir um conjunto de direitos e obrigações no âmbito de um sistema de congressos que acompanhou todo o século[7]. Desta forma, existiu uma alteração dos hábitos que até então faziam parte daquela sociedade, e que devido as alterações que passaram a existir, que foi necessário evoluir o pensamento daquela época.

---

5 Cfr. Papa Francisco, **Discurso do Papa Francisco aos Juízes do Continente Americano**, [Em linha]. [2019]. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://www.vatican.va/content/francesco/pt/speeches/2019/june/documents/papa-francesco_20190604_giudici-panamericani.html >.

6 Cfr. Legal Information Institute, **Separation of Powers** [Em linha]. []. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://www.law.cornell.edu/wex/separation_of_powers_0 >.

7 Cfr. FREITAS, Pedro Caridade de, **Portugal e a Comunidade Internacional – na Segunda Metade do Século XIX**, Lisboa: Quid Juris?, 2012, p. 29.

As ideologias marcam uma reconstrução de um processo histórico e assim se consegue projetar no passado os modelos inspiradores do presente[8].

Já na sociedade moderna, esta pode estar entusiasmada em relação às facilidades das novas tecnologias, em especial a IA, que está relacionada com o progresso. A novidade cria empolgação pelas ideias do "novo", as novidades deste progresso quase que diário levam à adesão das pessoas com mais facilidade, que se deixam seduzir pela tecnologia. Já disse o filósofo alemão Hans-Georg Gadamer[9] em 1972: Um "mundo sem história?", estas modernidades passam a falsa impressão de que o presente é levado ao futuro, não valorizando o processo histórico que nos levou ao presente, como se o mundo fosse a partir de agora.

Existe pessoas e um processo histórico que formou a cultura e a tradição jurídica. Não sendo construído a partir do presente, forma de maneira importante o pensamento, favorecendo um pensamento crítico para os juristas atuais. O passado é tão importante assim como o futuro para que não apenas se possa fazer justiça, como se possa entender essa alteração social e jurídica que se passa fruto da mudança tecnológica.

A história serve então, desta forma, como meio de formação de uma sensibilidade para a justiça e também para a defesa dos direitos e da dignidade da pessoa humana[10], sendo um dos campos importantes para o entendimento atual e para que se consiga ter um pensamento crítico jurídico face as exposições da sociedade à realidade tecnológica.

Observar-se-á que num futuro próximo a IA terá a possibilidade de substituir os três poderes[11], se não existirem leis apropriadas. O judiciário é um dos poderes que apresenta um ónus das pendencias de processos, e assim vários países estão prestes a utilizar a IA como forma de solução deste problema.

Em França a IA foi adotada pelo processo automatizado de dados pessoais chamado por DataJust, sendo criado pelo decreto de 27 de março de 2020. Este visou o

---

8 Cfr. PEREIRA, Maria Helena da Rocha, **Estudos sobre Roma Antiga A Europa e o Legado Clássico**, Coimbra: Fundação Calouste Gulbenkian Imprensa da Universidade de Coimbra, 2015, p. 238.
9 Cfr. GADAMER, Hans-Georg. **Verdade e Método II**. Complementos e índice. Tradução GIACHINI, Enio Paulo. Petrópolis: Vozes, 2011. p. 334.
10 Cfr. PINTO, Eduardo Vera-Cruz, **Terra de Santa Maria – Terra-Mãe de Império Portugal**. Vol II, Santa Maria da Feira: Comissão de Vigilância do Castelo de Santa Maria da Feira. 2007. p. 255.
11 Cfr. GATLEWAR, Aditya, **"Emergence of a New Dimension to the Judicial System:" "AI" – A Threat or Boon?**, [Em linha]. []. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://disputescentre.com.au/emergent-of-a-new-dimension-to-the-judiciary-system-ai-a-threat-or-boon/ >.

desenvolvimento, por dois anos, de um sistema algorítmico que identifica, por tipo de dano a analisar, os valores exigidos e oferecidos pelas partes em um litígio judicial, os montantes que são atribuídos às vítimas a título de reparação dos danos corporais nas decisões judiciais proferidas em recurso pelos tribunais administrativos e nas formações cíveis dos tribunais. O sistema DataJust é baseado na extração automática de dados contidos nas decisões judiciais e sua utilização. A longo prazo, o tratamento pelo sistema Datajust visará constituir um instrumento de restituição e divulgação destes valores relativos a indemnizações por lesões corporais das vítimas[12].

Segundo o jurista francês Fabrizio Papa Techera. que defende o risco de uma "Netflix de direito", a *common law*, dos países anglo-saxões, se presta particularmente às promessas de justiça algorítmica," porém, transposta para a França, poderia levar a um empobrecimento da cultura jurídica francesa e ser diminuída a margem de manobra dos profissionais do direito. Porém, existem outras opiniões, como a do professor de direito em Bruxelas Gregory Lewkowicz, que considera que os advogados devem adaptar-se, pois este tema da IA está a evoluir e desta forma o jurista deve adaptar-se às realidades[13] da época, pois o risco de caso de não adaptação será na medida em que se ficará refém de operadores privados e algoritmos opacos.

Em Espanha a IA *made in Europe* deverá garantir que os valores humanos e os direitos fundamentais sejam pontos centrais, na medida em que deverá garantir que o objetivo da tecnologia seja em função de reforçar o nível de bem-estar dos cidadãos. Desta forma, a investigação em Ciências Sociais e Inteligência Artificial, bem como em humanidades digitais, deve ser um vetor transversal em todas as áreas estratégicas incluídas nesta prioridade. Áreas como ética, psicologia, filosofia, linguística, direito, em particular os aspetos legais da IA, serão necessárias, assim como sistemas inteligentes que modelem fenómenos e sistemas sociais[14]. Desta forma a finalidade em Espanha é assegurar o crescimento do país através da digitalização de serviços.

---

12 Cfr. République Française, **L'intelligence artificielle (IA) dans les décisions de justice: une révolution en cours**, [Em linha]. [22-11-2021]. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://www.vie-publique.fr/eclairage/277098-lintelligence-artificielle-ia-dans-les-decisions-de-justice>.

13 *Idem, ibidem.*

14 Cfr. Ministerio de Ciencia, Innovación y Universidades, **Estrategia Española de I+D+I en Inteligencia Artificial**, [Em linha]. [2019]. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwik-bLm8bX8AhWn9LsIHYsNBJ8QFnoECCcQAQ&url=https%3A%2F%2Fwww.ciencia.gob.es%2Fdam%

A automatização das decisões judiciais poderá ser inclinada a tomar sempre as mesmas decisões e desta forma estaria em causa a independência do julgador, sendo que cabe ao Estado ser o garantidor da imparcialidade dos algoritmos utilizados. Os juízes sabem que o papel do poder público é, controlar as *legaltechs* que podem afetar os valores do julgador decidindo de forma diversa da que o juiz humano decidiria.

A transformação digital é uma preocupação na União Europeia, na medida em que deverão em breve ser discutidos no Parlamento Europeu assuntos relacionados com criptomoedas, Inteligência Artificial (IA), semicondutores e partilha de dados[15].

Os eurodeputados devem decidir a sua posição sobre um quadro jurídico para a Inteligência Artificial, a qual visa introduzir uma base regulamentar e jurídica comum para a IA em linha com os valores da União Europeia (UE). O foco está em aplicações específicas e os seus potenciais riscos.

A IA deverá ser ancorada na ética, na medida em que o Conselho da Europa criou a primeira Carta Ética Europeia que estabelece os princípios éticos relativo ao uso de IA nos sistemas judiciais, destinado aos advogados e profissionais da justiça na gestão deste rápido desenvolvimento.

A visão da Carta Ética é no sentido de gerir o uso da IA no campo da justiça na medida em que poderá contribuir para melhorar a eficiência e a qualidade dos trabalhos dos tribunais. A implementação deve ser feita de forma responsável de acordo com os direitos fundamentais garantidos em particular pela Convenção Europeia dos Direitos do Homem (CEDH) e pela Convenção do Conselho da Europa para a Proteção de Dados Pessoais[16]. É fundamental garantir que a IA continue a ser uma ferramenta ao

---

2Fjcr%3A5af98ba2-166c-4e63-9380-4f3f68db198e%2FEstrategia_Inteligencia_Artificial_IDI.pdf&usg=AOvVaw14aqKAHWJ322Ilg1Jx0e7k>.

15 Cfr. Parlamento Europeu, A agenda do PE em 2023: energia renovável, transformação digital, migração, [Em linha]. [27-12-2022]. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://www.europarl.europa.eu/news/pt/headlines/eu-affairs/20221205STO60502/o-parlamento-em-2023-renovaveis-transicao-digital-migracao >. *Vide* https://www.europarl.europa.eu/news/pt/headlines/society/20201015STO89417/regular-a-inteligencia-artificial-na-ue-as-propostas-do-parlamento>.

16 Cfr. Conselho da Europa, **Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires**, [Em linha]. [2023]. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://www.coe.int/fr/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>.

serviço do interesse geral e que a sua utilização seja feita com respeito pelos direitos individuais.

III. A tecnologia e implicações jurídicas

Quando se fala de tecnologia a primeira situação em que se pensa é no comércio eletrónico, aquisição de bens, serviços e licenças, contratos executados *online* ou *offline*, como exemplo a entrega de livros físicos. Porém, o mercado digital apresenta importância no âmbito de outras realidades que estão ligadas as responsabilidades dos prestadores de serviços intermediários, o direito da propriedade intelectual, gestão de plataformas em linha entre outros[17]. É um "mundo" que consegue alterar facilitando e agilizando a vida da maioria das pessoas e resulta em mudança de comportamento na vida social.

Algumas maiores mudanças sociais que convocam a intervenção do direito são o homem dinâmico que se torna homem pacífico; vontade esclarecida que passa à vontade adormecida; da massificação à personalização; da privacidade para a publicidade; do mundo corpóreo ao mundo virtual; da realidade antropocêntrica para a realidade maquinocêntrica e dos riscos monocausais para os riscos multicausais[18].

O homem dinâmico que se torna homem pacífico está relacionado com o trabalho e a mobilidade das pessoas. No trabalho o papel da IA começa na análise de *big data*, especialmente no aprendizado de máquinas, por meio do qual se pode identificar padrões de tomada de decisão e reduzir, desta forma a intervenção humana no

17 Para maior aprofundamento da matéria relacionada com o direito do consumidor e o comércio eletrónico *Vide* OLIVEIRA, Elsa Dias, Algumas considerações sobre a proteção do consumidor no mercado digital no âmbito do Direito da União Europeia, **Revista da Faculdade de Direito da Universidade de Lisboa**, número I, tomo I, [Em linha]. [2021]. [Consult. 08 jan. 2023]. Disponível em WWW:<URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj306TatLj8AhVMPewKHUH_DxIQFnoECAoQAQ&url=https%3A%2F%2Fwww.fd.ulisboa.pt%2Fwp-content%2Fuploads%2F2021%2F10%2FElsa-Dias-Oliveira.pdf&usg=AOvVaw3wFsljS_s6VQWlATmRph-W>.

18 Para o aprofundamento sobre as maiores mudanças sociais que necessitam da intervenção do direito *vide* ANTUNES, Henrique Sousa, **Direito e inteligência artificial**, Lisboa: Universidade Católica, Editora. 2020. p. 13.

trabalho[19]. O papel significativo da IA está crescendo rapidamente devido à precisão das tomadas de decisão. Quanto à mobilidade, esta é uma das questões em que se coloca em causa a dignidade humana na medida em que pode não ser mais necessário a deslocação presencial favorecendo assim a comunicação à distância[20], seja na encomenda de bens e serviços *online*, a virtualização com a administração pública[21] e com o setor privado, a criação de comunidades virtuais, atividades recreativas, a adoção de assistentes virtuais, o teletrabalho entre outras medidas. Desta forma a pessoa não é mais levada a necessidade de presença física.

A vontade esclarecida que passa à vontade adormecida está relacionada com a partilha generalizada de dados pessoais, potencializado pelas redes sociais. Sendo banalizada a prática de acesso à informação sobre o consentimento[22] ao tratamento de dados pessoais[23]. O que resulta numa tendência de uma decisão das pessoas teoricamente livre.

A massificação da personalização está relacionada com a oferta de produtos direcionada, que é fruto da recolha de dados. Neste caso em tela, observar-se-á a questão 3D, dos benefícios que esta a impressão possui, sendo um deles a personalização, que são as impressões direcionadas para cada indivíduo, existindo uma consciência ecológica deste serviço, pois evita desperdícios existindo uma resposta mais eficiente às necessidades. O desafio do direito está relacionado com violações dos direitos morais e patrimoniais de autor. Em relação aos direitos morais, destaca-se o direito de paternidade previsto no art. 9º, art. 27º ss e 56º, n.º 1, o direito ao inédito previsto no art. 6º e o direito de integridade e genuinidade da obra previsto no art. 56º,

---

19 Cfr. AGGARWAL, Karan, Has the Future Started? The Current Growth of Artificial Intelligence, Machine Learning, and Deep Learning. **Iraqi Journal For Computer Science and Mathematics**. Vol 3, nº 1. pp-115-123. [Em linha]. [2022]. [Consult. 08 jan. 2023]. Disponível em WWW:<URL: https://journal.esj.edu.iq/index.php/IJCM/article/view/100>.

20 Cfr. ANTUNES, Henrique Sousa, **Direito e inteligência artificial**, Lisboa: Universidade Católica, Editora. 2020. p. 17.

21 Em Portugal as pessoas já podem fazer marcações em praticamente todos os serviços públicos de forma virtual a través da plataforma SIGA *vide* https://siga.marcacaodeatendimento.pt/ >.

22 Para aprofundamento da matéria *vide* artigo 7º do **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, que é o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (UE), estabelece as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na UE.

23 A previsão de um direito específico de dados pessoais foi classificada como direito de última geração, *vide* MOREIRA, Vital. Carta dos Direitos Fundamentais da União Europeia in PORTO, Manuel Lopes e ANASTÁCIO, Gonçalo, Coord. **Tratado de Lisboa Anotado e Comentado**. Cimbra: Almedina, 2012. p. 1400.

n.º 1 e o direito de retirada previsto no art. 62º todos do Código do Direito de Autor e dos Direitos Conexos (CDADC). Levantam-se aqui também os problemas de *upload* das obras em linha.

Da privacidade para a publicidade é quando as pessoas fornecem os seus dados às empresas de tecnologia, sendo estes dados utilizados posteriormente para publicidade direcionada as preferências de acordo com o perfil de cada pessoa, baseado no histórico de navegação.

Existindo assim, a relação no surgimento de ofertas digitais na mobilidade, no alojamento, na economia colaborativa[24], na prestação de serviços domésticos, entre outros, possuindo desta forma implicações de responsabilidade civil, comercial e nos contratos[25].

Do mundo corpóreo ao mundo virtual, apesar de que a virtualização hoje é uma tendência generalizada em escala global, as moedas virtuais que possuem implicações na tecnologia *blockhain*, são as que mais carecem das razões do direito na proteção financeira e dos consumidores. Hodiernamente a aquisição desta forma financeira está a cada ano se popularizando, na medida em que houve um aumento considerável nesta área, pois, 43 milhões de pessoas - já tiveram criptomoedas em algum momento de suas vidas nos EUA, revelou uma nova pesquisa divulgada pelo banco JPMorgan Chase. Em 2020 eram apenas 3% e em 2022 subiu para 13%[26] a aquisição destas moedas. O governo dos Estados Unidos divulgaram a sua preocupação em relação ao uso da tecnologia de IA através de um projeto para uma Declaração de Direitos de IA[27], que visa a proteção do povo americano.

---

24 Atualmente o *Airbnb* é uma das *startups* mais valorizadas no mundo. É uma ótima representante de economia colaborativa. O *Airbnb* retrata um novo tipo de *mindset* que valoriza a experiência do consumidor, dando assim um certo modelo de confiabilidade social. Vide RIBEIRO, Renato, **Entenda o que é economia colaborativa e como aplicá-la**, [Em linha]. [2022]. [Consult. 08 jan. 2023]. Disponível em WWW:<URL: https://www.iugu.com/blog/o-que-e-economia-colaborativa >.

25 Cfr. ANTUNES, Henrique Sousa, **Direito e inteligência artificial**, Lisboa: Universidade Católica, Editora. 2020. p. 23.

26 Cfr. EXAME, **Estudo revela que 13% da população dos EUA já teve *criptomoedas* em algum momento**, [Em linha]. [2022]. [Consult. 09 jan. 2023]. Disponível em WWW:<URL: https://exame.com/future-of-money/estudo-revela-que-13-da-populacao-dos-eua-ja-teve-criptomoedas-em-algum-momento/>.

27 Cfr. CASA BRANCA, Projeto para uma Declaração de Direitos de IA – Fazendo Sistemas Automatizados Funcionarem para o povo americano, [Em linha]. [2023]. [Consult. 11 jan. 2023]. Disponível em WWW:<URL: https://www.whitehouse.gov/ostp/ai-bill-of-rights/ >.

Da realidade antropocêntrica para a realidade maquinocêntrica constando-se que a participação cada vez mais efetiva dos sistemas de IA nas relações sociais, como agentes intermediários ou principalmente como protagonistas, fomenta maior relação entre homens e máquinas, deixando desta forma a clássica relação de homens entre si. Nunca a humanidade passou por essa experiência de ter um objeto que fosse capaz de pensar como os homens ou mesmo superá-los de forma mais rápida e eficaz.

Com a possibilidade de executar tarefas eficientes a IA necessita de enquadramento jurídico dado que é uma nova fonte de riscos para a sociedade.

Um dos problemas em relação à atribuição da responsabilidade no caso de IA, também é denominado de "problema de muitas mãos", está em saber se existe o nexo causal, pois pode haver a falta ou a dificuldade de identificação deste nexo causal entre a conduta do agente e o dano produzido e entre as diferentes partes envolvidas no processo, já que há um complexo sistema sociotécnico envolvido[28]. Existe a discursão sobre a identificação e a legitimidade quanto a criação da personalidade eletrónica[29], na medida em que dever-se-á reconhecer um novo centro de imputação de direitos e deveres.

De uma sociedade dos riscos monocausais para os riscos multicausais está-se diante de vários fatores de riscos que podem causar danos, tanto para o próprio utilizador como para demais pessoas conectadas na mesma rede referente a internet das coisas[30]. Esta nova realidade é caracterizada pela interconexão ancorada nas técnicas de IA, que pode causar vários transtornos. Como exemplo tem-se quando os dados que são fornecidos estão incorretos, defeito dos sensores, falha na internet, falta de atualização do *software*, quando existam vícios da tomada de decisões fruto de ciberataque, entre outros. Assim, necessita de nova abordagem da responsabilidade no direito.

---

28 Cfr. CANTARINI, Paola, **Personalidade jurídica eletrônica (*epersonality*) de aplicações de IA**, [Em linha]. [2022]. [Consult. 09 jan. 2023]. Disponível em WWW:<URL: https://www.migalhas.com.br/coluna/humanidades-e-novas-tecnologias/371055/personalidade-juridica-eletronica-epersonality-de-aplicacoes-de-ia>.

29 Cfr. Cfr. ANTUNES, Henrique Sousa, **Direito e inteligência artificial**, Lisboa: Universidade Católica, Editora. 2020. p. 31.

30 A internet das coisas é um sistema sem fio que tem se desenvolvido rapidamente em vários setores. É também conhecida no termo em inglês por *IoT (Internet of Things)* sendo a rede na qual dispositivos físicos, equipamentos, sensores e vários outros objetos podem se comunicar entre si sem necessariamente precisar de envolvimento humano. *Vide* GULATI, Kamal, **A review paper on wireless sensor network techniques in Internet of Things (IoT),** [Em linha]. [2022]. [Consult. 09 jan. 2023]. Disponível em WWW:<URL: https://www.sciencedirect.com/science/article/pii/S2214785321036439>:

Quanto às pessoas, observa-se o aumento do seu conhecimento, mas não conseguiu manter a inteligência necessária para utilizar consigo e para si, pois as máquinas atualmente podem ser programadas para aprenderem sozinhas (*machine learning*). A criação de uma inteligência não humana pode ser de difícil controlo pelas pessoas, mudará a noção de privacidade e de segurança, cibersegurança. O Direito da Cibersegurança passará a ser uma exigência horizontal no exercício das profissões jurídicas. As máquinas já passaram a realizar operações autónomas de associação (inteligência associativa), tratando-se de uma fonte de ação inteligente, não sendo apenas de automação ou internet das coisas. As máquinas e os algoritmos poderão substituir os humanos[31] brevemente e o direito é provocado pela dinâmica própria.

IV. Conclusões

Diante das fragilidades que o direito dever-se-á adequar, as máquinas não podem substituir os juízes e nem os advogados. A IA poderá de certeza auxiliar o judiciário, acelerando algumas tarefas administrativas que fornecem dados para análise de casos, sendo um aliado, um beneficiador não só do judiciário como da humanidade. No entanto, mesmo que muitos países estejam a utilizar os juízes robôs ou advogados eletrónicos, não significa que esta alternativa seja a melhor e a mais adequada à justiça, pois a sensibilidade e a fragilidade humana somente podem ser entendidas pelos humanos.

Este ano de 2023 pela primeira vez um advogado será substituído pela IA[32] num processo em tribunal nos EUA relacionado com multas de trânsito. Tendo em conta que esta relação de máquina e homem nunca foi tão discutida, é o homem capaz de analisar a melhor forma de melhorar a técnica jurídica auxiliado pelo seu pensamento crítico e o sentimento humano. Por mais que exista ou que esteja já em desenvolvimento uma IA dotada de "poderes" aproximados aos homens, a rapidez e a forma como consegue analisar os dados, decerto que são mais valias, porém, não é melhor que essas duas

31 Cfr. PINTO, Eduardo Vera-Cruz, **Filosofia para um Direito em espera. O Jurídico em tempos de Covid-19**. Prelo, gentilmente cedido pelo autor. 2020. p.13.
32 Cfr SPARKES, Matthew. **AI legal assistant will help defendant fight a speeding case in court**. [Em linha]. [2023]. [Consult. 10 jan. 2023]. Disponível em WWW:<URL: https://www.newscientist.com/article/2351893-ai-legal-assistant-will-help-defendant-fight-a-speeding-case-in-court/>.

características humanas, a análise crítica e o sentimento, que permitiu o desenvolvimento do direito atual.

V. Bibliografia

ANTUNES, Henrique Sousa, **Direito e inteligência artificial**, Lisboa: Universidade Católica, Editora. 2020.

AGGARWAL, Karan, Has the Future Started? The Current Growth of Artificial Intelligence, Machine Learning, and Deep Learning. **Iraqi Journal For Computer Science and Mathematics**. Vol 3, nº 1. pp-115-123. [Em linha]. [2022]. [Consult. 08 jan. 2023]. Disponível em WWW:<URL:

https://journal.esj.edu.iq/index.php/IJCM/article/view/100 >.

Conselho da Europa, **Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires**, [Em linha]. [2023]. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://www.coe.int/fr/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment >.

CASA BRANCA, **Projeto para uma Declaração de Direitos de IA** – Fazendo Sistemas Automatizados Funcionarem para o povo americano, [Em linha]. [2023]. [Consult. 11 jan. 2023]. Disponível em WWW:<URL: https://www.whitehouse.gov/ostp/ai-bill-of-rights/ >.

CANTARINI, Paola, **Personalidade jurídica eletrônica (*epersonality*) de aplicações de IA**, [Em linha]. [2022]. [Consult. 09 jan. 2023]. Disponível em WWW:<URL: https://www.migalhas.com.br/coluna/humanidades-e-novas-tecnologias/371055/personalidade-juridica-eletronica-epersonality-de-aplicacoes-de-ia >.

Discurso do Papa Francisco aos Juízes do Continente Americano, [Em linha]. [2019]. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://www.vatican.va/content/francesco/pt/speeches/2019/june/documents/papa-francesco_20190604_giudici-panamericani.html >.

EXAME, **Estudo revela que 13% da população dos EUA já teve *criptomoedas* em algum momento**, [Em linha]. [2022]. [Consult. 09 jan. 2023]. Disponível em WWW:<URL: https://exame.com/future-of-money/estudo-revela-que-13-da-populacao-dos-eua-ja-teve-criptomoedas-em-algum-momento/ >.

FREITAS, pedro Caridade de, **Portugal e a Comunidade Internacional – na Segunda Metade do Século XIX**, Lisboa: Quid Juris?, 2012.

GATLEWAR, Aditya, "Emergence of a New Dimension to the Judicial System:" "AI" – A Threat or Boon?, [Em linha]. []. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://disputescentre.com.au/emergent-of-a-new-dimension-to-the-judiciary-system-ai-a-threat-or-boon/ >.

GADAMER, Hans-Georg. **Verdade e Método II**. Complementos e índice. Tradução GIACHINI, Enio Paulo. Petrópolis: Vozes, 2011.

GULATI, Kamal, **A review paper on wireless sensor network techniques in Internet of Things (IoT),** [Em linha]. [2022]. [Consult. 09 jan. 2023]. Disponível em WWW:<URL: https://www.sciencedirect.com/science/article/pii/S2214785321036439 >.

Legal Information Institute, Separation of Powers [Em linha]. []. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://www.law.cornell.edu/wex/separation_of_powers_0 >.

Mr. Robot takes on law&order: Malaysia tests AI in judicial system, [Em linha]. [2022]. [Consult. 05 jan. 2023]. Disponível em WWW:<URL: https://www.dailysabah.com/life/mr-robot-takes-on-laworder-malaysia-tests-ai-in-judicial-system/news >.

MONARO, Merylin, MALDERA, Stéphanie, SCARPAZZA, Cristina, SATORI, Giuseppe e NAVARIN, Nilocoló, **Detecting deception through facial expressions in a dataset of videotaped interviews: A comparison between human judges and machine learning models**, [Em linha]. [2021]. [Consult. 06 jan. 2023]. Disponível em WWW:<URL: https://www-sciencedirect-com.translate.goog/science/article/abs/pii/S0747563221003861?_x_tr_sl=auto&_x_tr_tl=pt&_x_tr_hl=pt-PT&_x_tr_pto=wapp >.

Ministerio de Ciencia, Innovación y Universidades, **Estrategia Española de I+D+I en Inteligencia Artificial**, [Em linha]. [2019]. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact

=8&ved=2ahUKEwik-bLm8bX8AhWn9LsIHYsNBJ8QFnoECCcQAQ&url=https%3A%2F%2Fwww.ciencia.gob.es%2Fdam%2Fjcr%3A5af98ba2-166c-4e63-9380-4f3f68db198e%2FEstrategia_Inteligencia_Artificial_IDI.pdf&usg=AOvVaw14aqKAHWJ322Ilg1Jx0e7k >.

MOREIRA, Vital. Carta dos Direitos Fundamentais da União Europeia in PORTO, Manuel Lopes e ANASTÁCIO, Gonçalo, Coord. **Tratado de Lisboa Anotado e Comentado**. Cimbra: Almedina, 2012.

OLIVEIRA, Elsa Dias, Algumas considerações sobre a proteção do consumidor no mercado digital no âmbito do Direito da União Europeia, **Revista da Faculdade de Direito da Universidade de Lisboa**, número I, tomo I, [Em linha]. [2021]. [Consult. 08 jan. 2023]. Disponível em WWW:<URL:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj306TatLj8AhVMPewKHUH_DxIQFnoECAoQAQ&url=https%3A%2F%2Fwww.fd.ulisboa.pt%2Fwp-content%2Fuploads%2F2021%2F10%2FElsa-Dias-Oliveira.pdf&usg=AOvVaw3wFsljS_s6VQWlATmRph-W

Parlamento Europeu, A agenda do PE em 2023: energia renovável, transformação digital, migração, [Em linha]. [27-12-2022]. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://www.europarl.europa.eu/news/pt/headlines/eu-affairs/20221205STO60502/o-parlamento-em-2023-renovaveis-transicao-digital-migracao >.

PEREIRA, Maria Helena da Rocha, **Estudos sobre Roma Antiga A Europa e o Legado Clássico**, Coimbra: Fundação Calouste Gulbenkian Imprensa da Universidade de Coimbra, 2015.

PINTO, Eduardo Vera-Cruz, **Terra de Santa Maria – Terra-Mãe de Império Portugal**. Vol II, Santa Maria da Feira: Comissão de Vigilância do Castelo de Santa Maria da Feira. 2007.

PINTO, Eduardo Vera-Cruz, **Filosofia para um Direito em espera. O Jurídico em tempos de Covid-19**. Texto em aberto. 2020.

République Française, **L'intelligence artificielle (IA) dans les décisions de justice: une révolution en cours**, [Em linha]. [22-11-2021]. [Consult. 07 jan. 2023]. Disponível em WWW:<URL: https://www.vie-publique.fr/eclairage/277098-lintelligence-artificielle-ia-dans-les-decisions-de-justice >.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho

RIBEIRO, Renato, **Entenda o que é economia colaborativa e como aplicá-la**, [Em linha]. [2022]. [Consult. 08 jan. 2023]. Disponível em WWW:<URL: https://www.iugu.com/blog/o-que-e-economia-colaborativa >.

SIGA, https://siga.marcacaodeatendimento.pt/ >.

SPARKES, Matthew. **AI legal assistant will help defendant fight a speeding case in court**. [Em linha]. [2023]. [Consult. 10 jan. 2023]. Disponível em WWW:<URL: https://www.newscientist.com/article/2351893-ai-legal-assistant-will-help-defendant-fight-a-speeding-case-in-court/ >.

The World's First Robot Lawyer, [Em linha]. [2022]. [Consult. 04 jan. 2023]. Disponível em WWW:<URL: https://donotpay.com/>.

A Possibilidade de Aceder à Caixa de Correio Eletrónico Corporativo do Trabalhador: O Caso Específico da Rastreabilidade do PAN (*Primary Account Number*) Utilizado em Operações de Pagamento

ANA LÚCIA DA SILVA GONÇALVES

"A segurança dos pagamentos eletrónicos afigura-se como um aspeto fundamental para assegurar a proteção dos utilizadores e a promoção adequada do desenvolvimento do comércio eletrónico em condições concorrenciais."

(Nota preambular do Decreto-Lei n.º 91/2018, de 12 de novembro)

SUMÁRIO: I. Da escolha do tema; II. Do caráter reservado e confidencial da informação contida no correio eletrónico corporativo do trabalhador; III. Da possibilidade de acesso à informação contida no correio eletrónico corporativo do trabalhador. Da Deliberação da CNPD n.º 1638/2013; IV. Da possibilidade acesso ao correio eletrónico corporativo do trabalhador para rastrear o conteúdo PAN utilizado em operações de pagamento; V. Métodos De Controlo Não Invasivos: As Soluções *Data Loss Prevention*;

I. Da escolha do tema

O tema da segurança dos pagamentos eletrónicos, designadamente dos que são efetuados através de cartões bancários, tem constituído uma fonte de preocupação, em particular para os prestadores de serviços de pagamento, os utilizadores dos cartões e as marcas dos cartões, tendo vindo a ser elaboradas normas e recomendações destinadas a mitigar o risco de fraude associado a estes pagamentos.

Na verdade, há muitos prestadores de serviços de pagamento que, no âmbito da sua atividade, prestam serviços de aceitação e realização de operações bancárias com cartões quer da marca nacional Multibanco quer, ainda, das marcas internacionais, como a Visa e MasterCard, nas vertentes de débito e de crédito.

Estas operações realizam-se mediante a utilização de terminais de pagamento automático (TPA), físicos e virtuais (estes assentes em plataforma web), os quais servem, a título exemplificativo, para o pagamento de bens e/ou serviços nos comerciantes que contratualizam o serviço.

Tal serviço, internacionalmente designado por Acquiring, consubstancia a atividade através da qual o comerciante contrata com o prestador de serviços de pagamento/acquirer/adquirente a aceitação da marca de pagamento que este representa por forma a que seja autorizada a realização da operação de pagamento pelo titular do cartão. O acquirer assegura assim o pagamento (ou seja, adquire o crédito) ao comerciante e é reembolsado pela entidade emitente do cartão. Numa operação de compra, o acquirer/adquirente remunera a entidade emitente do cartão através de uma comissão que se designa por taxa de intercâmbio (ou "interchange fee")[1].

1 Tomámos de empréstimo a noção de *acquiring* constante do sítio eletrónico do Banco de Portugal (Cfr. https://clientebancario.bportugal.pt/pt-pt/glossario). Salientamos, não obstante, a existência de instrumentos normativos de âmbito comunitário que definem o conceito em causa: o Regulamento n.º 1409/2013, do Banco Central Europeu, de 28 de novembro de 2013 relativo às estatísticas de pagamento, o qual, na versão consolidada de 1 de janeiro de 2022, define o acquiring, no seu Anexo II, por remissão para o Regulamento (UE) n.º 2015/751 do Parlamento Europeu e do Conselho de 29 de abril de 2015 relativo às taxas de intercâmbio aplicáveis a operações de pagamento baseadas em cartões. Este Regulamento refere no seu considerando 30 que *"[a] atividade de adquirente* [leia-se acquirer] *é constituída por uma cadeia de operações que vão desde o início de uma operação de pagamento baseada num cartão até à transferência de fundos para a conta de pagamento do beneficiário. (...) Os intermediários que prestem parte dos serviços de aceitação de operações de pagamento baseadas em cartões, mesmo que não tenham uma relação direta com os beneficiários deverão ser abrangidos pela definição de adquirente nos termos do presente regulamento. (...)."*

Salientamos que no âmbito da atividade de *acquiring* as marcas dos cartões exigem ao acquirer o cumprimento de determinadas regras de segurança com o objetivo de se garantir a reserva das informações bancárias sigilosas relativas aos cartões bancários e, dessa forma, aumentar os controlos para prevenir a fraude.

Uma dessas normas de segurança respeita ao rastreio, monitorização e verificação de acessos dos dados dos cartões, nos quais se incluiu o *Primary Account Number* (PAN), isto é, o número do cartão de débito e de crédito. Esta norma de segurança decorre do *"Payment Card Industry (PCI) DataSecurity Standard - Requirements and Security Assessment Procedures*"[2]/[3]/[4]: o requisito 10 estabelece a necessidade de implementar mecanismos que permitam rastrear as atividades das pessoas com acesso aos dados dos cartões e o requisito 3 estabelece, de forma expressa, que o PAN não deve circular através de *e-mails*, a menos que se encontre protegido, designadamente, através de métodos de encriptação.

Com efeito, uma das questões que se poderá colocar no âmbito da implementação de mecanismos que permitem rastrear as atividades dos trabalhadores com acesso a dados dos cartões guardados nos servidores da propriedade do acquirer/entidade empregadora é a de saber se o acquirer/entidade empregadora poderá, com vista a rastrear o PAN utilizado em operações de pagamento, aceder ao correio eletrónico corporativo do colaborador, isto é, ao correio eletrónico profissional que lhe foi atribuído no sentido de garantir o cumprimento do supramencionado requisito 3 do *"Payment Card Industry (PCI) DataSecurity Standard - Requirements and Security Assessment Procedures"*. Esta questão é particularmente relevante, uma vez que o trabalhador pode, intencionalmente ou não, exportar os dados dos cartões que estão

---

2 *"The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. The PCI DSS was created jointly in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express."* (*https://www.techtarget.com/searchsecurity).*

3 De acordo com a parte introdutória do "Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures": "*The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).*

4 Consultámos, para a elaboração deste trabalho, a versão 3.2.1.

guardados nos servidores da propriedade do acquirer/entidade empregadora[5], incluindo o PAN utilizado em operações de pagamento, para o seu correio eletrónico corporativo, potenciando, por essa via, a atividade fraudulenta (do próprio ou de terceiros): nota-se que a facilidade e rapidez com que a informação circula hoje através do correio eletrónico (e, como tal, também através do correio eletrónico corporativo) tornou-o um dos principais alvos de ciberataques ou de acesso ilegítimo[6], pelo que poderá constituir um risco, designadamente financeiro, reputacional e de *compliance*, a circulação de dados dos cartões em correios eletrónicos corporativos.

Face ao exposto, a questão que nos propomos resolver, através do presente trabalho, é a de saber se, à luz da legislação portuguesa, o acquirer/entidade empregadora pode aceder ao correio eletrónico corporativo do trabalhador para rastrear o PAN utilizado em operações de pagamento.

II. Do caráter reservado e confidencial da informação contida no correio eletrónico corporativo do trabalhador

O artigo 34.º da Constituição da República Portuguesa (CRP) consagra, como direito fundamental, a inviolabilidade do domicílio e da correspondência: refere expressamente o número 1 desta disposição legal que o domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis.

---

5 Nota-se que as informações dos clientes que sejam pessoas singulares a que os bancos têm acesso poderão ser qualificados como dados pessoais na aceção do art. 4.º/1 do Regulamento Geral da Proteção de Dados (RGPD), merecendo, desde logo, por via dessa qualificação, proteção reforçada quanto ao seu tratamento nos termos do artigo 32.º do RGPD, incluindo a adoção das seguintes medidas, consoante o que for adequado: a pseudonimização e a cifragem dos dados pessoais; a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico e um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

6 No artigo 6.º da Lei do Cibercrime, aprovada pela Lei n.º 109/2009, de 15 de setembro, na versão conferida pela Lei n.º 79/2021, de 24 de novembro, encontra-se previsto o crime de acesso ilegítimo. De acordo com o n.º 1 "[q]*uem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias*." Há circunstâncias que poderão agravar a moldura penal tipificada, das quais destacamos o conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei e a obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento (cfr. artigo 6.º, n.ºs 2-5).

Este direito fundamental decorre de um outro – o direito à reserva da intimidade da vida privada e familiar - que goza também de proteção constitucional nos termos do artigo 26.º da CRP. De acordo com esta norma a todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação, prevendo-se ainda que a lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.

Os supramencionados direitos fundamentais têm ramificações em vários diplomas legais infraconstitucionais. Em matéria laboral, é relevante o artigo 22.º do Código do Trabalho (CT), com a epígrafe *"Confidencialidade de mensagens e de acesso a informação",* cuja transcrição efetuamos na íntegra na medida em que a norma em causa constituirá uma peça angular na apreciação da questão que nos propusemos resolver. Dispõe, assim, esta norma, no seu número 1, que *"[o] trabalhador goza do direito de reserva e confidencialidade relativamente ao conteúdo das mensagens de natureza pessoal e acesso a informação de caráter não profissional que envie, receba ou consulte, nomeadamente através do correio eletrónico"*. Acrescenta o número 2 da mesma norma que "[o] *disposto no número anterior não prejudica o poder do empregador estabelecer regras de utilização dos meios de comunicação na empresa, nomeadamente do correio eletrónico.*"

A doutrina que tem refletido sobre o conteúdo normativo do artigo 22.º do CT afirma que esta disposição legal abrange *"não só as cartas que o trabalhador envie ou receba, como as mensagens que receba ou envie através do telefone, bem como as mensagens de correio eletrónico que o trabalhador envie ou receba, e ainda quaisquer outras mensagens enviadas ou recebidas, utilizando meios da empresa, independentemente do meio tecnológico em causa, que tenham caráter pessoal. A mais, incluindo no seu âmbito de aplicação o acesso a informação de caráter profissional que*

o trabalhador envie, receba ou consulte, a norma abrange também os websites ou sítios da Internet a que o trabalhador aceda, utilizando meios do empregador."[7]

Da interpretação que é feita pela doutrina, e na qual nos revemos, podemos concluir que o direito à reserva e confidencialidade previsto nesta norma, abrange, e para o que ora tem utilidade, não apenas a informação pessoal[8]/[9], mas também a informação de cariz profissional, contida no correio eletrónico corporativo. Não será, em nossa opinião, alheia a esta interpretação o facto de poder ser difícil, *a priori*, individualizar ou segmentar a informação que é pessoal daquela que é estritamente profissional: fazemos notar que, mesmo em relação a esta última, embora respeite à vida da empresa, o trabalhador pode ter querido tratá-la efetivamente com intenção de confidencialidade[10]. Daí que toda a informação contida no endereço de correio eletrónico corporativo do trabalhador seja, à partida, reservada e confidencial.

Também a jurisprudência dos nossos tribunais superiores se pronuncia no mesmo sentido: conforme sustentado, quer no Acórdão do Supremo Tribunal de Justiça, de 05.07.2007, quer, ainda, no Acórdão do Tribunal da Relação de Lisboa de 05.06.2007 *"A falta de referência prévia, expressa e formal da "pessoalidade" da mensagem, não afasta a tutela do art. 21.º, n.º 1, do CT" [atual artigo 22.º, n.º 1, do CT].* De igual modo, o Acórdão do Tribunal da Relação do Porto de 15.12.2016 faz bastião do seguinte entendimento*:"(…) não pode o empregador aceder ao conteúdo dos emails, e dos seus anexos, enviados ou rececionados nessa conta, mesmo que não estejam marcados como pessoais (…)."*

---

7 Cfr. Código do Trabalho Comentado, da autoria de Diogo Vaz Marecos, Almedina, 2023, 5.ª Edição, página 157.

8 Como assinala DIOGO VAZ MARECOS, op. cit., páginas 157 e 158 "[c]*om efeito, o desenvolvimento tecnológico, cultural, social e económico determina que a esfera privada do trabalhador acabe por penetrar no seu local de trabalho durante o tempo de trabalho, não raro sem que o trabalhador o consiga evitar. A própria dignidade da pessoa humana, princípio estruturante e matriz de vários direitos constitucionalmente consagrados, não obsta a tal penetração conduzindo a semelhante resultado."*

9 Como esclarece ANTÓNIO MONTEIRO FERNANDES "[s]*e o empregador, no uso da faculdade a que se refere o artigo 22.º/2, estabelece regras de utilização dos meios de comunicação da empresa, essas regras não podem ir ao ponto de privarem o trabalhador da comunicação pessoal com o exterior – por exemplo, proibindo totalmente o uso do correio eletrónico com mensagens de natureza não profissional. Essas regras podem definir restrições – "imposição de limites, tempos de utilização, acessos ou sítios vedados aos trabalhadores, mas não a exclusão absoluta da comunicação pessoal."* Cfr. ANTÓNIO MONTEIRO FERNANDES, "Direito do Trabalho", 2020, 20.ª Edição, Almedina, pág. 301.

10 Assinalando a possibilidade de determinadas mensagens relativas à vida da empresa poderem ser enviadas com intenção de confidencialidade, confira-se o emblemático Acórdão do Supremo Tribunal de Justiça (STJ), de 05/07/2007, Relator Mário Pereira.

Tomando como assente que a informação contida no *e-mail* corporativo do trabalhador tem caráter reservado e confidencial, cabe questionar, considerando o tema do nosso trabalho, se o acesso à caixa de correio eletrónico corporativo do trabalhador está irremediavelmente vedado à entidade empregadora[11].

III. Da possibilidade de acesso à informação contida no correio eletrónico corporativo do trabalhador. Da Deliberação da CNPD n.º 1638/2013.

Embora do número 1 do artigo 22.º do CT decorra o caráter reservado e confidencial da informação contida no *e-mail* corporativo do trabalhador, o Código do Trabalho não parece assumir uma solução normativa irredutível no sentido de não ser, de todo, possível aceder ao *e-mail* corporativo do trabalhador, já que no número 2 do artigo 21.º do CT está expressamente previsto que a reserva e confidencialidade de que goza a informação contida no e-mail do trabalhador *"não prejudica o poder de empregador estabelecer regras de utilização dos meios de comunicação na empresa, nomeadamente do correio eletrónico."* Daqui parece, pois, resultar que o legislador não quis vedar de forma absoluta a possibilidade de acesso ao *e-mail* corporativo do trabalhador. No entanto, não podemos deixar de observar que o legislador não consagrou em que termos e condições é que a entidade empregadora o poderá fazer.

A questão, embora não se encontre resolvida pelo legislador, foi objeto de pronúncia pela Comissão Nacional de Proteção de Dados (CNPD), a qual, através da Deliberação n.º 1638/2013[12], aplicável aos tratamentos de dados pessoais decorrentes do controlo de utilização para fins privados das tecnologias de informação e comunicação no contexto laboral, que revogou a deliberação de 29 de outubro de 2002, sobre o tratamento de dados em centrais telefónicas, o controlo de *e-mail* e do acesso à Internet, estabeleceu as condições gerais em que o tratamento de dados pode ser feito.

---

11 Da nossa apreciação excluímos a possibilidade de acesso ao *e-mail* pessoal do colaborador, uma vez que é consensual que fica de fora do espectro do artigo 22.º, n.º 2 do CT qualquer mensagem ou comunicação que o trabalhador efetue através de contas de correio eletrónico, de redes sociais ou de quaisquer outras contas às quais o trabalhador aderiu a título pessoal, ainda que a elas aceda através do computador da empresa. Está absolutamente vedada ao empregador qualquer forma de controlo do conteúdo da informação da área privativa do trabalhador enquanto utilizador de um daqueles serviços (cfr. Deliberação da CNPD n.º 1638/2013).

12 Disponível para consulta em https://www.cnpd.pt/media/kuqbxfdv/delib_controlo_tics.pdf.

De forma sintética de acordo com a deliberação da CNPD:

- O confronto entre o vínculo laboral e a possibilidade legal de tratamento de dados por parte do empregador deve cumprir os princípios do fim, da adequação, da necessidade e da proporcionalidade, da transparência e da boa-fé.

- Os termos em que esse controlo pode ser efetuado, ou seja, a delimitação das condições do tratamento de dados e a especificação das formas de controlo, uma vez verificados os pressupostos enunciados acima, de acordo com a deliberação da CNPD, devem constar de Regulamento interno porque se trata de matéria subsumível ao artigo 99.º do CT.

- Independentemente das regras definidas pela empresa para a utilização do correio eletrónico para fins privados, o empregador não tem o direito de abrir, automaticamente, o correio eletrónico dirigido ao trabalhador.

- O facto de certas mensagens ficarem gravadas em servidores da propriedade do empregador não lhe dá o direito de aceder àquelas mensagens, as quais não perdem a sua natureza pessoal ou confidencial, mesmo quando esteja em causa investigar e provar uma eventual infração disciplinar, embora deva ser exigida aos trabalhadores a criação de pastas próprias, devidamente identificadas, onde o trabalhador arquive os correios eletrónicos de conteúdo pessoal que constam da caixa de correio profissional.

- A entidade empregadora deve escolher metodologias de controlo não intrusivas, que estejam de acordo com os princípios previamente enunciados, *maxime*, o da proporcionalidade, e que sejam do conhecimento dos trabalhadores.

- A entidade empregadora não deve fazer um controlo permanente e sistemático do correio eletrónico dos trabalhadores: o controlo deve ser pontual e direcionado para as áreas e atividades que apresentem um maior "risco" para a empresa.

- O grau de autonomia do trabalhador e a natureza da atividade desenvolvida, bem como as razões que levaram à atribuição de um endereço de correio eletrónico àquele, devem ser tomadas em conta, decisivamente, em relação à forma como vão ser exercidos os poderes de controlo. Também no que diz respeito ao correio eletrónico, o segredo profissional específico que impende sobre o empregado (v.g., sigilo médico, sigilo profissional de advogado, ou segredo das fontes) tem de ser preservado, não

devendo o conteúdo das suas mensagens ser acedido em circunstância alguma nem os dados de tráfego reveladores dos remetentes ou destinatários exteriores ser objeto de tratamento para fins de controlo.

- Por princípio, o controlo dos correios eletrónicos deve ser realizado de forma aleatória. Sublinha-se que a necessidade de deteção de vírus ou de outro tipo de software malicioso não justifica, só por si, a leitura dos correios eletrónicos recebidos. A entidade empregadora pode adotar os procedimentos necessários para – sempre com o conhecimento dos trabalhadores – fazer uma «filtragem» de certos ficheiros que, pela natureza da atividade desenvolvida pelo trabalhador podem indiciar, notoriamente, não se tratar de correios eletrónicos de serviço (v.g., ficheiros «.exe», .mp3 ou de imagens).

- Também eventuais controlos fundamentados na prevenção ou deteção da divulgação de segredos comerciais devem ser direcionados, exclusivamente, para as pessoas que têm acesso a esses segredos e apenas quando existam fundadas suspeitas daquele facto.

- É de diferenciar claramente o grau de exigência e de rigor em relação ao controlo das mensagens expedidas e recebidas, uma vez que a entrada de correspondência na caixa de correio eletrónico do trabalhador é independente da sua vontade. Por isso, devem ser dadas instruções ao trabalhador para que apague as mensagens eventualmente recebidas que contrariem o Regulamento Interno.

- O acesso ao correio eletrónico deverá ser o último recurso a utilizar pela entidade empregadora, sendo necessário que seja feito na presença do trabalhador visado e, de preferência, na presença de um representante da comissão de trabalhadores ou de outra estrutura representativa (v.g., delegados sindicais-) ou de alguém indicado pelo trabalhador. O referido acesso deve limitar-se à visualização dos endereços dos destinatários, o assunto, a data e hora do envio, podendo o trabalhador – se for o caso – especificar a existência de algumas mensagens de natureza privada e que não pretende que sejam lidas pela entidade empregadora, caso ainda não tenha tido a oportunidade de os eliminar ou arquivar em pasta específica. Perante tal situação, a entidade empregadora tem de abster-se de consultar o conteúdo das mensagens de correio eletrónico, uma vez que o mero registo do envio das mesmas cumpre o objetivo do tratamento. Eventual consulta constituirá um acesso não autorizado, porque extravasa a finalidade do tratamento.

- Impõe-se ao empregador (e qualquer seu representante) que, tendo consciência da natureza pessoal de uma comunicação, desista da leitura do seu conteúdo e não o divulgue.

- É também necessário que sejam definidos procedimentos internos relativamente ao conteúdo de caixas de correio eletrónico de trabalhadores que saem da empresa. Nestes casos, deve dar-se um prazo ao trabalhador para retirar o conteúdo de cariz pessoal dos arquivos do correio eletrónico, decorrido o qual o empregador deve eliminar a conta, para evitar que continue em funcionamento um endereço de correio eletrónico que já não é acedido pelo seu titular. Além disso, o empregador deve assegurar que o mesmo endereço eletrónico não será ulteriormente atribuído a outro trabalhador (*email heritage*).

IV. Da possibilidade acesso ao correio eletrónico corporativo do trabalhador para rastrear o conteúdo PAN utilizado em operações de pagamento

A questão que se pretendeu resolver através do presente trabalho prende-se com a possibilidade do acquirer/entidade empregadora poder controlar a atuação do trabalhador credenciado a aceder a dados dos cartões, em concreto a rastrear o PAN utilizado em operações de pagamento no seu *e-mail* corporativo. Este controlo visa mitigar o risco de o utilizador (intencionalmente ou não) exportar para o seu e-mail corporativo informação (em concreto, o PAN) que colheu dos servidores propriedade do acquirer/entidade empregadora. Nota-se que uma eventual exportação do PAN para o *e-mail* corporativo do trabalhador poderá pôr em causa o cumprimento dos requisitos do *"Payment Card Industry (PCI) DataSecurity Standard - Requirements and Security Assessment Procedures"*, em concreto o requisito 3: conforme vimos, este requisito veda a circulação do PAN por *e-mail*.

Atenta a exposição sequencial que temos vindo a fazer será possível, em nossa opinião, monitorizar a informação PAN no correio eletrónico corporativo dos trabalhadores cumpridos que estejam determinados requisitos. Com efeito, será possível efetuar tal monitorização mediante:

(i) Implementação de uma metodologia de controlo não intrusiva que filtre apenas o conteúdo "PAN", o qual é, aliás, um conteúdo codificado e identificável como não sendo, indiciariamente, um conteúdo de cariz pessoal.

(ii) Este rastreio tem de ser o único meio possível de cumprimento das normas de segurança da informação e proteção de dados sensíveis de terceiros, sendo portanto necessário e proporcional aos fins visados. Neste caso o direito à reserva da vida privada do trabalhador está limitado pelo confronto com outros direitos, designadamente o relativo ao cumprimento de procedimentos de segurança impostos no âmbito do exercício da atividade de acquiring e que se destinam a evitar atividades ilícitas.

(iii) O controlo tem de ser pontual, não podendo ter uma rotina periódica: é pontual e aleatório, incidindo numa atividade de risco (dados de cartões).

(iv) O trabalhador tem de conhecer que o acquirer/entidade empregador poderá rastrear o conteúdo PAN no seu *e-mail* corporativo.

(v) Esta forma de controlo é aquela que menor impacto tem de ter na situação jurídico-constitucional do trabalhador, designadamente nos seus direitos fundamentais, em especial no seu direito à reserva da vida privada.

(vi) A consulta a efetuar não poderá ser individualizada. A consulta terá de ser feita, de forma aleatória, aos postos dos utilizadores credenciados para aceder a essa informação. A metodologia empregue tem de "varrer" aleatoriamente os postos de trabalho e só quanto a dado (no caso, o PAN) previamente fixado; salvo claro está se num determinado posto for gerado um alerta. Aí já estaremos no tratamento de uma situação indiciária de fraude cujo tratamento correrá os seus termos devidamente regulamentados.

(vii) Uma vez que se irá aceder a determinado conteúdo, da caixa de correio corporativo do trabalhador, mais que o seu conhecimento, salvo melhor opinião, dever-se-á obter o seu consentimento, considerando que se trata de uma limitação voluntária a um direito de personalidade (artigo 81.º/1 do Código Civil).

(viii) Deve ser elaborado um Regulamento Interno que justifique o acesso, o tipo de acesso, conteúdo, requisitos, limites, acessos, garantias do trabalhador, consequências da verificação de um alerta de evento fraudulento que se conclua existir, salvo se devidamente esclarecido e justificado pelo trabalhador;

(ix) O Regulamento deve ser submetido a parecer da Comissão de Trabalhadores.

V- Métodos De Controlo Não Invasivos: As Soluções *Data Loss Prevention*

Conforme acima referimos, em nossa opinião será possível monitorizar a informação PAN no correio eletrónico corporativo dos trabalhadores cumpridos que estejam determinados requisitos. Um dos requisitos que apontámos prende-se com a implementação de uma metodologia de controlo não intrusiva que filtre apenas o conteúdo "PAN".

Uma das metodologias que poderá ser ponderada para os efeitos aqui relevantes são as designadas soluções Data Loss Prevention (DLP).

Salientamos que as soluções DLP não são um *software*, mas sim um conceito: tal conceito dá nome a um conjunto de tecnologias e práticas destinadas a proteger dados confidenciais com vista a reduzir o acesso não autorizado e a perda de dados. As soluções DLP são, assim, "desenhadas" para identificar, monitorizar e proteger informações confidenciais em todo o seu ciclo de vida dentro de uma organização.

São habitualmente identificadas três tipologias de soluções DLP, a saber[13]:

(i) **Network DLP**: são ferramentas ou plataformas de software e/ou hardware que integram uma rede corporativa para monitorizar o tráfego, podendo monitorizar internamente a circulação desses dados a fim de não facilitar a saída de dados de maneira suspeita ou não autorizada.

(ii) **Endpoint DLP:** monitoriza os dados em uso pelos utilizadores entre computadores, servidores e até dispositivos removíveis como pen-drive por

13 A enunciação da tipologia aqui referida seguiu de perto a informação constante do seguinte sítio eletrónico: https://www.jusbrasil.com.br/artigos/data-loss-prevention/927310859.

exemplo. Após instalado e configurado no posto de trabalho, ele monitoriza os dados em uso daquele posto de trabalho.

(iii) **Storage DLP:** monitoriza os arquivos armazenados e/ou compartilhados. Níveis de restrição de acesso podem ser aplicadas e relacionadas as credenciais de cada utilizador. Além disso, e dependendo do produto ou serviço adquirido é possível verificar pontos sensíveis que podem ocasionar um acesso não autorizado.

Considerando a tipologia de soluções DLP acima identificadas, cremos que para efeitos de rastrear o PAN utilizado em operações de pagamento no correio eletrónico corporativo do trabalhador poderá ser, então, ponderada a adoção de uma solução Endpoint DLP.

Não obstante, damos nota, por nos parecer relevante, que a adoção desta solução DLP (ou outras equivalentes) não deverá ser desacompanhada de uma ação pedagógica e sensibilizadora junto dos trabalhadores no sentido de ser reforçada a importância da segurança da informação e do cumprimento das práticas, políticas e formações implementadas pela organização para esse efeito: *"as pessoas importam tanto quanto, senão mais, do que a tecnologia, e podem causar elevados prejuízos às organizações."*[14]

O sucesso da segurança da informação da organização depende, pois, e já em tom conclusivo, de uma combinação equilibrada entre o elemento técnico, com a adoção de soluções e ferramentas técnicas robustas, e o elemento humano, mediante uma consciencialização da importância, por parte dos trabalhadores, da segurança da informação e da necessidade de, para o efeito, cumprirem de forma escrupulosa todas as diretrizes emanadas pela organização, quer estas estejam relacionadas com políticas, procedimentos ou formações.

14 Cfr. TELMA KIDY TAVARES, "O Fator Humano na Segurança de Informação nas Organizações", Dissertação para a obtenção do grau de Mestre em "Segurança da Informação e Direito no Ciberespaço", Dezembro 2017, página 1.

O Sistema de Governação no Contexto da Cibersegurança – Um Modelo Inspirado no Setor Segurador

ANA MOITINHO BYRNE[1]

GONÇALO NUNO BAPTISTA DE SOUSA

1 As opiniões expressas neste artigo não vinculam a entidade patronal da autora e, como tal, por elas só a autora é responsável.

SUMÁRIO: Resumo; I. Enquadramento; II. A segurança da informação e a governação das TIC – resenha histórica; III. Princípios basilares aplicáveis ao sistema de governação para gestão da cibersegurança; IV. Responsabilização e envolvimento do órgão de administração; V. Definição de uma estratégia e de uma política de cibersegurança e concretização através de processos e procedimentos; VI. Estrutura organizacional adequada, alocação de responsabilidades clara e transparente e autonomia e independência das funções associadas; VII. Enquadramento dos riscos de cibersegurança no sistema de gestão de riscos; i) Realização de testes e simulacros; ii) Sujeição a auditorias periódicas; iii) Alocação dos recursos humanos e financeiros necessários e adequados; iv) Cultura de cibersegurança, sensibilização e formação; VIII. Conclusão; IX. Referências.

RESUMO:

No presente artigo, pretende-se assinalar a importância de implementar um sistema de governação no contexto da gestão da cibersegurança. Para o efeito, sublinha-se o facto de que a segurança da informação (com especial foco no ciberespaço) não se esgota nas medidas operacionais nem no cumprimento, ainda que escrupuloso, dos requisitos técnicos aplicáveis e que há um outro conjunto de aspetos igualmente cruciais que, ao assegurar uma visão holística e integrada da organização, permitem uma adequada gestão da cibersegurança – o sistema de governação.

Assim, o artigo elenca e descreve, ainda que de forma genérica, alguns princípios de governação que foram identificados como essenciais num contexto de gestão da cibersegurança.

Palavras-chave: segurança da informação; cibersegurança; gestão da cibersegurança; sistema de governação; governação da cibersegurança.

ABSTRACT:

The aim of this article is to highlight the importance of implementing a governance system in the context of cybersecurity management. To this end, it highlights the fact that information security (with a special focus on cyberspace) is not

limited to operational measures or compliance, albeit scrupulous, of the applicable technical requirements and that there is another set of equally crucial aspects which, by ensuring a holistic and integrated vision of the organization, allow for adequate cybersecurity management - the governance system.

The article therefore lists and describes, albeit in general terms, some of the governance principles that have been identified as essential in a cybersecurity management context.

Keywords: *information security; cybersecurity; cybersecurity management; governance system; cybersecurity governance.*

I. Enquadramento

A cibersegurança[2] – enquanto "*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*" – é um tema que está na moda.

A esta constatação não é certamente alheio o facto de, nos últimos anos, ter ocorrido um conjunto de incidentes cibernéticos importantes, alguns com efeitos à escala global[3], que vieram colocar a cibersegurança na agenda das organizações e os riscos a ela ligados nos *rankings* mundiais de riscos[4].

Por outro lado, com a publicação do Regulamento Geral sobre a Proteção de Dados (RGPD)[11], em 2018, a proteção dos dados pessoais e a sua reafirmação enquanto direito fundamental, especialmente no seio da União Europeia, veio trazer uma nova dimensão à importância de assegurar medidas de cibersegurança adequadas para esse efeito[17].

Mais recentemente, a pandemia do coronavírus SARS-CoV-2, que provoca a doença COVID-19, provocou uma forte aceleração no processo de transformação digital da economia, ao implicar a adoção do teletrabalho como regra (nos casos em que as funções são compatíveis com esse modelo) e, consequentemente, obrigar as organizações a reinventar-se e migrar os seus *modi operandi* para formatos quase ou mesmo totalmente assentes em tecnologias de informação e comunicação (TIC).

Esta evolução tem vindo a ser acompanhada pelo reforço (e, em alguns casos, construção) de um quadro legal e regulamentar que procura acomodar e dar resposta aos crescentes desafios em matéria de segurança da informação em geral e de cibersegurança em particular.

---

2 O presente artigo adota o conceito de "cibersegurança" enunciado na Estratégia Nacional de Segurança do Ciberespaço – 2019-2023, aprovada pela Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho de 2019.

3 Considere-se, por exemplo, o caso dos ataques de *malware* WannaCry e NotPetya, em 2017.

4 Vd. *The Global Risks Report 2022*, *17th Edition*, *World Economic Forum*. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf.

Contudo, no presente artigo pretende-se dar destaque a uma componente da gestão da cibersegurança que ainda é, muitas vezes, considerada acessória: a respetiva governação. Com efeito, ao conceito de cibersegurança vem – e bem – associada a gestão dos riscos a que os sistemas de TIC estão expostos e as medidas técnicas e operacionais que é necessário implementar para os endereçar. Mas há uma componente que não pode ser descurada: se essas mesmas medidas não foram enquadradas por um adequado sistema de governação, com responsabilidades claramente definidas e comunicadas, processos e procedimentos documentados e testados, envolvimento de pessoas com as competências necessárias, entre outros aspetos igualmente fundamentais, a cibersegurança fica em risco.

II. A segurança da informação e a governação das TIC – resenha histórica

As preocupações com a segurança da informação não são recentes no contexto da gestão das organizações. Numa perspetiva histórica, constata-se que, inicialmente, as medidas de proteção se aplicavam sobretudo à informação em suporte físico.

Com efeito, no âmbito nacional, a SEGNAC 1[12], de 1988, que apresenta um conjunto de medidas relativas ao tratamento de matérias classificadas, no respetivo Capítulo 10 faz uma referência à "*proteção das informações classificadas e postas em memória nos sistemas e redes de tratamento automático de dados*" (ainda que remeta esta matéria para outras instruções específicas). De resto, aquela Instrução incide, sobretudo, nos procedimentos relacionados com a segurança física e das instalações.

A SEGNAC 2[13], publicada no ano seguinte, introduz os conceitos de "segurança eletrónica (ELSEC)", "segurança informática" e "segurança das telecomunicações (COMSEC)". Contudo, só as SEGNAC 3[15] (1994) e SEGNAC 4[14] (1990) abordam já explicitamente matérias relacionadas com a segurança das telecomunicações e a segurança informática, respetivamente.

Mas é também nessa altura, i.e., na transição para a década de 1990, que começam a surgir os primeiros quadros de referência internacionais (*frameworks*) que abordam a ideia de associar as TIC a mecanismos de governação (*IT Governance*), incorporando-os num conjunto de boas práticas que assegurem a fiabilidade dos sistemas de

informação. É o caso, por exemplo, da metodologia ITIL[5] (1989), publicada pela agência britânica *Central Computer and Telecommunications Agency* (CCTA), e da COBIT[6] (1996), desenvolvida pela associação norte-americana *Information Systems Audit and Control Association* (ISACA), com o intuito de apoiar a auditoria das tecnologias de informação como suporte à auditoria financeira. Já no início do milénio foram publicadas as Orientações da Organização para a Cooperação e Desenvolvimento Económico (OCDE) sobre segurança da informação em sistemas e redes, que desenvolvem a ideia da "cultura de segurança"[8] (2002), e a norma internacional ISO/IEC 27001[7] relativa aos requisitos para sistemas de gestão de segurança da informação, que na sua primeira versão propõe a integração do sistema de gestão de segurança da informação[8] numa abordagem holística aos riscos de uma organização, incluindo a atribuição de responsabilidades à gestão (2005)[7]. Todos estes *frameworks* evoluíram e são hoje robustos quadros de referência para a gestão da cibersegurança, extravasando o âmbito estrito das TIC.

Já mais recentemente, no espaço europeu, em fevereiro de 2013, foi adotada a Estratégia da União Europeia para a Cibersegurança[3], na altura acompanhada por uma proposta de Diretiva, mais tarde publicada como Diretiva relativa à segurança das redes e da informação (Diretiva SRI[6] ou, no acrónimo anglo-saxónico, NIS)[9] e acolhida ao nível nacional como Lei[7], em 2018[10].

Na Diretiva SRI, é estabelecida a obrigação de os Estados-membros adotarem uma Estratégia nacional de segurança das redes e dos sistemas de informação que contemple, entre outros aspetos, "*um quadro de governação para alcançar os objetivos e as prioridades da estratégia nacional de segurança das redes e dos sistemas de informação, incluindo as funções e responsabilidades dos organismos governamentais*

5 ITIL – *Information Technology Infrastructure Library*.
6 COBIT – *Control Objectives for Information and Related Technology*.
7 ISO/IEC – *International Organization for Standardization/International Electrotechnical Commission*.
8 *Information Security Management System* (ISMS).
9 Esta Diretiva está atualmente em processo de revisão, cf. informação disponível em: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.
10 Importa referir que este quadro legal tem sido complementado com regulamentação específica, como é o caso do Decreto-Lei n.º 65/2021, de 30 de julho, que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE)[4].

e dos outros intervenientes relevantes"[11]. Consequentemente, em junho de 2019, é publicada uma nova versão da Estratégia Nacional de Segurança do Ciberespaço, para o triénio 2019-2023[18], que vem reforçar algumas das matérias que já constavam da versão anterior[16], designadamente em matéria de estrutura de segurança do ciberespaço e de prevenção, educação e sensibilização.

Ainda num contexto de convergência europeia, em 2019, o Centro Nacional de Cibersegurança (CNCS) publicou o Quadro Nacional de Referência para a Cibersegurança (QNRCS), que materializa um conjunto de boas práticas com vista a permitir às organizações "*reduzir o risco associado às ciberameaças, disponibilizando as bases para que qualquer entidade possa, de uma forma voluntária, cumprir os requisitos mínimos de segurança das redes e sistemas de informação, (...) incluindo a organização necessária para a sua gestão*"[12].

Considerando que as ideias defendidas no presente artigo se inspiram no setor segurador, não se poderia encerrar esta secção sem fazer referência à proposta de Regulamento relativo à resiliência operacional digital do setor financeiro[10], que procura agregar num único instrumento legal, aplicável a 20 tipos distintos de instituições financeiras, incluindo empresas de seguros e resseguros, um conjunto de regras e requisitos com o objetivo de "*instituir um quadro pormenorizado e abrangente para a resiliência digital operacional das entidades financeiras da UE*"[13]. Em especial, há que sublinhar o artigo 4.º da proposta, exclusivamente dedicado aos requisitos relacionados com a governação e com a organização das entidades financeiras abrangidas.

III. Princípios basilares aplicáveis ao sistema de governação para gestão da cibersegurança

A presente secção apresenta um conjunto de princípios que são classificados pela autora como basilares para assegurar que a gestão da cibersegurança é suportada por um sistema de governação robusto.

11 Cf. Artigo 7.º, n.º 1, alínea b) da Diretiva SRI.
12 Prefácio do Quadro Nacional de Referência para a Cibersegurança (QNRCS).
13 Cf. Exposição de motivos da proposta de Regulamento DORA.

Os princípios apresentados não devem ser confundidos com as etapas de gestão da cibersegurança preconizadas por algumas abordagens metodológicas. Por exemplo, o QNRCS[2] organiza as medidas de segurança em cinco objetivos de segurança: identificar, proteger, detetar, responder e recuperar. Também a proposta de Regulamento DORA[10] apresenta um conjunto de funções específicas para efeitos da gestão do risco das TIC, que incluem a identificação, a proteção e prevenção, a deteção, a resposta e recuperação, a aprendizagem e evolução, e a comunicação. Ao invés, os princípios abaixo enunciados estão organizados e agrupados enquanto mecanismos e estruturas de governação que apoiam uma adequada gestão da cibersegurança, podendo (e devendo) cruzar-se com aquelas etapas em vários momentos.

Adicionalmente, importa referir que as orientações ora apresentadas devem ser consideradas à luz do princípio da proporcionalidade, ou seja, a sua adequação deve sempre ser aferida numa perspetiva idiossincrática, tendo por base as características específicas de cada organização, incluindo, entre outros aspetos, a sua dimensão e os riscos de cibersegurança concretos a que está exposta.

Como já referido anteriormente, as características do sistema de governação que inspiram os princípios enunciados neste artigo têm por base os requisitos aplicáveis ao setor segurador e, mais concretamente, as disposições da Diretiva que estabelece o regime que lhes é aplicável (Diretiva Solvência II[5]), assim como a regulamentação e as orientações[1] que a complementam. Apesar de, na sua génese, estas regras não terem sido concebidas explicitamente para um contexto de cibersegurança, são suficientemente genéricas para poderem ser adaptadas a esta realidade concreta e a qualquer tipo de organização, em qualquer setor de atividade.

Finalmente, importa clarificar que a gestão da cibersegurança não se esgota nos princípios aqui apresentados. Com efeito, a premissa subjacente é que estes são complementares ao conjunto de medidas técnicas e operacionais em matéria de cibersegurança das TIC que a organização deve pôr em prática.

IV. Responsabilização e envolvimento do órgão de administração

Um dos princípios centrais da governação é o conceito de "*tone at the top*". Apesar de uma organização não se limitar, naturalmente, ao órgão de administração, há que reconhecer que este deve ser o garante do cumprimento da sua missão e da vivência dos valores estabelecidos. Assim, num contexto de cibersegurança, é crucial assegurar o envolvimento do órgão de administração em todas as decisões que digam respeito a esta matéria, afastando-se a visão de que as questões relacionadas com as TIC são do exclusivo interesse das áreas técnicas.

Consequentemente, os membros do órgão de administração devem ser devidamente formados e sensibilizados para a relevância da cibersegurança e, de preferência, deve ser nomeado um elemento que detenha as competências necessárias e suficientes para lidar com essas questões, esteja apto para desafiar e questionar as propostas que sejam apresentadas a este órgão colegial e tenha condições para apoiar a tomada de decisões informadas sobre as matérias em apreço, dado que, no limite, a responsabilidade pelas ações realizadas é do órgão de administração.

V. Definição de uma estratégia e de uma política de cibersegurança e concretização através de processos e procedimentos

Se a gestão da cibersegurança for vista como uma preocupação para toda a organização, a consequência natural é que a mesma seja enquadrada na sua estratégia global e posta em prática através de políticas concretas aprovadas pelo órgão de administração, documentadas e amplamente divulgadas a todos os níveis hierárquicos.

Em especial, no caso da política de cibersegurança, esta deve concretizar a estratégia definida pelo órgão de administração; conter os principais objetivos da organização neste contexto, que devem pelo menos abranger a intenção de assegurar a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não repudio da informação; e definir a forma como a instituição pretende dar cumprimento às disposições legais e regulamentares aplicáveis.

Apesar de as orientações estratégicas e subsequentes políticas diferirem entre instituições, na medida em que respondem à visão e missão de cada, há um conjunto de

áreas que devem necessariamente ser abordadas num contexto de cibersegurança e postas em prática através de processos e procedimentos, alguns de cariz mais técnico, que considerem, pelo menos, as seguintes matérias:

— segurança física da informação, incluindo acesso às instalações (por terceiros) ou a espaços específicos (e.g. centro de processamento de dados), mas também salvaguardas em caso de falhas de abastecimento de energia ou acidentes (incluindo catástrofes naturais);

— segurança lógica, incluindo regras claras para a gestão de acessos e para a atribuição de autorizações de acesso, contemplando igualmente os acessos remotos, e definição dos mecanismos de autenticação;

— gestão dos riscos de cibersegurança, incluindo a respetiva identificação, avaliação, monitorização, gestão e reporte;

— relação com prestadores de serviços terceiros em matéria de TIC;

— registo de incidentes de cibersegurança e reporte nos casos aplicáveis (cf. legislação e regulamentação em vigor); e

— gestão da continuidade da atividade e recuperação em caso de interrupção provocada por um incidente de cibersegurança, que deve ser materializada num plano específico, que inclua a definição das etapas a concretizar, a informação sobre as pessoas, equipas e entidades (e.g. autoridades de supervisão) a contactar e as medidas a aplicar para assegurar o menor impacto possível na continuidade da atividade, caso esta seja interrompida.

A estratégia, a política de cibersegurança, bem como os processos e procedimentos que a materializam devem ser revistos periodicamente, para assegurar a sua contínua adequação à realidade da organização.

VI. Estrutura organizacional adequada, alocação de responsabilidades clara e transparente e autonomia e independência das funções associadas

A gestão da cibersegurança deve estar assente numa estrutura organizacional adequada, com uma clara alocação de responsabilidades e funções.

Caso as características da organização o justifiquem, deve ser nomeado um responsável de cibersegurança, que seja o interlocutor no que respeita às questões relacionadas com este tema. Contudo, independentemente das opções e das características concretas de cada organização, nomeadamente em termos de nomenclatura e enquadramento na estrutura organizacional (e.g. nomeação de um *Chief Information Security Officer* ou CISO), o que é fundamental é assegurar que existe uma figura de referência que tenha a autonomia e a independência necessárias para atuar, assegurando que as ocorrências são endereçadas de forma consistente e fundamentada, por exemplo, em caso de ocorrência de um incidente cibernético – naturalmente em articulação com o órgão de administração e em linha com a estratégia, políticas, processos e procedimentos estabelecidos.

VII. Enquadramento dos riscos de cibersegurança no sistema de gestão de riscos

Uma das peças-chave de um sistema de governação é a componente de gestão de riscos. Assim, independentemente da metodologia de gestão de riscos adotada pela organização, há que assegurar que os riscos de cibersegurança são tomados em devida consideração e que são contemplados nos limites globais de tolerância ao risco definidos.

Em especial, é necessário garantir que, na gestão dos riscos de cibersegurança, são tidos em conta tanto fatores internos como externos, abrangendo os processos, as pessoas e as TIC relevantes.

A organização deve estar ciente do facto de que, na gestão dos riscos, poderá encontrar desafios na determinação do equilíbrio adequado entre os recursos disponíveis e a necessidade de assegurar o nível de cibersegurança desejado. Para o efeito, há que considerar as estratégias e políticas previamente definidas.

i) Realização de testes e simulacros

Uma outra questão que assume especial relevância no contexto da gestão da cibersegurança é a realização de testes e simulacros, com o objetivo de assegurar que as políticas estabelecidas são consistentes, que os processos e procedimentos definidos são

claros e completos, que as responsabilidades estão claramente definidas e são bem apreendidas, entre outros aspetos.

Seja de uma forma mais simples, através de exercícios *table-top*, ou com um grau de sofisticação mais elevado, como é o caso dos testes de penetração motivados por ameaças[14], que podem inclusivamente prever o envolvimento de entidades externas à organização (e.g. autoridades de supervisão, prestadores de serviços), a intenção é verificar a contínua adequação das medidas de cibersegurança implementadas ou identificar novas ameaças ou vulnerabilidades.

Do mesmo modo, devem ser igualmente testados os processos e procedimentos em matéria de continuidade da atividade e recuperação em caso de interrupção provocada por um incidente de cibersegurança.

Independentemente do formato dos testes adotado, assim como do âmbito e da frequência, que deverão ser condicentes com os riscos em causa e com as características específicas de cada organização, é necessário assegurar que os mesmos são realizados com alguma regularidade.

ii) Sujeição a auditorias periódicas

A um sistema de governação vem normalmente associada a ideia de um modelo de três linhas de defesa: a frente operacional, que corresponde às operações de rotina e aos processos e procedimentos que asseguram o normal funcionamento da organização; a frente de controlo, onde são geridos os riscos; e a auditoria interna, enquanto estrutura com uma visão holística e independente sobre os processos e procedimentos.

A auditoria à gestão da cibersegurança deverá, naturalmente, fazer parte do plano global de auditoria interna da organização, com a particularidade de que os elementos envolvidos devem ter as competências adequadas e os conhecimentos necessários em matéria de cibersegurança de forma a que possam assegurar a necessária autonomia e independência para a realização de tais auditorias.

14 TLPT – *Threat Led Penetration Tests*.

Também o âmbito e a frequência das auditorias devem ser alinhados com as características específicas da organização e com os riscos de cibersegurança a que esta está exposta.

Ainda neste contexto, há que assegurar o adequado acompanhamento de eventuais recomendações, com vista a assegurar a melhoria contínua[15] da gestão de cibersegurança, incluindo as respetivas componentes de governação.

iii) Alocação dos recursos humanos e financeiros necessários e adequados

Num quadro de governação abrangente, é muito importante assegurar que são envolvidos os meios e os recursos necessários e adequados para fazer face aos objetivos estratégicos delineados.

Em matéria de recursos humanos, é crucial que a organização esteja dotada de pessoal com requisitos de qualificação e conhecimentos em matéria de cibersegurança adequados ao exercício das suas funções (conceito de *fitness*), de modo a que seja possível implementar um sistema de gestão da cibersegurança adequado às necessidades da instituição.

Contudo, esta é uma área que absorve igualmente muitos recursos financeiros, pelo que é fundamental que o órgão de administração seja devidamente informado sobre as opções e decisões que tem de tomar para obter o adequado equilíbrio entre os riscos de cibersegurança a que a organização está exposta e os meios que devem ser implementados por forma a limitar o nível de exposição ao risco predefinido.

iv) Cultura de cibersegurança, sensibilização e formação

Apesar de abordado em último lugar, este não é, seguramente, o aspeto menos relevante num quadro de governação aplicável à gestão da cibersegurança.

15 A ideia de melhoria contínua poderia ser, eventualmente, merecedora de um princípio específico.

Com efeito, é fundamental que toda a organização, desde as áreas operacionais e de suporte, atravessando todas as funções e estruturas orgânicas, até ao órgão de administração, estejam cientes dos riscos associados à utilização das TIC e, assim, atuarem como agentes da sua segurança.

Do mesmo modo, deve ser incorporada a premissa de que quaisquer novas atividades, serviços ou produtos desenvolvidos devem assegurar o cumprimento das políticas em vigor em matéria de cibersegurança – i.e. cibersegurança por desenho (*by design*) e por defeito (*by default*).

A gestão da cibersegurança, ainda que suportada por um robusto sistema de governação, que aplique os princípios até aqui descritos e enunciados, está em risco se o elemento que é muitas vezes apelidado de "elo mais fraco" – o utilizador – não estiver preparado, sensibilizado e consciencializado. É, com efeito, o comportamento dos utilizadores, que sem a formação adequada poderão ser permeáveis a esquemas de engenharia social, ataques de *phishing*, ou outras tipologias de ataques, que pode pôr em causa a cibersegurança da organização.

Assim, deve ser promovida uma cultura de cibersegurança a todos os níveis da instituição, que abranja desde os colaboradores recém-chegados aos membros do órgão de administração, e que esteja assente em práticas de formação, capacitação e sensibilização contínuas, incluindo a atualização face a novos tipos de ameaças e vulnerabilidades; na realização de testes e simulacros; e na adoção de processos e procedimentos claros, em linha com vários dos princípios já enumerados anteriormente.

VIII. Conclusão

Em matéria de cibersegurança, o *status quo* dita que esta é, mais do que nunca, um aspeto essencial a salvaguardar na gestão global de uma organização.

Para o efeito, a cibersegurança tem de ser devidamente suportada por um sistema de governação próprio, necessariamente integrado com as estruturas e mecanismos de governação da organização e em constante interação com estes.

É certo que cada organização tem as suas características específicas e que nem sempre é adequado aplicar todos os princípios enumerados (e outros considerados adequados) na sua plenitude, tomando em consideração uma abordagem proporcionada. Contudo, não se pode descurar o facto de que, com o atual grau de interconectividade entre as instituições, independentemente do seu maior ou menor grau de digitalização, o risco de propagação de um incidente cibernético é grande e, como tal, devem ser, no mínimo, tomadas as medidas que salvaguardem um grau aceitável de exposição a riscos cibernéticos.

Para concluir, não se pode correr o risco de que a cibersegurança seja vista apenas como uma obrigação legal ou regulamentar. Deve-se, inversamente, evoluir para um estado em que a cibersegurança seja abordada como prioridade e vantagem estratégica que crie valor para cada organização, protegendo os seus clientes e *stakeholders*, mas também para a sociedade como um todo.

IX. Referências

[1] Autoridade Europeia dos Seguros e Pensões Complementares de Reforma (EIOPA), *Orientações sobre segurança e governação das tecnologias de informação e comunicação*, EIOPA-BoS-20/600, 12 de outubro de 2020 (https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/eiopa-gls-ict-security-and-governance-pt.pdf)

[2] Centro Nacional de Cibersegurança (CNCS), *Quadro Nacional de Referência para a Cibersegurança (QNRCS)*, 2019 (https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf)

[3] Comissão Europeia, *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido*, 7 de fevereiro de 2013 (https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013JC0001&from=PT)

[4] Decreto-Lei n.º 65/2021, de 30 de julho, que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) (https://files.dre.pt/1s/2021/07/14700/0000800021.pdf)

[5] Diretiva 2009/138/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, relativa ao acesso à atividade de seguros e resseguros e ao seu exercício (Solvência II) (https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32009L0138&from=en)

[6] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=EN)

[7] ISO/IEC 27001:2003, *Tecnologia de informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos*, setembro de 2013

[8] Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do

Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (https://files.dre.pt/1s/2018/08/15500/0403104037.pdf)

[9] Organização para a Cooperação e Desenvolvimento Económico (OCDE), *OECD Guidelines for the Security of Information Systems and Networks – Towards a culture of Security*, 2002 (https://www.oecd.org/Sti/Ieconomy/15582260.Pdf)

[10] Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro e que altera os regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 e (UE) n.º 909/2014 (https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020PC0595&from=EN)

[11] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT)

[12] Resolução do Conselho de Ministros n.º 50/88, de 03-12-1988, que publica as Instruções para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas – SEGNAC 1 (https://files.dre.pt/1s/1988/12/27900/47724800.pdf)

[13] Resolução do Conselho de Ministros n.º 37/89, de 24-10-1989, que publica as Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Industrial, Tecnológica e de Investigação – SEGNAC 2 (https://files.dre.pt/1s/1989/10/24500/46724698.pdf)

[14] Resolução do Conselho de Ministros n.º 5/90, de 28-02-1990, que publica as Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Informática – SEGNAC 4 (https://files.dre.pt/1s/1990/02/04901/00020017.pdf)

[15] Resolução do Conselho de Ministros n.º 16/94, de 22-03-1994, que publica as Instruções para a Segurança Nacional – Segurança das Telecomunicações – SEGNAC 3 (https://files.dre.pt/1s/1994/03/068b00/14231427.pdf)

[16] Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho de 2015, que aprova a Estratégia Nacional de Segurança do Ciberespaço 2015 (https://files.dre.pt/1s/2015/06/11300/0373803742.pdf)

[17] Resolução do Conselho de Ministros n.º 41/2018, de 28 de março de 2018, que estabelece os requisitos técnicos mínimos das redes e sistemas de informação que são exigidos ou recomendados a todos os serviços e entidades da Administração direta e indireta do Estado (https://files.dre.pt/1s/2018/03/06200/0142401430.pdf)

[18] Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho de 2019, que aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (https://files.dre.pt/1s/2019/06/10800/0288802895.pdf)

O Impacto da Automa(tiza)ção e o (Reduzido) Papel Humano na Deteção de Vulnerabilidades

ALDEMAR WILSON DE ALMEIDA BONDIM DIAS

GONÇALO NUNO BAPTISTA DE SOUSA

SUMÁRIO: Resumo; I. Introdução; II. Segurança da Informação; III. Falsos Positivos. Quando o tempo ganho é tempo perdido; IV. A (Des)Humanização subjacente; V. Um outro ponto de vista e possíveis soluções; VI. Conclusão; VII. Bibliografia

RESUMO:

Com os avanços tecnológicos que continuam a surgir desde há alguns anos para cá, a capacidade de adaptação das organizações a todos os níveis é constantemente posta à prova. No que toca à cibersegurança, as empresas atualmente dispõem de cada vez mais métodos automatizados para testar os seus sistemas e poder ter a certeza de que os mesmos não estão sujeitos aos mais diversos tipos de ataques. Mas por vezes, com toda esta evolução, podemos ficar com a ideia de que o ser humano (que cria estes mesmos automatismos) acaba por ficar reduzido a um segundo plano de importância, e em muitos casos é mesmo esquecido nos processos. Mas é importante perceber quais podem ser as consequências para as organizações, se confiarem em demasia nestes mecanismos e se esquecerem de que os cria.

Palavras-chave: tecnologia, automatização, fator humano, segurança, empresas, máquina, robot.

ABSTRACT:

With the technological advances that have continued to emerge over the last few years, the ability for organizations to adapt at all levels is constantly being put to the test. When it comes to cybersecurity, corporations now have more and more automated methods to test their systems and be sure that they are not subject to the most diverse types of attacks. But sometimes, with all this evolution, we can get the idea that the human being (who creates these same automations) ends up being reduced to a secondary level of importance, and in many cases is even forgotten in the processes. But it's important to understand what the consequences can be for organizations if they rely too much on these mechanisms and forget who creates them.

Keywords: *technology, automation, human factor, security, corporations, machine, robot*

I. Introdução

A ideia de automatização de processos tem vindo a ganhar um destaque sem igual nas organizações no século XXI. Os recursos humanos e técnicos têm como principal objetivo transformar os procedimentos para que estes sejam executados no mínimo de tempo, mas sempre com os melhores resultados possíveis. De preferência sem uma intervenção humana constante.

No entanto, sabemos que estamos num período da história em que os ataques informáticos sucedem-se a um ritmo alucinante, e podem causar graves danos reputacionais, financeiros, logísticos e de outros níveis em empresas e pessoas por todo o mundo. A necessidade de adaptação é algo que tem vindo a ser priorizado perante tão grandes ameaças e os vetores de ataque multiplicam-se praticamente a cada dia que passa.

Como tal, as empresas muitas vezes encontram nos mecanismos automáticos de testagem de vulnerabilidades e em outros métodos semelhantes, uma resposta que permite averiguar a segurança dos seus sistemas de forma regular e menos dispendiosa, deixando muitas vezes de lado a figura humana (p.ex.: o *pentester* ou analista de segurança informática).

O mercado está inundado por produtos que garantem dar a melhor resposta no que toca à análise de um sistema (empresas e software como Qualys, Rapid7, Nessus, etc.), perante os mais recentes tipos de ataques informáticos. Tudo isto sem obrigarem a que um colaborador tenha de fazer o controlo permanente desse mesmo produto e se possa dedicar apenas a verificar os resultados (normalmente sob forma de relatórios personalizáveis e com bastante informação).

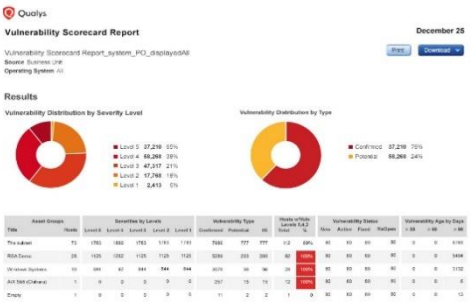

Figura 1. Exemplo de resultados de um scan automatizado

Importa saber se nos dias de hoje esta metodologia já pode ser considerada como suficiente para garantir a segurança dos sistemas informáticos a grande escala. Pode dar-se

o caso de as empresas em questão ficarem ainda mais expostas aos perigos que advém de técnicas de "hacking" (ou outras formas de intrusão em sistemas) que possam fazê-las implodir, e que apenas pessoas devidamente preparadas conseguem entender.

Deve então ser feita uma reflexão sobre se o papel que começa a ser retirado ao ser humano neste âmbito algum dia poderá ser completamente desempenhado por automatismos, ou se podemos com certeza afirmar que a análise de vulnerabilidades em sistemas trará sempre novos desafios aos quais nem as melhores máquinas automatizadas poderão responder na totalidade.

Os exemplos dados seriam aplicáveis a empresas relativamente grandes e cujos sistemas ou aplicações devessem ser usados por uma quantidade considerável de colaboradores e clientes. O objetivo deste artigo é mostrar mais um ponto de vista que possa ajudar a entender onde estamos e para onde caminhamos nesta temática.

Procura-se fazer não só um contraste, mas também uma sincronização, entre o sistema automatizado de testagem de vulnerabilidades (ou *scanner de vulnerabilidades*) e as diferenciadas capacidades humanas para realizar essas mesmas tarefas.

Sabemos que Inteligência Artificial, *Machine Learning* e testagem automática de sistemas ou vulnerabilidades, entre outras, são expressões que têm vindo a ocupar um espaço cada vez maior dentro das equipas de segurança informática.

Isto acontece nos mais diversos tipos de organizações (publicas, privadas, desde a área da banca até à defesa nacional). No entanto, apesar destes chavões aparentemente "modernos", será que ainda há (ou deve sempre haver) espaço para um cérebro humano capaz de separar o trigo do joio, e que possa ligar todas as vertentes de analise de uma forma que um sistema automatizado dificilmente o poderá fazer? Ou estaremos já perante um tal domínio do "automático", em que a pressão do resultado imediato faz-se valer de uma forma sem precedentes?

II. Segurança da Informação

Vale sempre a pena pensar na segurança de informação como um todo antes de analisar o tema propriamente dito da automatização da mesma. É importante termos em mente os conceitos de **Confidencialidade, Integridade, Autenticidade, Não-Repudio, Rastreabilidade.**

Por **confidencialidade**, entende-se a garantia de que os todos os dados transmitidos entre entidades são apenas visíveis por quem está autorizado a vê-los (ex.: tem as permissões para tal). Neste aspeto, podemos considerar que um automatismo só terá os acessos que o humano que o configura permitir, e dificilmente conseguirá efetuar os testes de intrusão normalmente feitos pelos *pentesters*.

Podemos pensar em **integridade** como sendo a garantia de que os dados transmitidos entre entidades não sofreram qualquer alteração desde o seu envio pelo remetente até à receção pelo destinatário. Tal como com a confidencialidade, podemos confiar que os dados trabalhados pelos automatismos se manterão íntegros, exceto se um mecanismo de testagem for programado para adulterar os mesmos – algo que atualmente não se tem verificado e que poderia até levar a ações judiciais contra os fabricantes.

Em relação à **disponibilidade, esta é a g**arantia de que os dados transmitidos estão sempre disponíveis para aqueles que os devem consultar. Podemos também concluir que muito dificilmente os sistemas seriam tornados inacessíveis por ação de um automatismo.

Já os conceitos de **Não-Repudio** e **Rastreabilidade** ganham uma nova dimensão no que toca à forma como depositamos a confiança em sistemas de testagem automática de vulnerabilidades. Por **não-repudio**, entende-se a garantia de que uma ação tomada (seja por um humano ou automatismo) não poderá ser negada pelo próprio. **Rastreabilidade** é a garantia de que todos os passos dados na execução das ações que impactam um sistema (desde o início até ao fim) podem ser facilmente identificados (no tempo, espaço físico/virtual, entre outros).

Para que um sistema esteja seguro, é importante que estes cinco conceitos estejam bem assegurados. Se é verdade que maioria deles é de verificação direta, no que toca à

rastreabilidade, os sistemas automáticos de deteção de vulnerabilidades tendem a não corresponder tão bem como se precisaria.

A diretiva NIST[2], um conjunto de praticas e recomendações para a cibersegurança, publicada pelo Americano **National Institute of Standards and Technology** e frequentemente usada como guia para as organizações planearem a defesa dos seus sistemas informáticos, aponta nas suas fases "DETECT" e "RESPOND", o que deve ser feito para detetar e responder a possíveis riscos que existam. É nestas fases que se insere a deteção de vulnerabilidades. Estas são também as fases em que os automatismos mais têm vindo a adquirir uma importância por vezes desmedida nas organizações.

Figura 2.Fases da Diretiva NIST

III. Falsos Positivos. Quando o tempo ganho é tempo perdido

Imaginemos a seguinte situação: uma equipa utiliza um automatismo de deteção de vulnerabilidades para avaliar o seu parque aplicacional durante o fim de semana. Não será necessária qualquer intervenção humana durante o período em que os "*scans*" estão a ser efetuados. No final obtém-se um relatório pormenorizado de "vulnerabilidades" (algumas delas possivelmente muito graves).

O normal será que os analistas da equipa estejam a postos para remediar as vulnerabilidades descritas no relatório. Acontece que após uma análise detalhada, percebe-se que maioria dessas vulnerabilidades não existe realmente. Tudo isto levou a um gasto (muitas vezes elevado) de recursos técnicos e humanos, o que poderia ter sido evitado se desde o início do processo, a confiança para a analise tivesse sido colocado nos mesmos analistas que teriam a tarefa de resolver as vulnerabilidades, e não apenas nos automatismos.

De um modo geral, a maior qualidade apontada aos métodos automáticos de testagem, é a rapidez com que possibilitam analisar centenas de ativos (aplicações e servidores, entre outros) e fornecer relatórios detalhados das vulnerabilidades que os

mesmos possam ter. Pois bem, sendo isto inegável, também o é o facto de que por poderem gerar imensos falsos positivos, por vezes o tempo que ganhamos, é perdido na análise de problemas onde eles podem não existir.

Compreender o contexto no qual um sistema será testado é fulcral para o sucesso desse mesmo teste. Entendemos que na génese de um ataque informático estará sempre um ser humano. Sabemos que um ataque informático poder ser realizado num contexto básico pelo cibercriminoso (sem grande capacidade técnica) requerendo medidas de deteção certamente mais elementares, mas também pode ser executado por um atacante especialista capaz de ludibriar qualquer automatismo. Além disso, um *scan* automatizado não tem a capacidade de entender se todas as vulnerabilidades encontradas podem ser efetivamente exploradas no sistema em que são encontradas.

Ora, para que uma organização se possa defender de um ataque mais bem organizado, a análise de todo o contexto deverá ser feita por alguém com a mesma capacidade cognitiva e os mesmos "reflexos" técnicos que o atacante – PENSAR E AGIR COMO UM ATACANTE PARA PERCEBER COMO O ATACANTE AGIU.

É certo que os cibercriminosos muitas vezes também usam ferramentas automatizadas nas suas tentativas de acesso a sistemas. Podemos entendê-las como ferramentas de apoio à execução, e não como substitutas do criminoso em si. São formas de ajudar a poupar tempo, e não a penetrar nos sistemas. Como tal, do lado da defesa de sistemas, o pensamento deve ser semelhante.

IV. A (Des)Humanização subjacente

Este tema insere-se dentro de outro ainda maior. A procura pela automatização de processos nas empresas, como forma de reduzir tempo e custos nas operações do dia-a-dia pode levar a que também a qualidade da segurança informática seja afetada.

Os sistemas são preparados para necessitar de cada vez menos interação humana na realização de tarefas. Os *scanners* cada vez mais "retiram o elemento humano do centro de operações de segurança" [1]. Ao depositarem a sua quase total confiança nestes sistemas

automáticos, as empresas estão também a colocar em risco a capacidade de resposta dos seus técnicos, que por falta de "desafio mental" acabam por se tornar apáticos e podem mesmo perder a vontade de se atualizarem regularmente num mundo da cibersegurança em que a evolução deve ser constante.

Façamos então a pergunta: o que leva as organizações a optar cada vez mais por estes métodos, deixando de parte o fator humano da cibersegurança? Seria fácil apontar apenas para questões financeiras reiterando que o custo de uma licença anual de software de testagem pode ser bem menor do que o de manter uma equipa adequada às dimensões da empresa para tratar de forma recorrente das vulnerabilidades e tudo o que elas podem implicar num sistema ou aplicação. No entanto, outros fatores merecem uma certa atenção. Vamos falar de três específicos.

Em primeiro lugar, podemos falar de uma cultura de **resultadismo.** Este termo, normalmente aplicado ao desporto, define a ideia de que é melhor obter um bom resultado final do que utilizar os melhores métodos para executar uma tarefa. Na segurança informática, e especificamente no que toca a testes de vulnerabilidades de sistemas e aplicações, o resultadismo pode manifestar-se na vontade das equipas de mostrar rapidamente as (muitas dezenas de) vulnerabilidades que podem existir em vez de fazerem uma análise mais precisa de cada uma e das suas opções de mitigação.

A quantidade sobrepõe-se à qualidade como forma de mostrar serviço e isso leva a que muitas vezes se perca tempo com questões triviais, quando o mais adequado para as equipas seria focar-se em resolver as reais vulnerabilidades.

Em segundo lugar, analisemos a constante necessidade de **rapidez** nos processos. Os *scans* prometem resultados minuciosos em poucas horas. Tal como o resultadismo, com a necessidade de rapidez prometida pelos *scanners*, as empresas apostam num modelo em que o que é apresentado como final, pode ficar bastante aquém do que é necessário testar.

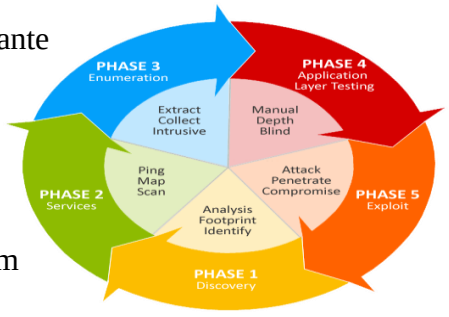

Figura 3.Exemplo de uma correta metodologia para realizar um Pentest. Um scan de vulnerabilidades dificilmente terá este nível de profundidade.

Tomemos como exemplo uma aplicação web de uma empresa, que pode ser acedida por clientes numa rede que não esteja ligada de nenhuma forma à empresa em si.

Um *scan* de vulnerabilidades a essa aplicação deve com certeza demorar mais do que apenas uma hora. Caso contrário é provável que não revele os resultados mais precisos possíveis.

Por último, e aliado a estes dois aspetos está a **Eficácia** prometida por estes métodos para tarefas de tamanha importância e envergadura. As organizações são levadas a assumir que algo tão moderno é quase infalível, ajudando a atingir os objetivos de testagem e outros parâmetros pré-estabelecidos de uma forma completamente segura, e útil para quem implementa.

V. Um outro ponto de vista e possíveis soluções

Sendo certo que há muitas características negativas associadas ao uso de *scanners* automáticos, também é verdade que se podem retirar fatores positivos dos mesmos. A sua utilidade manifesta-se acima de tudo ao nível do combate aos zero-days (vulnerabilidades encontradas recentemente para as quais não foi desenvolvida nenhuma forma de mitigação).

Nestes casos, partindo do princípio de que a empresa responsável pelo *scanner* atualiza os seus parâmetros de testagem numa base quase diária (como quase todas asseguram), será possível à equipa de segurança entender se os seus sistemas carecem de ser atualizados o mais rapidamente possível ou não.

Por fim, tendo olhado para alguns dos problemas que a dependência da automatização pode levantar nas equipas de segurança informática das organizações, importa também perceber como podem as mesmas reduzir essa independência e ainda assim obter bons resultados no que toca à sua proteção.

Já foi mencionada a diretiva NIST e aplicando a mesma poderemos fortalecer os nossos sistemas organizada e eficazmente. Sabendo que as primeiras fases do processo são

a IDENTIFICAÇÃO e a PROTEÇÃO de todos os envolvidos nos processos de cibersegurança de uma empresa, é importante que estas duas fases e tudo o que elas implicam estejam bem acauteladas para que a Deteção e Resposta a vulnerabilidades se processe de forma igualmente eficaz, organizada e em que os automatismos sejam complementares e não basilares.

A primeira solução, e muitas vezes a menos favorecida, é um aumento dos membros especializados em segurança informática, apropriada às reais necessidades da organização. Um número de membros reduzidos nas equipas leva a sobrecargas de trabalho por vezes desnecessárias. Esta sobrecarga faz com que os automatismos sejam vistos como peças fundamentais quando devem ser apenas complementos de uma análise de vulnerabilidades.

Em equipas em que o trabalho é distribuído de forma adequada por todos os membros, pode haver uma melhor capacidade de análise e teste, o que por conseguinte, aumenta a proteção da organização. Esta medida permitiria, de igual modo, aumentar o volume de testes e assim detetar e mitigar as vulnerabilidades mais atempadamente. A segunda opção, quase obrigatória perante o que foi discutido até agora passa por uma maior harmonização entre o humano e a máquina ou automatismo. Os *pentests* (realizados por humanos) devem ser efetuados pelo menos uma vez por ano e sempre que uma aplicação seja alvo de grandes mudanças a nível de código.

A harmonização resultante permitiria que os técnicos se mantivessem constantemente atualizados no que toca à segurança de informação e se apoiassem nos mecanismos automáticos apenas quando estritamente necessário. Uma utilização capaz, com regras fortes estabelecidas previamente e sempre com o a supervisão de uma pessoa, permitem que estas ferramentas se possam tornar num importante aliado no combate aos vírus e vulnerabilidades informáticas.

VI. Conclusão

Pretendeu-se analisar a forma como as ferramentas automatizadas são usadas pelas organizações para se defenderem de possíveis ataques. É sabido que podem ser um aliado

muito importante nesta questão. Conseguimos perceber que embora haja aspetos positivos em automatizar a segurança dos sistemas, o cérebro humano ainda é e vai continuar a ser a máquina mais importante em termos de cibersegurança, para as organizações.

No entanto, é importante que estas se continuem a adaptar a uma realidade em que os *scanners* de vulnerabilidades e outras ferramentas semelhantes se tornam mais fiáveis, precisos e uteis no dia a dia. Isto não deverá levar a uma total substituição do *pentester* por estes mesmos *scanners*. Deverá, no entanto, levar a que as empresas reflitam seriamente sobre o rumo que estão a tomar e adotem medidas que permitem interligar o humano e o automatismo.

VII. Bibliografia

DEANGELO, Dena. 4 reasons to automate security testing with appsec instrumentation. CONTRAST SECURITY, 20/02/2020. Disponível em: https://www.contrastsecurity.com/security-influencers/4-reasons-automate-security-testing-with-appsec-instrumentation. Acesso em: janeiro 2022.

JAMES, Rebecca. What Impact Do AI and ML Have on Security Testing? BECOMING HUMAN: ARTIFICIAL INTELLIGENCE MAGAZINE, 19/06/2020. Disponível em: https://becominghuman.ai/what-impact-do-ai-and-ml-have-on-security-testing-f620c70eb3c1. Acesso em janeiro 2022.

LEMOS, Robert. Efficient Security Testing Requires Automation, but Humans Are Needed Too. DARK READING, 10/06/2020. Disponível em: https://www.darkreading.com/application-security/efficient-security-testing-requires-automation-but-humans-are-needed-too. Acesso em: janeiro 2022.

NIST CYBERSECURITY FRAMEWORK. Disponível em: https://www.nist.gov/cyberframework. Acesso em: dezembro 2021.

SANTARCANGELO, Michael. *We need to stop dehumanizing security before it's too late.* CSO ONLINE, 05/09/2017. Disponível em: https://www.csoonline.com/article/3221373/we-need-to-stop-dehumanizing-security-before-its-too-late.html. Acesso em: janeiro 2022.

The Human Element of Pen Testing and the Role Tools Can Play. CORE SECURITY. Disponível em: https://www.coresecurity.com/blog/human-element-pen-testing-and-role-tools-can-play. Acesso em: janeiro 2022.

WILLIAMS, Jeff. The true cost of "false positives" in application security. CONTRAST SECURITY, 19/06/2016. Disponível em: https://www.contrastsecurity.com/security-influencers/the-true-cost-of-false-positive-vulnerabilities-in-application-security. Acesso em: janeiro 2022.

Artificial Intelligence Applied to Health in an International Regulatory Perspective

DANIEL FREIRE E ALMEIDA[1], VERÔNICA SCRIPTORE FREIRE E ALMEIDA[2] & RENATA SALGADO LEME[3]

1 -Postdoctor in International Law - Georgetown University - Law Center, Washington DC, United States of America (2015-2017).
-PhD in International Law - Faculty of Law - University of Coimbra, Portugal (2008-2012).
-Permanent Professor of the Postgraduate Program - PhD and Masters in International Law - Catholic University of Santos (UNISANTOS).
-Lawyer, acting, in Brazil and abroad, in the areas of International Law, Digital Law, Space Law, and International Relations. -E-mail: lawyer@adv.oabsp.org.br .
2 -PhD in Economic Law - Faculty of Law - University of Coimbra, Portugal (2009-2016).
Conducted research in Washington DC, USA, during a period of PhD Academic Research (2015-2016) and Post-Doctoral Academic Research (2016-2017) at Georgetown University - Law Center.
-Permanent Professor of the Postgraduate Program - Masters in Health Law – Santa Cecilia University (UNISANTA).
--Lawyer, acting, in Brazil and abroad, in the areas of International Law, Digital Law, Health Law, Trust Law, Economic Law and International Relations. - E-mail: veronicascriptore@adv.oabsp.org.br

SUMMARY: Abstract; I. Initial Considerations; II. Artificial Intelligence; III. The International Regulation of Artificial Intelligence; IV. Artificial Intelligence Applied in Healthcare - European Union Regulatory Perspective; V. Artificial Intelligence Applied to Health – Perspectives from Brazilian Law; VI. The General Personal Data Protection Law and the impacts on the regulation of artificial intelligence and the protection of sensitive data; VII. Final Considerations; VIII. Bibliographic references

ABSTRACT:

This article analyzes aspects of artificial intelligence applied in healthcare, from an international regulatory perspective. To this end, the essay is divided into the following parts. Firstly, it introduces the topic in the legal sphere, with its problems in the current context. It then deals with artificial intelligence, proceeding to its international regulation, with emphasis on initiatives by the United Nations and the World Health Organization. It then raises some characteristics of European Union regulation, to, in the end, culminate with Brazilian regulatory treatment. Lastly, it develops final considerations on the topic.

Keywords: Artificial intelligence; Digital Law; Health Law; European Union; United Nations; World Health Organization.

RESUMO:

O presente artigo analisa aspectos da inteligência artificial aplicada na saúde, em perspectiva regulatória internacional. Para tanto, o ensaio está dividido nas seguintes partes.

---

3 Graduated from the Faculty of Philosophy, Letters and Human Sciences at the University of São Paulo (1987). Graduated in Law from the Catholic University of Santos (1992). Master's in Law from the University of São Paulo (1998). PhD in Law at the University of São Paulo (2004). Doctorate in Law Recognized by the General Directorate of Higher Education - DGES of Portugal, conferred the rights inherent to the Portuguese academic degree of Doctor, registered with nº 120220195621 (2022). Full professor at University Santa Cecilia, in the Faculty of Law Graduation and in the Master's Degree in Health Law. As a researcher, she coordinates the research group Transdisciplinary and Human Rights - CNPQ. She has worked as a lawyer since 1992. Member of IASP - São Paulo Lawyers Institute. Member of the OAB Santos Health Law Commission.

Primeiramente, introduz o tema na esfera jurídica, com sua problemática no contexto atual. Em seguida, trata da inteligência artificial, prosseguindo para sua regulação internacional, com destaque para iniciativas da Organização das Nações Unidas, e da Organização Mundial da Saúde. Em prosseguimento, eleva algumas características da regulação da União Europeia, para, ao final, culminar com o tratamento regulatório brasileiro. Por derradeiro, desenvolve considerações finais sobre o tema.

Palavras-chave: *Inteligência artificial; Direito Digital; Direito da Saúde; União Europeia; Organização das Nações Unidas; Organização Mundial da Saúde.*

I. Initial Considerations

In several segments of current interest, modern technologies leveraged by the Internet are bringing challenges and innovative solutions.

In this context, artificial intelligence presents a revolutionary scenario. This is because, in addition to presenting increasingly impactful applications, it raises problems that require regulatory positions.

In healthcare, for example, the digital conflagration of healthcare and therapeutic enhancement, which includes exploring the applied uses of artificial intelligence, has the potential to improve healthcare outcomes by facilitating medical diagnosis, digital therapeutics, clinical trials, self-care, and evidence-based knowledge.

With the increasing availability of healthcare data and rapid progress in analytical techniques, artificial intelligence has the potential to transform the healthcare sector, which is one of the most important sectors for societies and economies around the world.

However, the segment is not immune to challenges. In fact, negative uses may occur. In effect, artificial intelligence systems can have access to sensitive personal information, violating the privacy, security and integrity of patients and healthcare professionals.

Consequently, regulatory treatment needs to be strengthened.

Therefore, this article has a precise address: to present a brief overview of artificial intelligence applied in healthcare, adopting an international regulatory perspective.

In this sense, to achieve this goal, we will introduce artificial intelligence into the legal sphere, with its problems in the modern context. Next, we will deal with artificial intelligence, moving on to its international regulation, with emphasis on initiatives by the United Nations and the World Health Organization. In continuity, we will highlight some characteristics of European Union regulation, and Brazilian regulatory treatment.

II. Artificial Intelligence

The automation of intelligent behavior has gained new contours with artificial intelligence being used massively on the Internet. Initially reserved for corporate applications from technology companies, it quickly became popular with the launch of ChatGPT. This tool is an artificial intelligence-based language model developed by OpenAI, capable of generating human-like text based on advanced programming, digital context, and algorithmic interactions. In fact, its global projection drew attention to artificial intelligence in a diffuse and definitive way.

Basically, artificial intelligence is the ability of a digital computer, or computer-controlled robot, to perform tasks normally associated with intelligent beings. The term is often applied to the project of developing systems endowed with intellectual processes characteristic of human beings, such as the ability to reason, discover meaning, generalize, treat, or learn from past experiences. In fact, this last point (learning) makes artificial intelligence a mechanism with unlimited potential, and which raises concerns about the limits that should be imposed, and its global regulation.

Since the beginning of the development of the digital computer, its usefulness has been intricately linked to programming, the software that would give the device its function. In this step, increasingly complex tasks that would require repetition, or enormous work, began to require continuous and in-depth development of coding. The combination of codes that have been developed since then represent significant advances in the use of devices, such as computers, tablets, and cell phones.

In an essential complement, if not fundamental, the Internet enabled the global interconnection of different programs and applications based on artificial intelligence, solving entangled problems, presenting advanced solutions, and learning, automatically, from other digital uses that were based on artificial intelligence.

In truth, this is a revolution. The Internet has catapulted artificial intelligence to a globalized status of relevance and application.

Initially, we can exemplify its basic use in chess games, which in addition to the programming that allowed the computer to beat common players, also provided continuous learning through games, becoming almost unbeatable in subsequent clashes.

However, more complex activities required greater performance from programmers, who, with advanced techniques and faster devices for processing and storing data, have brought artificial intelligence closer to human intelligence, in many domains.

The Internet, however, has increased the demand for tasks on the part of users, allowed worldwide learning without previous precedents, and with the combination of many intelligent and diverse skills, such as reasoning, problem solving, learning, self-programming, perception and use from ordinary computer language, has made artificial intelligence a distinct and global tool. Likewise, artificial intelligence has applications in autonomous vehicles, smart cities, and virtual assistants, such as Alexa, for example.

On the other hand, its full and widespread application, integrated with robotization and the Internet, raises challenges that must be faced across the planet. The future involves the assessment and regulation of artificial intelligence at an international level. This is because, with the qualitative advancement of artificial intelligence, the topic becomes complex and decisive.

The new context involves general artificial intelligence, already disseminated throughout the digital environment, continues through applied artificial intelligence or cognitive simulation, in the process of acquiring knowledge and self-programming, and also through that which aims to build thinking machines. Everything, therefore, with the ultimate aim of producing devices with an intellectual capacity that is indistinguishable from that of a human being. More directly, the future points to the use of artificial intelligence in all segments, bringing impacts to people.

As BREMMER and SULEYMAN (2023) highlight, productivity is expected to reach unprecedented levels and countless previously unimaginable companies will grow at breakneck speed, generating immense advances in well-being. New products, cures and innovations will hit the market daily as science and technology accelerate.

III. The International Regulation of Artificial Intelligence

Despite the extraordinary difficulties involved, the evolving reality already demonstrates that artificial intelligence is faced with challenges that require a certain global order.

The problems involve digital human practices, such as all deviant conduct, as well as the new negative applications of artificial intelligence. In particular, the crimes that can be committed, their unethical application, and their use in activities that would be very particular to human beings.

In brief illustration, negative applications, and in part criminal, occur through the invasion of systems, fake news, deep fakes, capture of passwords, espionage, fraud, digital forgeries, false profiles, accidents with the use of robots, nuclear risks, wars cybernetics, and anticipation of actions (before the human being who would give the order) without evaluating the harmful consequences. This is just to name a few problems.

Furthermore, the replacement of human beings in repetitive activities, removing jobs, is already a reality. Even though innovative technologies create new jobs and indicate the way forward, artificial intelligence requires certain skills and abilities that are still far from academic training in many countries. People's privacy is another aspect that raises concerns, as the collection, processing of massive amounts of data makes the security and availability of this data vulnerable to reaching organizations focused on criminal or malicious practices.

In any case, it is not easy to create rules that enhance the benefits of artificial intelligence and, at the same time, minimize risks and make its practice accountable, even more so when the action involves intelligent machines and software.

In another sphere, the subject is of interest to all people, involving multinational companies and developers, giving rise to a global, rather than local, approach. In effect, the focus must be global on the challenges arising from the Internet, and not on the liberating permission of one or another location that would be considered a “digital paradise”.

It is very opportune, very clear to note, that artificial intelligence will cause disruptions, create risks, and bring social and legal repercussions that will configure a new digital society, integrated by super-intelligent, hyper-evolutionary, ambivalent people and machines, biased by algorithms, integrated with other technologies, with the ability to easily deceive human beings.

Programmers, developers, and later programming robots, who will use artificial intelligence for new applications, will determine the ways in which private and public power is exercised, to the point that we may no longer have control over humanity's decisions.

Even though it is said that “not everything seems to be what it is”, in terms of problems, and that “we are still far from this reality”, we can say that the future holds a panorama of practical digital insecurity. The power currently exercised by big tech is just the beginning of a new digital era, but one that may not be regulated in time by human beings.

In addition, with artificial intelligence, machines learn, self-program, self-improve, reason, and decide. By conducting these actions, we will have no control over whether this will be for the good or not. Artificial intelligence will put fundamental points of humanity at risk, and at a constant and speed that may be impossible to reverse, except in a preventive, rapid, and globally ordered manner.

Because of this, and with the aim of resolving these issues, governments have already started to act, as BREMER and SULEYMAM (2023) warn, in these words:

> *Thankfully, policymakers around the world have begun to wake up to the challenges posed by AI and wrestle with how to govern it. In May 2023, the G-7 launched the “Hiroshima AI process,” a forum devoted to harmonizing AI governance. In June, the European Parliament passed a draft of the EU's AI Act, the first comprehensive attempt by the European Union to erect safeguards around the AI industry. And in July, UN Secretary-General Antonio Guterres called for the establishment of a global AI regulatory watchdog. Meanwhile, in the United States, politicians on both sides of the aisle are calling for regulatory action.*

At this step, it is important to highlight that the United Nations has established a “Roadmap for Digital Cooperation” (A/74/821), which addresses how the international community can better take advantage of the opportunities presented by digital technologies, while at the same time faces its challenges. Between the different points of action, the paradox of artificial intelligence emerges, which must be regulated (UNITED NATIONS, 2020).

For us, based on the innovative European initiative, which we will see below, and with the important contribution of different sectors of interest, from the perspective of Member States, digital companies, users, the technical community and other groups seeking international interoperability, the global approach of the United Nations seems the most appropriate for the future, due to the globality of the topic (INTERNATIONAL TELECOMMUNICATION UNION, 2022).

In fact, recently (2023), the United Nations created a body to put artificial intelligence at the service of humanity and ensure that its risks are contained and reduced. This involves the creation of a high-level, multi-sector advisory group, made up of thirty-two experts from various parts of the world.

The advisory body's efforts will be inclusive and based on the universal values enshrined in the United Nations Charter. The group's role will be to assess various artificial intelligence governance initiatives that are already underway and generate recommendations on three aspects: international rules, consensus on risks and challenges, and taking advantage of opportunities to accelerate the achievement of the AI Goals. Sustainable Development (UNITED NATIONS, 2023).

This advisory body should be gender-balanced, geographically diverse and span different generations. According to the United Nations, members have deep experience in government, business, technology, civil society, and academia.

For the United Nations, despite being surrounded by incredible possibilities, artificial intelligence presents potential dangers. Among the risks are the increase in misinformation,

the consolidation of prejudice and discrimination, surveillance, invasion of privacy, fraud and human rights violations, and dangers in the health sector (UNITED NATIONS, 2023).

The malicious use of artificial intelligence, according to the UN, could undermine trust in institutions, weaken social cohesion and threaten democracy itself, in addition to deepening inequalities and transforming digital divisions into abyss.

To prevent these threats, the new body will be the space for a global, multidisciplinary and multisectoral dialogue on the governance of artificial intelligence, so that benefits are maximized, and risks contained.

For its part, the World Health Organization launched in 2023 the report on "Regulatory considerations on artificial intelligence for health", which emphasizes the importance of establishing the safety and effectiveness of artificial intelligence systems, so that they are made available in an appropriate way for who needs (WORLD HEALTH ORGANIZATION, 2023).

The World Health Organization also highlights the advantages of modern technology, with the identification of potential new medicines, the acceleration of clinical research and the prevention and prediction of diseases and risks. However, when using health data, artificial intelligence systems can gain access to sensitive personal information. Therefore, the Organization advocates the creation of robust legal and regulatory structures to protect the privacy, security, and integrity of patients (WORLD HEALTH ORGANIZATION, 2023).

The new guidance from the World Health Organization will support countries to regulate artificial intelligence effectively, to harness its potential, whether in treating cancer or diagnosing tuberculosis, while minimizing risks. The UN health agency emphasizes that care is becoming more patient-centered, with personalized approaches to decision-making. Based on this trend, the positive use of artificial intelligence can improve the well-being of people and the population, bringing more patient education and involvement and medication adherence, contributing to disease management, in an approach that reinforces

individualization and personalization of care (WORLD HEALTH ORGANIZATION, 2023).

In this sense, with clearer regulations, the World Health Organization hopes that the innovative technology will contribute to improving medical diagnosis and complementing the knowledge, skills, and competencies of health professionals. In response to countries' growing needs to responsibly manage the rapid rise of artificial intelligence-based health technologies, the report outlines six areas for regulation: transparent documentation of the product lifecycle from development, risk management, external data validation, data quality, privacy protection and collaboration between all interested parties, including patients and healthcare professionals.

The World Health Organization also highlights that artificial intelligence systems are complex and depend not only on the code with which they are built, but also on the data on which they are trained, which comes from clinical settings and user interactions.

The World Health Organization's 2023 report aims to outline key principles that countries and regulatory authorities can follow to develop new guidance or adapt existing guidance on artificial intelligence at a national or regional level.

IV. Artificial Intelligence Applied in Healthcare - European Union Regulatory Perspective

It appears that the European Union, within the scope of its digital strategy, has sought, more specifically since 2021, to regulate artificial intelligence to guarantee better conditions for the development and use of this innovative technology, and to establish the necessary limits. In Europe, there is an understanding that systems must be analyzed and classified according to the risk they pose to users, meaning, therefore, more or less regulation. A pioneer in this line, the European Union wants to ensure that artificial intelligence systems are safe, transparent, traceable, non-discriminatory, ecological, and with different rules for different levels of risk (EUROPEAN PARLIAMENT, 2023).

In addition to holding providers and users accountable, the European Union understands that certain risks are unacceptable and should be banned, such as cognitive-behavioral manipulation of specific vulnerable people or groups, for example, voice-activated toys that encourage dangerous behaviors in children. Also, social scoring, which classifies people based on behavior, socioeconomic status or personal characteristics, and real-time remote biometric identification systems such as facial recognition (with the exception of later remote biometric identification systems, where identification occurs after a significant delay in prosecuting serious crimes, and with judicial approval (EUROPEAN PARLIAMENT, 2023).

The European Union still considers some systems to be high risk, which could negatively affect security or fundamental rights, and must be evaluated before being placed on the market and throughout their life cycle. Generative intelligence systems such as ChatGPT must meet transparency requirements, for example. Finally, limited risk systems must also meet minimum transparency requirements that allow users to make informed decisions and decide whether to continue using them (EUROPEAN PARLIAMENT, 2023).

We will now move on to analyzing the application of artificial intelligence in healthcare, considering aspects related to the protection of personal medical data when these data are used by artificial intelligence devices. In the same vein, we will discuss the potential benefits of using artificial intelligence to aid medical diagnoses and treatments, consequently benefiting European citizens.

The European Union brings together twenty-seven important countries, which annually remain in prominent positions in the Human Development Index (HDI), which, among other relevant dimensions, analyzes health as a fundamental point of consideration. Furthermore, the European Union provides relevant evidence in the pioneering implementation of fundamental regulations that cover global concerns such as, most relevant here, artificial intelligence and data protection. Therefore, when we aim to deal with artificial intelligence applied in healthcare, the European Union is an extremely

important legal space in the contexts of healthcare and advanced regulations involving data protection and artificial intelligence.

In fact, both regulations, mentioned above, are fundamental to health law and, therefore, in understanding the legal aspects related to artificial intelligence applied in Health, and it is in this line that we will follow due to the objective of this article.

As a basic rule, and demonstrating its pioneering spirit in identifying future concerns, the Charter of Fundamental Rights of the European Union, which dates back to 2000, already includes the right to protection of personal data in its article 8, in the part in which deals with freedoms, as follows:

> ***1. Everyone has the right to the protection of personal data concerning him or her.***
>
> ***2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.***
>
> *3. Compliance with these rules shall be subject to control by an independent authority.*
> *(emphasis added)*

In turn, the right to health is also included in the important Charter, namely in its article 35, in chapter IV, which deals with solidarity:

> *Everyone has the right to access preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices. A high level of human health protection shall be ensured in the definition and implementation of all the Union's policies and activities.*

In this context, with regard to health, the European Union is responsible for complementing national policies, supporting local governments to achieve common

objectives. To this end, they can adopt legislation[4]and European standards applicable to health products and services. In turn, the countries that are members of the European Union are responsible for organizing healthcare, as well as ensuring that it is effectively provided.

In this context, many new challenges emerged or were heightened due to the Covid-19 pandemic, triggering a greater need for coordination between countries in protecting people's health. In line with the challenges, the European Commission is building a European Health Union, and in this perspective, among other initiatives, it aims, through Regulation (2022/0140 (COD)), to create the European Health Data Space.

The main objective of this regulation is to help people take control of their own electronic data in European Union member countries, allowing access and sharing with healthcare professionals. Furthermore, it also aims to support the use of these data to facilitate the provision of healthcare and promote European Union research, innovation, and policymaking (European Health Data Space, 2022).

This initiative is linked to the General Data Protection Regulation (2016), since in order to allow full use of the potential offered by the exchange and use of this data, the European Union must offer legal security through the establishment of principles and rules on data protection. and processing of personal health data. Indeed, as the European Health Data Space aims to build a single market for electronic health record systems, the regulation must ensure strong protection of these data.

In line with this, when we see the wide use of these personal health data, by technological tools and devices, integrated with artificial intelligence in its various modalities (for example, generative artificial intelligence), associated with the Internet, there is an urgent need for greater concern in terms of more specific regulations.

In this context, the General Data Protection Regulation (2016) already establishes certain specific requirements to guarantee the protection of the freedoms and rights of

4The European Union can adopt health legislation based on article 168 (protection of public health); Article 114 (approximation of legislation); and article 153 (social policy) of the Treaty on the Functioning of the European Union. See: EUROPEAN UNION. Treaty on the Functioning of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016E/TXT.

individuals, in the context of automated processing of personal data, referring here to the use of artificial intelligence.

From this perspective, at the outset, we can refer to the provisions of Article 2 of the General Data Protection Regulation (2016), which in the "Scope of material application", indicates that the regulation applies to the processing of automated data[5]. Likewise, recital 15 of the Regulation states that "*The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing*".

In the same sequence of ideas, article 4, which deals with Definitions, warns about the protection of automated data by defining the term "Definition of profiles", in its item 4, as follows:

> *(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;*

In this aspect, the European Union's concern remains evident regarding the use of artificial intelligence in the evaluation of automated data, which consider personal issues of a particular individual, namely, here, in analyzing or predicting singularities related to behavior and health.

Finally, it is worth mentioning recital 63 of the Regulation under analysis, which grants the right of access to personal data to the holders of this data, highlighting those relating to health (for example, data from medical records containing information such as:

5See: "Article 2. Material scope - 1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." 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). Available at:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

diagnoses, test results, doctors' assessments and any interventions or treatments carried out).

In fact, the unprecedented development of technology has provided the application of artificial intelligence in healthcare, whether through the use of advanced technological instruments or through the analysis and treatment of patient-related databases. Without a doubt, technological innovation, optimized by artificial intelligence and enhanced by the Internet, provides healthcare professionals with advanced medical devices, fantastic tools to aid decision-making (from robot-assisted surgery, medical treatment planning, interventional diagnostic radiology, among others).

We must add that artificial intelligence is capable of gathering and comparing a large number of images, developing complete databases to support patient diagnosis. Furthermore, the interconnection of the patient's electronic medical record, with the use of Big data and algorithms, generates the ability to evaluate the patient's entire medical history, measuring a series of health-related components.

From this perspective, a fundamental study carried out by the European Parliamentary Research Service (2022) highlights the main applications of artificial intelligence in healthcare. The aforementioned study highlights the enormous potential of artificial intelligence in various healthcare segments, corroborating what has been explained so far. In relevant examples, we can mention:

-In clinical practice, with the automation of diagnostic processes for therapeutic decision-making and research;

-As we have already mentioned, in radiology where artificial intelligence works to help radiologists in the work of quantifying and qualifying medical images;

-In the same vein, artificial intelligence can collaborate in medical emergencies, for example, to improve the prioritization of patients during triage (through advanced treatment of patients' previous databases, assisting in better diagnosis);

-In addition, artificial intelligence is highlighted in studies as a fundamental tool in surgical procedures, as a source of analysis and information (such as: patient risk factors,

and anatomical information), thus supporting the doctor's understanding and leading to better surgical decisions;

-Artificial intelligence has also been working in home monitoring of patients, for example, in the self-management of chronic diseases and diseases that affect the elderly (for example: in monitoring medications, adjusting the patient's diet, as well as in managing health devices. health);

-Another indicated potential of artificial intelligence is in understanding mental health, as a tool to help diagnose diseases such as depression and anxiety. In fact, instruments using artificial intelligence can act in the digital tracking of depression, through identification of the patient's mood, through keyboard interaction, through speech, voice, and through facial recognition.

In addition to everything already listed above, it is worth mentioning the many benefits that artificial intelligence can provide to public health. For example, identifying specific demographics or geographic locations where there is a prevalence of diseases or high-risk behaviors. Likewise, in digital epidemiological surveillance, with optimization of health care based on cases and events reported in the database, which favor the preventive detection of warning signs for the occurrence of outbreaks and epidemics.

Specifically, now, in relation to the Artificial Intelligence Act and its application in healthcare, firstly, the proposed rules establish obligations for suppliers and users depending on the level of risk of artificial intelligence. In this sense, artificial intelligence systems identified as high risk include artificial intelligence technology used in healthcare, which may negatively affect security or fundamental rights. Therefore, artificial intelligence instruments applied in healthcare must be evaluated before being placed on the European Union market, as well as throughout their life cycle.

The regulation determines that any artificial intelligence products and services governed by existing European Union legislation on product safety must fall within existing laws and structures. (n. 41 of the Artificial Intelligence Act).

Currently, the applicable regulations for medical devices in the European Union are: the Medical Devices Regulation (MDR) 2017/745 and the In Vitro Diagnostic Medical Devices Regulation 2017/746 (IVDR), both approved in 2017. However, because they were derived at a time when artificial intelligence was at an early stage of its development, many specific aspects of artificial intelligence were not considered, such as the continuous learning of artificial intelligence models or the identification of algorithmic biases (EUROPEAN PARLIAMENTARY RESEARCH SERVICE, 2022).

Likewise, another point considered to be of high risk by the regulation concerns artificial intelligence systems intended to be used to make decisions or materially influence decisions on the eligibility of natural persons for health and life insurance. In fact, it risks resulting in a significant impact on people's livelihoods, potentially infringing their fundamental rights. For example: limiting access to healthcare or perpetuating discrimination based on personal characteristics. (n. 37 of the Artificial Intelligence Act).

It also remains to be mentioned that the artificial intelligence systems used to evaluate and classify emergency calls, or also to send or establish priorities in sending emergency services, since in such circumstances, could make decisions in extremely critical situations for life and health of people. (n. 37 of the Artificial Intelligence Act).

Furthermore, the Artificial Intelligence Act establishes that medical artificial intelligence technologies can only be permitted when the tools comply with specific requirements and obligations, which allow for adequate risk management, such as: ensuring human supervision and admitting carrying out continuous monitoring after being placed on the market.

Lastly, it is important to mention that the regulation under analysis requires Member States to designate one or more competent authorities, including a national supervisory authority, which would be responsible for supervising the application and implementation of the Artificial Intelligence Act.

Likewise, the regulation creates a European Artificial Intelligence Council, made up of representatives from the Member States and the Commission. Designated authorities

would have access to confidential information, including the source code of artificial intelligence systems.

V. Artificial Intelligence Applied to Health – Perspectives from Brazilian Law

The widespread use of innovative technologies can contribute to consolidating the universality, equality, and integrality of the Brazilian health system, in line with constitutional dictates.

At the moment, there is a set of trends related to new technologies that configure a series of innovations, which can be grouped into physical (autonomous vehicles, 3D printing or additive manufacturing, advanced robotics, new materials), digital (Internet of Things - IOT, big data and blockchain technology) and biological (biotechnology and genetics) and which are interconnected by a main base: digital technologies (SCHWAB, 2016). Applications of several of these technologies have also been adopted in the manufacturing sector, in a process known as "Industry 4.0", modifying the mode and forms of production, as well as the business model, that is, the ways of structuring and organizing production stages.

This revolution is also underway in the health sector (Biology, Medicine, Nursing, Pharmacy) with the increasing and accelerated introduction of innovative technologies.

In Biology, there are innovations related to genetic mapping that allow for a reduction in costs and greater efficiency in identifying genetic traits and diseases, given that several incurable diseases are related to genetic factors. With increased efficiency in identifying and mapping genes, a broad technological base is opened for the development of synthetic biology (SCHWAB, 2016).

In Medicine, the advancement of information and communication technologies allows the practice of medicine at a distance through Telemedicine, whose regulation, in Brazil, was made by the Federal Council of Medicine, through Resolution No. 1,643/2002[6],

6Please consult at: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1643.

enabling videoconferencing between doctors to discuss cases and exchange opinions. And with the publication of Law No. 13,989/20[7], the CFM recognized both the possibility and the ethicality of using Telemedicine, during the fight against Covid-19, in addition to maintaining what was already regulated by Resolution No. 1,643/2002.

We can also observe the development of Precision Medicine, the objective of which is to make it possible to prescribe medication only to those individuals for whom the drug works effectively. Therefore, to achieve this precision, it will be essential to increase the size of research samples, so that they represent the universe studied reliably. Therefore, the digitization of more patient information by health services is essential to increase the size and detail of samples.

The digitization of patient information, in turn, is another essential trend for organizing, updating, and transferring data. The universalization of digitalization of medical records in Brazil, still insufficient, is also essential to promote advancements in health care for citizens and the development of scientific research in the health area. Therefore, in addition to the implementation of the electronic patient record (PEP), it will be necessary to enable its remote use by all health establishments, that is, to facilitate the integrated use of this database.

Another field for the use of Big Data is Internet of Things, that is, all objects will be connected to each other through the Internet. Or even the possibility of using electronic objects connected to people's bodies. The volume and detail of the data generated by the Internet of Things will be immensely useful for the healthcare sector, which will be able to identify the causes and causes of illnesses and accidents, with the aim of taking preventive action, mitigating risks, and defining conduct and treatments with greater precision.

In the last two decades, Brazil has invested, albeit in an oscillating and non-systematic way, in human resources, science, technology and basic health care. The government, inspired by positive experiences in countries such as Canada, Australia, New Zealand, and European nations, designed and implemented the e-Health system. This

7Please consult at: https://www.in.gov.br/en/web/dou/-/lei-n-13.989-de-15-de-abril-de-2020-252726328.

system aims to increase the quality of the health care service, improve teamwork, streamline care and improve the flow of information for clinical decision-making, surveillance, regulation, and health promotion, as well as decision-making regarding health management (MINISTRY OF HEALTH, 2017).

Furthermore, in 2019, the National Health Information and Informatics Policy (PNIIS) promoted by the Ministry of Health, through DATASUS, established the National Health Data Network, enabling partnerships (public-private). This cooperation allows greater circulation of citizen health information among professionals involved in care, optimizing the efficiency of the service (MINISTRY OF HEALTH, 2019).

The expansion and dissemination of databases, however, can make the holder of the information increasingly vulnerable, whether due to negligence in the collection, use, sharing, storage, or disposal of data, or due to improper commercialization or leakage of information.

VI. The General Personal Data Protection Law and the impacts on the regulation of artificial intelligence and the protection of sensitive data

In Brazil, the initial framework for regulating the use of artificial intelligence is supported by the General Data Protection Law (2018). It should be noted, however, that the General Law does not specifically address the regulation of artificial intelligence, but rather the protection of personal data. However, as it was inspired by the European Union's General Data Protection Regulation, it established the right to explanation and review of automated decisions, based on the application of artificial intelligence. In Brazilian law, the explanation is not textual, but arises from the systematic interpretation of the General Data Protection Law articulated with constitutional provisions and consumer legislation (DOURADO, AITH, 2022).

The General Data Protection Law, 13,709/2018, was published on August 14, 2018, effective from September 2020, seeking to establish greater rigor in the regulation of

personal data protection[8] by more effectively safeguarding the fundamental rights of freedom, privacy and informational autonomy, whose individual and social protection is vital for the consolidation of the democratic regime in contemporary societies. It is worth noting that the Brazilian legal system was not devoid of regulatory instruments for data protection, however, there were sectoral and special laws, devoid of a systematization capable of providing, both to the public and private sectors, a paradigm guided by principles, categories, and general and specific institutes applicable to the matter.

The main objectives of data processing according to Brazilian standards are: the purpose (legitimate purpose); suitability (compatibility); the need (mandatory data collection) and transparency. The aforementioned Law, in its article 5, establishes a list of classification of types of data: non-personal data and anonymous data; personal data: name, address, email, cookies, IP; sensitive personal data: racial origin, religion, political positioning, data relating to health, genetics or biometrics.

Sensitive personal data can be classified by nature, but also by use and purpose. Trivial and common data can, through technological tools, be organized and compiled based on mathematical algorithms, making them sensitive data. (DONEDA, 2021, p. 160-161).

Brazilian law prescribes that the holder must consent to the processing of data (article 7) and requires that consent be in writing (article 8). Furthermore, consent may be revoked at any time, due to a change of purpose and consent will be declared null in case of abuse and non-transparency (article 9).

It is therefore clear that with the new rules established by the standard, services provided on social networks cannot collect data using generic terms of consent. Furthermore, the processing of sensitive data must be reported separately, and its sharing with other controllers is prohibited. The processing of data from children and adolescents must be authorized by their parents or legal representatives. And still in line with

88 Recognition of the right to protection of personal data arises from the constitutional protection of the person
human dignity, as provided in art. 1st, item III, of the Federal Constitution of 1988.

regulation, platforms have the burden of checking the authenticity of authorizations. (BIONI, 2018, p. 14).

Regarding the right to review automated decisions, there is an explicit definition in the text of article 20 of the Brazilian Law, which states that the holder has the right to request the review of decisions taken solely based on automated processing of personal data, which affect their interests. It should be noted that, unlike the European statute, Brazilian law does not enshrine a person's right not to be subject to an exclusively automated decision, nor to obtain human intervention in the event of a review. The exercise of the right to explanation in healthcare, however, is conditioned on the development of criteria and mechanisms, which should guide the construction of explainable artificial intelligence systems. However, developing a system to provide explanations is a complex and expensive task, especially when it comes to high-risk areas and sectors, such as healthcare. For these reasons, the regulation of artificial intelligence for clinical use requires joint action by the National Data Protection Authority, the National Health Surveillance Agency, as well as the Medical Councils (DOURADO, AITH, 2022)

Regarding data leakage, the aforementioned Law imposes sanctions in article 52 (warning; fine of 2% of the company's revenue in the last year, excluding taxes, limited to R$ 50,000,000.00 (reais) per infraction; blocking data and data deletion).

Therefore, the development of risk management is essential to safeguard the confidentiality, integrity, and security of information.

Therefore, the health sector must increasingly take care of information security, using secure servers and providers; instituting high database security standards; encrypting the collected data and information; adopting certified digital signature; using secure computers and software; defense mechanisms against hacker attacks, and prohibiting unauthorized individuals from accessing confidential information.

There are emblematic cases of data leaks occurring in Brazil in the context of public health. The media reported widely that on December 10, 2021, the Ministry of Health website and, particularly, the Conect-SUS application and page, used by citizens to obtain

the National Covid-19 Vaccination Certificate, required for access to various public places, as well as information about the application of vaccines, were unavailable. Furthermore, the web page began to display a warning stating that the site had suffered a ransomware attack and that the data had been copied, tampered and deleted by the hackers who took control of the page. Data demonstrate that the Incidents involving ransomware are increasingly recurring. Hackers use flaws in system encryption to prevent website owners from accessing them and, in order to return electronic addresses and data, request payment of a sum, an action similar to extortion and kidnapping.

Regarding what happened, the National Data Protection Authority released a press release informing that the security incident was already being monitored, and that the Ministry of Health had already been notified to provide clarifications, under the terms of the General Data Protection Law Personal. Furthermore, he explained that the Institutional Security Office and the Federal Police had been contacted so that they could conduct the appropriate investigation and supervision of the incident.

It is noteworthy that the Ministry of Health was already involved in another security accident that resulted in the leakage of sensitive personal data of several citizens. In November 2020, it was discovered that an employee at Albert Einstein Hospital, who participated in the Proadi-SUS Project, in which information is exchanged between the public health system and private hospitals to improve the system, had exposed data from around 16 million patients who would have undergone some treatment or test related to Covid-19.

The two incidents mentioned bring into focus the difficulty and absence of strong security systems at the Ministry of Health. The data processed are all characterized as sensitive, in accordance with article 5, II, of the LGPD, as they involve information about the health of the holders.

It is well known that it is up to the Ministry of Health to process this information, as there is a legal basis, including for the purposes of implementing public policies.

However, the question arises as to what risks citizens are exposed to and how the National Data Protection Authority should act to prevent these incidents from being so recurrent and that the Ministry of Health, as well as any other agent that carries out processing of data, be held responsible for repairing the damage caused.

Likewise, challenges arise regarding the massive implementation of artificial intelligence in the Brazilian health sector.

VII. Final Considerations

From everything examined, it is worth highlighting, finally, that in addition to the potential and great opportunities that we find in the application of artificial intelligence, there are implications for society, especially in the healthcare sector.

Therefore, the creation of robust legal and regulatory structures regarding the use and application of artificial intelligence has been gaining attention from countries and international organizations.

For everything analyzed, we sought to highlight the initial initiatives and guidelines of the United Nations, the World Health Organization, the European Union and Brazil, on artificial intelligence.

The emphasis sought was to highlight health-related measures. This segment proves to be of enormous importance for health, not immune to serious challenges, including data collection, digital security threats, disinformation, and discriminatory application.

Therefore, the need for regulation arises. Due to the characteristics of the Internet and artificial intelligence, such as internationality, digitalization, new global actors, such as companies and programs, we propose an international regulatory approach. Therefore, it is important to know how the main actors on the global stage, such as the United Nations, the World Health Organization, the European Union, can provide guidelines that harmonize the global legal framework for the governance of artificial intelligence.

From the above, we conclude that there is a need for new rules, specific to the phenomenon of artificial intelligence in general, and its application in the health sector, in particular.

VIII. Bibliographic references

BIONI BR. Proteção de Dados Pessoais – A Função e os Limites do Consentimento. Rio de Janeiro: Forense, 2018.

BRAZIL. Constitution of the Federal Republic of Brazil. 1988. Available at: https://www25.senado.leg.br/web/atividade/legislacao/constituicao-federal .

BRAZIL. Law n. 13.709, de 14 de agosto de 2018. General Data Protection Law Available at: www.planalto.gov.br.

BRAZIL. Law n. 13.989/2020, sanctioned on April 16, 2020, the Law authorizes the practice of Telemedicine while the pandemic continues, on an emergency basis. Available at: https://www.in.gov.br/en/web/dou/-/lei-n-13.989-de-15-de-abril-de-2020-252726328 . Repealed by Law n. 14.510/2022, sanctioned on December 27, 2022. The Law authorizes and regulates the practice of telehealth throughout the national territory. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14510.htm#:~:text=LEI%20N%C2%BA%2014.510%2C%20DE%2027,15%20de%20abril%20de%202020.

BRAZIL. Provisional Measure No. 959 of 2020 (establishes rules for emergency aid and postponement of the LGPD). Authorship: Presidency of the Republic. Available at: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141753 . Transformed into Ordinary Law n. 14058/2020, sanctioned on September 17, 2020. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L14058.htm#:~:text=Estabelece%20a%20operacionaliza%C3%A7%C3%A3o%20do%20pagamento,6%20de%20julho%20de%202020.

BRAZIL. Federal Senate. Bill n. 1,179 of 2020. Rule generated by Law No. 14,010 of 06/10/2020. Available at: https://www25.senado.leg.br/web/atividade/materias/-/materia/141306 .

BREMMER, Ian; SULEYMAN, Mustafa. The AI Power Paradox. Can States Learn to Govern Artificial Intelligence—Before It's Too Late? Foreign Affairs, 2023. Available at: https://www.foreignaffairs.com/world/artificial-intelligence-power-paradox .

CENTRE FOR INFORMATION POLICY LEADERSHIP-CIPL. Ten Recommendations for Global AI Regulation. Washington-DC, 2023. Available at: https://www.informationpolicycentre.com/ai-project.html .

CFM - Federal Council of Medicine. Resolution n. 1,643/2002, published in the D.O.U., of August 26, 2002, Section I, p. 205, the Resolution defines and regulates the provision of services through Telemedicine. Available at: http://sistemas.cfm.org.br .

DONEDA D. Da privacidade à proteção de dados. Rio de Janeiro: Renovar, 2021.

DOURADO DA; AITH FMA. A regulação da inteligência artificial na saúde no Brasil começa com a Lei Geral de Proteção de Dados Pessoais. Rev Saude Publica. 2022; 56:80. https://doi.org/10.11606/s1518- 8787.2022056004461 .

EUROPEAN COMMISSION. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF .

EUROPEAN PARLIAMENT. EU AI Act: first regulation on artificial intelligence. 2023. Available at:

https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence .

EUROPEAN PARLIAMENT. Artificial intelligence act. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf .

EUROPEAN PARLIAMENTARY RESEARCH SERVICE. Artificial intelligence in healthcare, Applications, risks, and ethical and societal impacts. EPRS | European Parliamentary Research Service. Scientific Foresight Unit (STOA). PE 729.512 – June 2022. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729512/EPRS_STU(2022)729512_EN.pdf .

EUROPEAN UNION. Charter of Fundamental Rights of the European Union. (2007/C 303/01). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12007P/TXT .

EUROPEAN UNION. Treaty on the Functioning of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016E/TXT .

https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf.

INTERNATIONAL TELECOMMUNICATION UNION. United Nations Activities on Artificial Intelligence (AI). 2022. Available at: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2022-PDF-E.pdf .

MINISTRY OF HEALTH. Comitê Gestor da Estratégia e-Saúde. Estratégia E-Saúde para o Brasil. 2017. Available at: https://www.gov.br/saude/pt-br/composicao/seidigi/saude-digital/a-estrategia-brasileira/EstrategiaesaudeparaoBrasil_CIT_20170604.pdf .

MINISTRY OF HEALTH. Conecte SUS avança em todo país com a implantação da rede nacional de dados em saúde. 2019. Available at: https://www.gov.br/saude/pt-br/assuntos/noticias/2020/junho/conecte-sus-avanca-em-todo-pais-com-a-implantacao-da-rede-nacional-de-dados-em-saude

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). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 .

SCHWAB, Klaus. A quarta revolução industrial (tradução Daniel Moreira Miranda). São Paulo: Edipro, 2016. Original title: The fourth industrial revolution.

UNITED NATIONS. High-Level Advisory Body on Artificial Intelligence. 2023. Available at: https://www.un.org/techenvoy/ai-advisory-body .

UNITED NATIONS. Roadmap for Digital Cooperation. 2020. Available at: https://www.un.org/techenvoy/content/roadmap-digital-cooperation#:~:text=On%2011%20June%202020%2C%20the,technologies%20while%20addressing%20their%20challenges.

WORLD HEALTH ORGANIZATION. Regulatory considerations on artificial intelligence for health. 2023. Available at: https://iris.who.int/bitstream/handle/10665/373421/9789240078871-eng.pdf?sequence=1&isAllowed=y .

A Summary on:

Cybersecurity for Critical Infrastructures

ADOLFO CALDEIRA*

ABSTRACT:

This paper explores the complexities and challenges in securing critical infrastructure, focusing on the vulnerabilities introduced by the convergence of Information Technology (IT) and Operational Technology (OT). Through case studies of Stuxnet and the Ukrainian Power Grid, the paper highlights the tangible risks of cyber-attacks on essential systems. It discusses the hurdles posed by technological heterogeneity, lack of standardization, human factors, and resource constraints. The paper advocates for a multi-layered, defense-in-depth approach to cybersecurity, emphasizing the need for regulatory oversight, continuous monitoring, and real-time updates. It concludes by calling for adaptive cybersecurity frameworks that can navigate the intricacies of the IT-OT landscape, thereby ensuring the resilience and security of critical infrastructure.

Keywords: Critical Infrastructure, Cybersecurity, Information Technology (IT), Operational Technology (OT)

RESUMO:

Este artigo explora as complexidades e os desafios da segurança das infra-estruturas críticas, centrando-se nas vulnerabilidades introduzidas pela convergência das tecnologias da informação (TI) e das tecnologias operacionais (TO). Através da análise de casos relativos à Stuxnet e à Rede Elétrica Ucraniana, salientamos os riscos tangíveis de ciberataques a sistemas essenciais. Discutimos os obstáculos colocados pela heterogeneidade tecnológica, a falta de estandardização, os fatores humanos e as limitações de recursos. Neste sentido, defendemos uma abordagem da cibersegurança com vários níveis de defesa em profundidade, salientando a necessidade de supervisão

regulamentar, monitorização contínua e atualizações em tempo real. Concluímos, por fim, apelando a quadros de cibersegurança adaptáveis que possam navegar pelas complexidades do cenário TI-OT, garantindo assim a resiliência e a segurança das infraestruturas críticas.

I. INTRODUCTION

To commence our exploration of cybersecurity for critical infrastructure, it is essential to first establish a general understanding of what encompasses critical infrastructure.

As the name suggests, critical infrastructure refers to the essential systems and assets that are necessary for the functioning of society, economy, and state[1]. Therefore, critical infrastructures prevent us, members of society, from plunging into chaos and anarchy, for without them, there would be no emergency number to reach in case of distress, there would be no electricity, there would be no water supply[2], all of which we take for granted as a functioning member of society, would be forfeit.

In today's digital age, the threat of cyberattacks has become increasingly prevalent, highlighting the need to protect our valuable assets and ensure the security of our society. The consequences of cyberattacks can be devastating, leaving us vulnerable and exposed when we least expect it.[3]

Despite the growing concern about cybersecurity, there is a paradoxical gap between public perception and action. Studies have shown that the public expresses great concern about cybersecurity but fails to take adequate measures to protect their safety online[4], which can by extension, be applied to the lack of cybersecurity measures in the workplace, be it neglect from the user, under-enforced cybersecurity policies, or even governmental funding.[5]

Regardless of this lack of awareness, by the public, governments and organizations, the ever-increasing frequency and severity of cyberattacks on critical

---

* Author Adolfo Caldeira is pursuing his Master's Degree in Information Security and Cyberspace Law at Instituto Superior Técnico in Lisbon, Portugal. Contact: adolfo.caldeira@tecnico.ulisboa.pt

1 M. Pavić, I. Jokanović, and M. Svilar, 'Kritična Infrastruktura U Saobraćaju', *Zb. Rad. Građev. Fak.*, 2021, doi: 10.14415/konferencijagfs2021.38.

2 R. L. Church, M. P. Scaparra, and R. S. Middleton, 'Identifying Critical Infrastructure: The Median and Covering Facility Interdiction Problems', *Ann. Assoc. Am. Geogr.*, 2004, doi: 10.1111/j.1467-8306.2004.00410.x.

3 H. Alqahtani and M. Kavakli, 'Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR)', *Information*, 2020, doi: 10.3390/info11020121.

4 H. Aljihani, F. Eassa, K. A. Almarhabi, A. Algarni, and A. Attaallah, 'Standalone Behaviour-Based Attack Detection Techniques for Distributed Software Systems via Blockchain', *Appl. Sci.*, 2021, doi: 10.3390/app11125685.

5 D. F. Norris, L. Mateczun, A. Joshi, and T. Finin, 'Cybersecurity at the Grassroots: American Local Governments and the Challenges of Internet Security', *J. Homel. Secur. Emerg. Manag.*, 2018, doi: 10.1515/jhsem-2017-0048.

infrastructures have highlighted the urgent need for effective cybersecurity measures. Prominent examples such as the Stuxnet attack, the Ukrainian power grid outage, and the Viasat attack[6] serve as stark reminders of the potential consequences of cyberattacks on our critical infrastructures. These incidents have raised awareness about the vulnerabilities and risks associated with industrial environments and underscored the importance of cybersecurity in safeguarding critical infrastructures.[7]

In this paper, we are going to explore exactly why it is it not only of paramount importance to protect our critical assets, but also, why it can be an extremely cumbersome task to accomplish, as there is an overlap between new and old technology, in a field that forgives no mistakes.

II. WHERE *IT* AND *OT* MEET

Critical infrastructures predominantly serve industrial functions, as they are designed to provide essential services and goods like energy and transportation.[8] These infrastructures largely operate on Operational Technology (OT), also known as Industrial Control Systems (ICS).

Initially, the design of industrial operations did not factor in cybersecurity, for reasons that were evident at the time. However, the landscape has dramatically shifted, rendering what was once considered "air-gapped" and impenetrable in the OT world as vulnerable as its IT counterpart.[9]

The shift towards integrating Information Technology (IT) with OT has gained

---

6 'Viasat cyberattack blamed on Russian wiper malware | TechCrunch'. Accessed: Oct. 22, 2023. [Online]. Available: https://techcrunch.com/2022/03/31/viasat-cyberattack-russian-wiper/?guce_referrer=aHR0cHM6Ly9jeWJlcmNvbmZsaWN0cy5jeWJlcnBlYWNlaW5zdGl0dXRlLm9yZy8&guce_referrer_sig=AQAAAA-76w1U0VWPeQcKthA8Qn9FrbGFn_LJ8Gpo7BTmkqi9hLH5jeR9s07fHSq1qJzCTYEq1y-LySbAVo65P_m7pls-XHMA9IzCiD_UzDIX3ULjIbpPM6cL5Cu0iCDl3ONOYPmCRkAsCcUTo2jw9KbrxrvLud47B7hCu7t0fTGcjjij&guccounter=2

7 V. D. Savin, 'Cyber-Security in the New Era of Integrated Operational – Informational Technology Systems', *Bus. Excell. Manag.*, 2021, doi: 10.24818/beman/2021.11.1-05.

8 E. Ferrario, N. Pedroni, and E. Zio, 'Evaluation of the Robustness of Critical Infrastructures by Hierarchical Graph Representation, Clustering and Monte Carlo Simulation', *Reliab. Eng. Syst. Saf.*, 2016, doi: 10.1016/j.ress.2016.06.007.

9 'Common ICS Cybersecurity Myth #1: The Air Gap'. Accessed: Oct. 23, 2023. [Online]. Available: https://gca.isa.org/blog/common-ics-cybersecurity-myth-1-the-air-gap

momentum, a trend further accelerated by the COVID-19 lockdowns that necessitated remote work.[10] This convergence, while beneficial for operational efficiency, introduces a unique set of challenges, particularly in cybersecurity.

IT systems, designed primarily for data processing and transfer, focus on the Confidentiality and Integrity aspects of the CIA triad in Information Security. In stark contrast, OT systems, which are engineered to monitor and control physical processes, prioritize Availability. This is especially crucial as these systems have a direct impact on human safety.[11]

Navigating this complex landscape requires a nuanced understanding of the operational priorities of both IT and OT systems. While IT systems can afford frequent updates to address security vulnerabilities, OT systems must exercise caution. Any downtime in OT could lead to catastrophic operational disruptions with the potential to endanger human lives.

III. CHALLENGES IN SECURING CRITICAL INFRASTRUCTURE

i) Technological Heterogeneity

The inherent technological heterogeneity in critical infrastructure systems introduces a significant layer of complexity to cybersecurity efforts. These systems frequently encompass a broad spectrum of technologies, each with distinct security vulnerabilities and requirements. On one end, there are Operational Technology (OT) devices, often legacy systems that have been running continuously for decades and consequently lack modern security features. On the other end are state-of-the-art Information Technology (IT) and Internet of Things (IoT) devices, which present their own unique security challenges.[12]

In this context, cybersecurity professionals face formidable challenges related to

10 'How COVID-19 affects OT Security', Applied Risk. Accessed: Oct. 28, 2023. [Online]. Available: https://applied-risk.com/resources/covid19-ot-security

11 G. Murray, M. N. Johnstone, and C. Valli, 'The convergence of IT and OT in critical infrastructure', *Aust. Inf. Secur. Manag. Conf.*, 2017, doi: 10.4225/75/5A84F7B595B4E.

12 T. Limba, T. Plėta, K. Agafonov, and M. Damkus, 'Cyber Security Management Model for Critical Infrastructure', *J. Entrep. Sustain. Issues*, 2017, doi: 10.9770/jesi.2017.4.4(12).

system integration. The melding of diverse technologies inherently expands the attack surface, offering more opportunities for malicious actors to exploit vulnerabilities. This complexity often results in security gaps, as traditional IT security solutions may not be directly transferable to OT environments. Consequently, specialized security protocols, tailored to the unique characteristics of each technology, become a necessity.[13]

ii) Lack of Standardization

The lack of uniform cybersecurity standards in critical infrastructures creates a significant hurdle in securing these systems. This inconsistency in security implementation and management across various sectors and technologies is exacerbated by the perception that existing standards are "too complex and hard to navigate." Due to the complexity inherent in ICT systems, industrial safety and security standards are often viewed as overly intricate and challenging to apply.[14]

Consequently, organizations may resort to simpler approaches, such as checklists, for security measures as the application of these industrial standards also frequently requires specialized technical skills.

The healthcare sector is notably impacted by the absence of standardized cybersecurity protocols. Research indicates that this lack of standardization, coupled with the interconnected nature of healthcare systems, significantly amplifies cybersecurity vulnerabilities, thereby posing a risk to the consistent and reliable delivery of healthcare services.[15]

In the energy sector, the issue of standardization is similarly pressing. While the adoption of the NIST Framework for Improving Critical Infrastructure[16] is prevalent in the United States, a notable lack of standardization exists in European countries. This discrepancy leads to inconsistencies in cybersecurity management policies across

13 M. M. El-Dyasty and A. A. Elamer, 'The Effect of Auditor Type on Audit Quality in Emerging Markets: Evidence From Egypt', *Int. J. Account. Inf. Manag.*, 2020, doi: 10.1108/ijaim-04-2020-0060.
14 Ruth Østgaard Skotnes, 'Standardization of cybersecurity for critical infrastructures', Nov. 2019, doi: https://doi.org/10.4324/9780429290817-10.
15 L. Coventry and D. B. Branley, 'Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward', *Maturitas*, 2018, doi: 10.1016/j.maturitas.2018.04.008.
16 M. P. Barrett, 'Framework for Improving Critical Infrastructure Cybersecurity Version 1.1', *NIST*, Apr. 2018, Accessed: Oct. 28, 2023. [Online]. Available: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

different regions.[17]

The railways also face these problems, with the adoption of ICT-based technologies, this sector is now more vulnerable to cyber-related threats. To help mitigate these threats, L. Coventry and D. Branley propose a Cybersecurity Capability Maturity Model (C2M2), that can be used to assess and enhance cybersecurity capabilities, diving the subject into different domains, each with different maturity levels and associated practices. Organizations can therefore use this model to identify gaps and improve their cybersecurity posture, aiding in compliance and risk management for the railway sector.[18]

It is, however, worth considering the adoption of the IEC 62443 standard, and although this framework is not addressed to a specific sector, it is designed to help secure Industrial Automation and Control Systems (ICS), which can be tailored to specific needs and complexities.[19]

iii) Human Factors

Human factors are integral to the efficacy of cybersecurity initiatives. Even with technological advancements, the security of critical infrastructure remains susceptible to human errors or lapses in awareness. The increasing body of research on the role of human factors in information security underscores their importance in fortifying cybersecurity measures.[20]

A key element in bolstering an organization's cybersecurity is the human aspect. The prevailing theory identifies three core components—human, technical, and organizational—as vital to enhancing cybersecurity measures.[21] This emphasizes the

17 M. Tvaronavičienė, T. Plėta, S. D. Casa, and J. Latvys, 'Cyber Security Management of Critical Energy Infrastructure in National Cybersecurity Strategies: Cases of USA, UK, France, Estonia and Lithuania', *Insights Reg. Dev.*, 2020, doi: 10.9770/ird.2020.2.4(6).
18 R. Kour, R. Karim, and A. Thaduri, 'Cybersecurity for Railways – A Maturity Model', *Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit*, 2019, doi: 10.1177/0954409719881849.
19 I. Mugarza, J. L. M. Flores, and J. L. Montero, 'Security Issues and Software Updates Management in the Industrial Internet of Things (IIoT) Era', *Sensors*, 2020, doi: 10.3390/s20247160.
20 L. Hadlington, 'Human Factors in Cybersecurity; Examining the Link Between Internet Addiction, Impulsivity, Attitudes Towards Cybersecurity, and Risky Cybersecurity Behaviours', *Heliyon*, 2017, doi: 10.1016/j.heliyon.2017.e00346.
21 M. Al-Ma'aitah, 'Investigating the Drivers of Cybersecurity Enhancement in Public Organizations: The Case of Jordan', *Electron. J. Inf. Syst. Dev. Ctries.*, 2022, doi: 10.1002/isd2.12223.

pivotal role that human factors play in shaping an organization's overall cybersecurity stance.

In the realm of critical infrastructure entities, human elements are indispensable for ensuring cybersecurity. The provision of comprehensive cybersecurity training to employees in these organizations is crucial for sustaining a secure operational landscape. This accentuates the vital role that human factors occupy in shaping an organization's collective cybersecurity defenses.[22]

Factors such as stress, occupational burnout, and security fatigue are human variables that can adversely affect cybersecurity measures. The ongoing issues related to human performance in cybersecurity can be traced back to insufficient education on these human-centric factors. Addressing and educating on these human elements can significantly enhance the efficacy of cybersecurity initiatives.[23]

iv) Resource Constraints

Resource constraints present formidable challenges to the effective deployment of cybersecurity measures, especially in sectors involving critical infrastructure.[24] Financial limitations often restrict organizations from procuring cutting-edge cybersecurity technologies, compounded by the ongoing costs of updates and maintenance. The scarcity of qualified cybersecurity professionals further aggravates these constraints, leaving organizations vulnerable to risks that could otherwise be managed.[25]

As stated previously, technological limitations are another facet of resource constraints. Legacy systems, often prevalent in critical infrastructure, may lack compatibility with contemporary security solutions, thereby hindering cybersecurity

22 N. Chowdhury, E. Nystad, K. Reegård, and V. Gkioulos, 'Cybersecurity Training in Norwegian Critical Infrastructure Companies', *Int. J. Saf. Secur. Eng.*, 2022, doi: 10.18280/ijsse.120304.
23 C. Nobles, 'Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem', *Holistica – J. Bus. Public Adm.*, 2022, doi: 10.2478/hjbpa-2022-0003.
24 L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, 'The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective', *J. Account. Public Policy*, 2015, doi: 10.1016/j.jaccpubpol.2015.05.001.
25 M. Sallos, A. Garcia-Perez, D. Bedford, and B. Orlando, 'Strategy and Organisational Cybersecurity: A Knowledge-Problem Perspective', *J. Intellect. Cap.*, 2019, doi: 10.1108/jic-03-2019-0041.

initiatives.[26]

To mitigate these constraints, organizations could explore economical options such as open-source software or cloud-based security solutions.[27] Collaborative endeavors, including inter-organizational information sharing and public-private partnerships, offer avenues for resource optimization and improved cybersecurity outcomes.[28]

Investment in intellectual capital, encompassing cybersecurity training and preparedness, can induce positive shifts in cybersecurity investment, especially in post-crisis scenarios.[29]

In the context of critical infrastructure, stringent cybersecurity protocols are imperative for safeguarding both sector-specific data and the infrastructure itself.[30]

IV. CASE STUDIES

i) Stuxnet

Stuxnet serves as a pivotal case study in cybersecurity, particularly illuminating vulnerabilities in critical infrastructure. Originating as a computer worm, it targeted SCADA systems with the aim of debilitating Iran's nuclear facilities.[31] The intricacy of the attack exposed gaps in existing cybersecurity frameworks and prompted scrutiny of their sufficiency.

One salient takeaway is the imperative for fortified cybersecurity protocols for SCADA systems. Research presents a fractional-order mathematical model of Stuxnet, facilitating the analysis of its propagation dynamics and attack vectors on isolated critical

26 A. Garcia-Perez, M. Sallos, and P. Tiwasing, 'Dimensions of Cybersecurity Performance and Crisis Response in Critical Infrastructure Organisations: An Intellectual Capital Perspective', *J. Intellect. Cap.*, 2021, doi: 10.1108/jic-06-2021-0166.
27 Supra note 24.
28 Ibid.
29 A. Garcia-Perez, M. Sallos, and P. Tiwasing, 'Dimensions of Cybersecurity Performance and Crisis Response in Critical Infrastructure Organisations: An Intellectual Capital Perspective', *J. Intellect. Cap.*, 2021, doi: 10.1108/jic-06-2021-0166.
30 K. K. Millett, E. d. Santos, and P. Millett, 'Cyber-Biosecurity Risk Perceptions in the Biotech Sector', *Front. Bioeng. Biotechnol.*, 2019, doi: 10.3389/fbioe.2019.00136.
31 T. Wu, J. F. P. Disso, K. Jones, and A. I. Campos, 'Towards a SCADA Forensics Architecture', 2013, doi: 10.14236/ewic/icscsr2013.2.

infrastructures.[32] This underscores the necessity of comprehending the behavior of such malware for devising effective countermeasures.

The Stuxnet incident also revealed the tangible impact of cyber-physical attacks. Discussions focus on the detrimental effects an informed adversary can exert on safety-critical infrastructures.[33] The authors advocate for data integrity monitoring in reactor protection systems, leveraging technologies like blockchain for enhanced security.

Moreover, the Stuxnet case accentuates the role of international collaboration in cybersecurity. Discussions around secure control frameworks for resource-constrained adversaries are pertinent, given Stuxnet's targeted nature.[34] Global cooperation is indispensable for tackling cyber threats with international ramifications.

Additionally, Stuxnet provides a framework for analyzing security threats in cyber-physical systems. Research employs a systems theoretic approach for a detailed analysis of the attack, emphasizing the need for a holistic understanding of vulnerabilities in cyber-physical systems.[35]

The feasibility of cyber manipulations affecting physical processes in SCADA networks was also highlighted by Stuxnet. Research discusses smart behavioral filters for SCADA networks, citing Stuxnet as a proof-of-concept.[36] This accentuates the need for advanced detection and prevention mechanisms, such as artificial intelligence.

Stuxnet was a watershed moment, being the first identified malware targeting critical infrastructure, specifically SCADA systems. The need for specialized SCADA forensics architectures for investigating such attacks is discussed,[37] emphasizing the importance of specialized investigative tools.

---

32 Z. Masood, M. A. Z. Raja, N. I. Chaudhary, K. M. Cheema, and A. H. Milyani, 'Fractional Dynamics of Stuxnet Virus Propagation in Industrial Control Systems', *Mathematics*, 2021, doi: 10.3390/math9172160.

33 M. K. Choi, C. Y. Yeun, and P. H. Seong, 'A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology', *Ieee Access*, 2020, doi: 10.1109/access.2020.3005134.

34 A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, 'A Secure Control Framework for Resource-Limited Adversaries', *Automatica*, 2015, doi: 10.1016/j.automatica.2014.10.067.

35 A. Nourian and S. E. Madnick, 'A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet', *Ieee Trans. Dependable Secure Comput.*, 2018, doi: 10.1109/tdsc.2015.2509994.

36 G. Corbò, C. Foglietta, C. Palazzo, and S. Panzieri, 'Smart Behavioural Filter for SCADA Network', 2017, doi: 10.1007/978-3-319-52569-3_9.

37 Supra note 31

Implications for smart grid security also arise from the Stuxnet case. Research focuses on the cyber-physical security aspects of wide-area monitoring in smart grids.[38] Stuxnet serves as a cautionary tale for the potential physical impacts of sophisticated cyber-attacks on smart grid systems.

Effective modeling and evaluation of cyber-physical system security are also necessitated by the Stuxnet attack. Research proposes methodologies for identifying vulnerabilities and assessing countermeasure effectiveness,[39] highlighting the need for proactive security strategies.

Stuxnet also raises alarms about the stability of power grids. Research discusses internet-based load-altering attacks against smart grids, emphasizing the need for robust cybersecurity measures.[40]

Lastly, the human element in cyber-attacks is not to be overlooked. Research discusses the social engineering tactics employed by Stuxnet's architects,[41] underlining the importance of user education and awareness.

The Stuxnet attack serves as a seminal case study, spotlighting the vulnerabilities in critical infrastructure and questioning the adequacy of extant cybersecurity measures. It underscores the need for robust SCADA system security, the tangible risks of cyber-physical attacks, and the indispensability of international cooperation. It also emphasizes the importance of proactive security measures, advanced technologies, and human factors in cybersecurity.

ii) Ukrainian Power Grid

The cyber-attack on Ukraine's power grid in 2015 serves as a critical case study, revealing the fragility of energy infrastructure in the face of sophisticated cyber threats. The incident led to widespread electrical outages and emphasized the sector's

38 A. Ashok, A. Hahn, and G. Manimaran, 'Cyber-Physical Security of Wide-Area Monitoring, Protection and Control in a Smart Grid Environment', *J. Adv. Res.*, 2014, doi: 10.1016/j.jare.2013.12.005.
39 H. Orojloo and M. A. Azgomi, 'A Method for Modeling and Evaluation of the Security of Cyber-Physical Systems', 2014, doi: 10.1109/iscisc.2014.6994036.
40 A.-H. Mohsenian-Rad and A. Leon-Garcia, 'Distributed Internet-Based Load Altering Attacks Against Smart Power Grids', *Ieee Trans. Smart Grid*, 2011, doi: 10.1109/tsg.2011.2160297.
41 V. Mancuso, A. J. Strang, G. J. Funke, and V. Finomore, 'Human Factors of Cyber Attacks', *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, 2014, doi: 10.1177/1541931214581091.

vulnerability.

One of the primary insights from this event is the crucial role of real-time surveillance and immediate incident management. The Ukraine incident demonstrates the urgency for vigilant oversight of essential systems to detect and neutralize cyber threats as they emerge.[42] Effective monitoring systems are vital for the early identification and mitigation of cyber risks.

Furthermore, the event underscores the strategic importance of alliances between public institutions and private corporations in enhancing cybersecurity. These synergies can pool resources and expertise from both sectors, thereby improving the overall security posture.[43] Such collaborations are instrumental in facilitating a culture of information sharing, collective threat analysis, and the establishment of cybersecurity best practices.[44]

To fortify the vulnerabilities exposed by the Ukraine incident, a multi-layered cybersecurity approach is advisable. This should include the incorporation of secure authentication methods, specialized hardware modules, and unique physical identifiers to deter unauthorized access and cyber-attacks.[45] Additionally, the entry of traditional energy players into emerging markets can foster technological credibility and facilitate the exchange of expertise, thereby strengthening the resilience of essential systems.[46]

The 2015 cyber-attack on Ukraine's power grid was a significant event that exposed the vulnerabilities inherent in critical energy infrastructure. It emphasized the need for advanced cybersecurity protocols, vigilant real-time monitoring, and effective incident response mechanisms. The collaboration between public and private sectors is vital for enhancing security measures, and a layered approach to cybersecurity is essential for protecting critical systems from future threats.

---

42 S. Atkins and C. Lawson, 'An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure', *Public Adm. Rev.*, 2021, doi: 10.1111/puar.13322.
43 M. Carr, 'Public-Private Partnerships in National Cyber-Security Strategies', *Int. Aff.*, 2016, doi: 10.1111/1468-2346.12504.
44 T. Bovaird, 'Public–Private Partnerships: From Contested Concepts to Prevalent Practice', *Int. Rev. Adm. Sci.*, 2004, doi: 10.1177/0020852304044250.
45 H. Thapliyal and S. P. Mohanty, 'Physical Unclonable Function (PUF)-Based Sustainable Cybersecurity', *Ieee Consum. Electron. Mag.*, 2021, doi: 10.1109/mce.2021.3065857.
46 M. Steen and T. J. Weaver, 'Incumbents' Diversification and Cross-Sectorial Energy Industry Dynamics', *Res. Policy*, 2017, doi: 10.1016/j.respol.2017.04.001.

V. RECCOMMENDATIONS AND FUTURE DIRECTIONS

i) *Implementation of Multi-Layered Security*

The rapidly evolving landscape of cyber threats demands a multi-layered, comprehensive approach to security, particularly in critical infrastructure sectors. This is often termed as defense-in-depth. Endpoint security is the first layer, employing antivirus software and intrusion detection systems to protect individual devices from cyber threats.[47] Network security forms the next layer, utilizing firewalls, virtual private networks (VPNs), and network segmentation to safeguard communication channels and infrastructure.[48]

Application security focuses on the integrity of software applications, employing secure coding practices, vulnerability assessments, and penetration testing.[49] Data security is another pivotal layer, emphasizing encryption, access controls, and data backup and recovery processes to ensure the confidentiality, integrity, and availability of data.[50] Identity and access management (IAM) is crucial for controlling user access to systems and resources, involving strong authentication, role-based access control, and user provisioning.[51]

Physical security is also essential, involving surveillance systems, access controls, and security guards to prevent unauthorized physical access and tampering.[52] Beyond these technical measures, a well-defined incident response plan is indispensable for effectively responding to and mitigating cyber incidents. This plan should outline the steps for incident detection, containment, eradication, and recovery.[53]

Collaboration between the public and private sectors is also beneficial for strengthening this multi-layered security approach. Such collaboration can involve

---

47 A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, 'A Strong User Authentication Framework for Cloud Computing', 2011, doi: 10.1109/apscc.2011.14.
48 P. Żebrowski, A. C. Vieira, and A. Mancuso, 'A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber-Physical Systems', Risk Anal., 2022, doi: 10.1111/risa.13900.
49 S. Li, T. Tryfonas, and H. Li, 'The Internet of Things: A Security Point of View', *Internet Res.*, 2016, doi: 10.1108/intr-07-2014-0173.
50 D. Pöhn and W. Hommel, 'Computer Security', 2020, doi: 10.1007/978-3-030-66504-3.
51 Ibid.
52 E. Viganò, M. Loi, and E. Yaghmaei, 'Cybersecurity of Critical Infrastructure', 2020, doi: 10.1007/978-3-030-29053-5_8.
53 R. Shandler, M. L. Gross, S. Backhaus, and D. Canetti, 'Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment', *Br. J. Polit. Sci.*, 2021, doi: 10.1017/s0007123420000812.

information sharing, joint exercises, and coordinated response efforts, leveraging the expertise and resources of both sectors.

In summary, the complex and ever-changing nature of cyber threats necessitates a robust, multi-layered security approach, augmented by public-private partnerships, for the protection of critical infrastructure sectors.

ii) ***Regulatory oversight***

Regulatory oversight is pivotal for establishing a foundational level of cybersecurity within critical infrastructure sectors. To this end, regulatory bodies should enforce compliance with recognized cybersecurity standards such as NIST or IEC 62443, providing a structured framework for these sectors to bolster their cybersecurity measures.[54]

Periodic audits are essential for ensuring sustained compliance and identifying areas for improvement within critical infrastructure. These audits scrutinize an organization's cybersecurity protocols, ensuring alignment with established standards and preemptively identifying vulnerabilities.[55]

To incentivize compliance within critical infrastructure sectors, stringent penalties for non-adherence should be enforced. The severity of these penalties should be commensurate with the level of non-compliance, compelling organizations to prioritize cybersecurity.[56]

Inclusive governance, involving non-state actors, can offer additional layers of oversight and critical policy assessment, specifically tailored for critical infrastructure.[57] Board members within these sectors are also pivotal, expected to be proactive in

54 Supra note 30

55 R. Messnarz, D. Ekert, G. Macher, A. Much, T. Zehetner, and L. Aschbacher, 'Experiences With the Automotive SPICE for Cybersecurity Assessment Model and Tools', *J. Softw. Evol. Process*, 2022, doi: 10.1002/smr.2519.

56 J. D'Arcy, A. Hovav, and D. F. Galletta, 'User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach', *Inf. Syst. Res.*, 2009, doi: 10.1287/isre.1070.0160.

57 S. Kumar, 'The Missing Piece in Human-Centric Approaches to Cybernorms Implementation: The Role of Civil Society', *J. Cyber Policy*, 2021, doi: 10.1080/23738871.2021.1909090.

comprehending and managing cybersecurity risks.[58]

As cyber threats evolve, continuous reassessment of cybersecurity measures is imperative for critical infrastructure. The role of auditors in these sectors extends to evaluating cybersecurity risks. While empirical data on this subject is limited, auditors can integrate cybersecurity risk disclosures into their assessments and fee structures, reflecting the unique challenges faced by critical infrastructure.[59]

Economic theories can offer insights into cybersecurity decision-making within critical infrastructure, addressing market failures and perverse incentives that are particularly relevant to these sectors.[60]

Regulatory oversight is, therefore, essential for maintaining a baseline cybersecurity standard in critical infrastructure sectors. This is augmented by periodic audits, stringent penalties, inclusive governance, continuous reassessment, and auditor involvement.

iii) *Continuous Monitoring and Updating*

Continuous monitoring and real-time updates are imperative for fortifying the cybersecurity posture of critical infrastructure, particularly in safeguarding vulnerable Operational Technology (OT) systems.[61] Traditional cybersecurity measures, often reliant on static algorithms, are increasingly inadequate for countering dynamically evolving cyber threats.[62] This necessitates the adoption of dynamic cybersecurity capabilities that can adapt to emerging threats, thereby offering a more robust defense mechanism.

The inability to regularly update OT systems due to operational constraints

58 T. G. Calderon and L. Gao, 'Cybersecurity Risks Disclosure and Implied Audit Risks: Evidence From Audit Fees', *Int. J. Audit.*, 2020, doi: 10.1111/ijau.12209.
59 P. Rosati, F. Gogolin, and T. Lynn, 'Audit Firm Assessments of Cyber-Security Risk: Evidence From Audit Fees and SEC Comment Letters', *Int. J. Account.*, 2019, doi: 10.1142/s1094406019500136.
60 A. Fedele and C. Roner, 'Dangerous Games: A Literature Review on Cybersecurity Investments', *J. Econ. Surv.*, 2021, doi: 10.1111/joes.12456.
61 X. Wang, Y. Han, C. Wang, Q. Zhao, C. Xu, and M. Chen, 'In-Edge AI: Intelligentizing Mobile Edge Computing, Caching and Communication by Federated Learning', *Ieee Netw.*, 2019, doi: 10.1109/mnet.2019.1800286.
62 D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. M. Khan, and N. Meskin, 'Cybersecurity for Industrial Control Systems: A Survey', *Comput. Secur.*, 2020, doi: 10.1016/j.cose.2019.101677.

accentuates the importance of the layers of protection that precede these systems.[63] Metrics for assessing the security posture of industrial control systems, including real-time monitoring and visualization, are thus critical.[64]

Moreover, the integration of cyber intelligence into security protocols is essential for proactively identifying and mitigating potential threats. Techniques such as machine learning can further enhance the efficacy of these intelligence systems by clustering malicious URLs, thereby aiding in the early identification of cyber threats.[65]

A multi-faceted approach involving continuous monitoring, dynamic capabilities, and cyber intelligence is crucial for safeguarding critical infrastructure. This is particularly relevant for OT systems, which due to their operational constraints, cannot be updated as frequently as their IT counterparts.

VI. CONCLUSION

The cybersecurity landscape for critical infrastructure is fraught with complexities and challenges, exacerbated by the convergence of Information Technology (IT) and Operational Technology (OT). This paper has elucidated the vulnerabilities inherent in critical infrastructure systems, emphasizing the urgent need for robust cybersecurity measures. The technological heterogeneity, lack of standardization, human factors, and resource constraints present formidable hurdles in securing these essential systems.[66]

The case studies of Stuxnet and the Ukrainian Power Grid serve as cautionary tales, highlighting the tangible risks and far-reaching consequences of cyber-attacks on critical infrastructure.[67] These incidents underscore the necessity for a multi-layered, defense-in-depth approach to security, involving endpoint, network, application, data, and physical security measures.[68]

Regulatory oversight is pivotal for establishing a foundational level of

63 H. Kim, 'Security and Vulnerability of SCADA Systems Over IP-Based Wireless Sensor Networks', *Int. J. Distrib. Sens. Netw.*, 2012, doi: 10.1155/2012/268478.
64 Ibid
65 A. Yeboah-Ofori and S. Islam, 'Cyber Security Threat Modeling for Supply Chain Organizational Environments', *Future Internet*, 2019, doi: 10.3390/fi11030063.
66 Supra note 12; Supra note 14; Supra note 20; Supra note 24
67 Supra note 31.; Supra note 42
68 Supra note 47, Supra note 48, Supra note 49, Supra note 50, Supra note 52

cybersecurity within critical infrastructure sectors. Compliance with recognized standards, periodic audits, and stringent penalties for non-compliance are essential components of a comprehensive cybersecurity strategy.[69] Inclusive governance and board engagement further augment these efforts, providing additional layers of oversight and critical policy assessment.[70]

The paper also advocates for continuous monitoring and real-time updates, particularly in the context of vulnerable OT systems. Given the operational constraints that limit frequent updates to OT systems, the layers of protection that precede these systems become even more critical.[71] The integration of cyber intelligence and dynamic capabilities into security protocols offers a more adaptive and proactive approach to countering evolving cyber threats.[72]

In summary, safeguarding critical infrastructure necessitates a multi-faceted, dynamic approach that integrates technological, human, and organizational elements. As cyber threats continue to evolve, so must our strategies for defending the essential systems that underpin our society, economy, and state. Future work should focus on the development of adaptive cybersecurity frameworks that can effectively navigate the complexities of the IT-OT landscape, thereby ensuring the resilience and security of our critical infrastructure.

69 Supra note 30, Supra note 55, Supra note 56
70 Supra note 57, Supra note 58
71 Supra note 61, Supra note 63
72 Supra note 62, Supra note 65

VII. BIBLIOGRAPHY

‘Common ICS Cybersecurity Myth #1: The Air Gap’. Accessed: Oct. 23, 2023. [Online]. Available: https://gca.isa.org/blog/common-ics-cybersecurity-myth-1-the-air-gap

‘How COVID-19 affects OT Security’, Applied Risk. Accessed: Oct. 28, 2023. [Online]. Available: https://applied-risk.com/resources/covid19-ot-security

‘Viasat cyberattack blamed on Russian wiper malware | TechCrunch’. Accessed: Oct. 22, 2023. [Online]. Available: https://techcrunch.com/2022/03/31/viasat-cyberattack-russian-wiper/?guce_referrer=aHR0cHM6Ly9jeWJlcmNvbmZsaWN0cy5jeWJlcnBlYWNlaW5zdGl0dXRlLm9yZy8&guce_referrer_sig=AQAAAA-76w1U0VWPeQcKthA8Qn9FrbGFn_LJ8Gpo7BTmkqi9hLH5jeR9s07fHSq1qJzCTYEq1y-LySbAVo65P_m7pls-XHMA9IzCiD_UzDIX3ULjIbpPM6cL5Cu0iCDl3ONOYPmCRkAsCcUTo2jw9KbrxrvLud47B7hCu7t0fTGcjjij&guccounter=2

A. Ashok, A. Hahn, and G. Manimaran, ‘Cyber-Physical Security of Wide-Area Monitoring, Protection and Control in a Smart Grid Environment’, J. Adv. Res., 2014, doi: 10.1016/j.jare.2013.12.005.

A. Fedele and C. Roner, ‘Dangerous Games: A Literature Review on Cybersecurity Investments’, J. Econ. Surv., 2021, doi: 10.1111/joes.12456.

A. Garcia-Perez, M. Sallos, and P. Tiwasing, ‘Dimensions of Cybersecurity Performance and Crisis Response in Critical Infrastructure Organisations: An Intellectual Capital Perspective’, J. Intellect. Cap., 2021, doi: 10.1108/jic-06-2021-0166.

A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, ‘A Strong User Authentication Framework for Cloud Computing’, 2011, doi: 10.1109/apscc.2011.14.

A. Nourian and S. E. Madnick, ‘A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet’, Ieee Trans. Dependable Secure Comput., 2018, doi: 10.1109/tdsc.2015.2509994.

A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, ‘A Secure Control Framework for Resource-Limited Adversaries’, Automatica, 2015, doi: 10.1016/j.automatica.2014.10.067.

A. Yeboah-Ofori and S. Islam, ‘Cyber Security Threat Modeling for Supply Chain Organizational Environments’, Future Internet, 2019, doi: 10.3390/fi11030063.

A.-H. Mohsenian-Rad and A. Leon-Garcia, ‘Distributed Internet-Based Load Altering Attacks Against Smart Power Grids’, Ieee Trans. Smart Grid, 2011, doi: 10.1109/tsg.2011.2160297.

C. Nobles, ‘Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem’, Holistica – J. Bus. Public Adm., 2022, doi: 10.2478/hjbpa-2022-0003.

D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. M. Khan, and N. Meskin, ‘Cybersecurity for Industrial Control Systems: A Survey’, Comput. Secur., 2020, doi: 10.1016/j.cose.2019.101677.

D. F. Norris, L. Mateczun, A. Joshi, and T. Finin, ‘Cybersecurity at the Grassroots: American Local Governments and the Challenges of Internet Security’, J. Homel. Secur. Emerg. Manag., 2018, doi: 10.1515/jhsem-2017-0048.

D. Pöhn and W. Hommel, ‘Computer Security’, 2020, doi: 10.1007/978-3-030-66504-3.

E. Ferrario, N. Pedroni, and E. Zio, ‘Evaluation of the Robustness of Critical Infrastructures by Hierarchical Graph Representation, Clustering and Monte Carlo Simulation’, Reliab. Eng. Syst. Saf., 2016, doi: 10.1016/j.ress.2016.06.007.

E. Viganò, M. Loi, and E. Yaghmaei, ‘Cybersecurity of Critical Infrastructure’, 2020, doi: 10.1007/978-3-030-29053-5_8.

G. Corbò, C. Foglietta, C. Palazzo, and S. Panzieri, ‘Smart Behavioural Filter for SCADA Network’, 2017, doi: 10.1007/978-3-319-52569-3_9.

G. Murray, M. N. Johnstone, and C. Valli, ‘The convergence of IT and OT in critical infrastructure’, Aust. Inf. Secur. Manag. Conf., 2017, doi: 10.4225/75/5A84F7B595B4E.

H. Aljihani, F. Eassa, K. A. Almarhabi, A. Algarni, and A. Attaallah, ‘Standalone Behaviour-Based Attack Detection Techniques for Distributed Software Systems via Blockchain’, Appl. Sci., 2021, doi: 10.3390/app11125685.

H. Alqahtani and M. Kavakli, ‘Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR)’, Information, 2020, doi: 10.3390/info11020121.

H. Kim, ‘Security and Vulnerability of SCADA Systems Over IP-Based Wireless Sensor Networks’, Int. J. Distrib. Sens. Netw., 2012, doi: 10.1155/2012/268478.

H. Orojloo and M. A. Azgomi, ‘A Method for Modeling and Evaluation of the Security of Cyber-Physical Systems’, 2014, doi: 10.1109/iscisc.2014.6994036.

H. Thapliyal and S. P. Mohanty, ‘Physical Unclonable Function (PUF)-Based Sustainable Cybersecurity’, Ieee Consum. Electron. Mag., 2021, doi: 10.1109/mce.2021.3065857.

I. Mugarza, J. L. M. Flores, and J. L. Montero, ‘Security Issues and Software Updates Management in the Industrial Internet of Things (IIoT) Era’, Sensors, 2020, doi: 10.3390/s20247160.

J. D’Arcy, A. Hovav, and D. F. Galletta, ‘User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach’, Inf. Syst. Res., 2009, doi: 10.1287/isre.1070.0160.

K. K. Millett, E. d. Santos, and P. Millett, ‘Cyber-Biosecurity Risk Perceptions in the Biotech Sector’, Front. Bioeng. Biotechnol., 2019, doi: 10.3389/fbioe.2019.00136.

L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, ‘The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective’, J. Account. Public Policy, 2015, doi: 10.1016/j.jaccpubpol.2015.05.001.

L. Coventry and D. B. Branley, ‘Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward’, Maturitas, 2018, doi: 10.1016/j.maturitas.2018.04.008.

L. Hadlington, ‘Human Factors in Cybersecurity; Examining the Link Between Internet Addiction, Impulsivity, Attitudes Towards Cybersecurity, and Risky Cybersecurity Behaviours’, Heliyon, 2017, doi: 10.1016/j.heliyon.2017.e00346.

M. Al-Ma’aitah, ‘Investigating the Drivers of Cybersecurity Enhancement in Public Organizations: The Case of Jordan’, Electron. J. Inf. Syst. Dev. Ctries., 2022, doi: 10.1002/isd2.12223.

M. Carr, ‘Public-Private Partnerships in National Cyber-Security Strategies’, Int. Aff., 2016, doi: 10.1111/1468-2346.12504.

M. K. Choi, C. Y. Yeun, and P. H. Seong, ‘A Novel Monitoring System for the Data

Integrity of Reactor Protection System Using Blockchain Technology', Ieee Access, 2020, doi: 10.1109/access.2020.3005134.

M. M. El-Dyasty and A. A. Elamer, 'The Effect of Auditor Type on Audit Quality in Emerging Markets: Evidence From Egypt', Int. J. Account. Inf. Manag., 2020, doi: 10.1108/ijaim-04-2020-0060.

M. P. Barrett, 'Framework for Improving Critical Infrastructure Cybersecurity Version 1.1', NIST, Apr. 2018, Accessed: Oct. 28, 2023. [Online]. Available: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

M. Pavić, I. Jokanović, and M. Svilar, 'Kritična Infrastruktura U Saobraćaju', Zb. Rad. Građev. Fak., 2021, doi: 10.14415/konferencijagfs2021.38.

M. Sallos, A. Garcia-Perez, D. Bedford, and B. Orlando, 'Strategy and Organisational Cybersecurity: A Knowledge-Problem Perspective', J. Intellect. Cap., 2019, doi: 10.1108/jic-03-2019-0041.

M. Steen and T. J. Weaver, 'Incumbents' Diversification and Cross-Sectorial Energy Industry Dynamics', Res. Policy, 2017, doi: 10.1016/j.respol.2017.04.001.

M. Tvaronavičienė, T. Plėta, S. D. Casa, and J. Latvys, 'Cyber Security Management of Critical Energy Infrastructure in National Cybersecurity Strategies: Cases of USA, UK, France, Estonia and Lithuania', Insights Reg. Dev., 2020, doi: 10.9770/ird.2020.2.4(6).

N. Chowdhury, E. Nystad, K. Reegård, and V. Gkioulos, 'Cybersecurity Training in Norwegian Critical Infrastructure Companies', Int. J. Saf. Secur. Eng., 2022, doi: 10.18280/ijsse.120304.

P. Rosati, F. Gogolin, and T. Lynn, 'Audit Firm Assessments of Cyber-Security Risk: Evidence From Audit Fees and SEC Comment Letters', Int. J. Account., 2019, doi: 10.1142/s1094406019500136.

P. Żebrowski, A. C. Vieira, and A. Mancuso, 'A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber-Physical Systems', Risk Anal., 2022, doi: 10.1111/risa.13900.

R. Kour, R. Karim, and A. Thaduri, 'Cybersecurity for Railways – A Maturity Model',

Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit, 2019, doi: 10.1177/0954409719881849.

R. L. Church, M. P. Scaparra, and R. S. Middleton, ‘Identifying Critical Infrastructure: The Median and Covering Facility Interdiction Problems’, Ann. Assoc. Am. Geogr., 2004, doi: 10.1111/j.1467-8306.2004.00410.x.

R. Messnarz, D. Ekert, G. Macher, A. Much, T. Zehetner, and L. Aschbacher, ‘Experiences With the Automotive SPICE for Cybersecurity Assessment Model and Tools’, J. Softw. Evol. Process, 2022, doi: 10.1002/smr.2519.

R. Shandler, M. L. Gross, S. Backhaus, and D. Canetti, ‘Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment’, Br. J. Polit. Sci., 2021, doi: 10.1017/s0007123420000812.

Ruth Østgaard Skotnes, ‘Standardization of cybersecurity for critical infrastructures’, Nov. 2019, doi: https://doi.org/10.4324/9780429290817-10.

S. Atkins and C. Lawson, ‘An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure’, Public Adm. Rev., 2021, doi: 10.1111/puar.13322.

S. Kumar, ‘The Missing Piece in Human-Centric Approaches to Cybernorms Implementation: The Role of Civil Society’, J. Cyber Policy, 2021, doi: 10.1080/23738871.2021.1909090.

S. Li, T. Tryfonas, and H. Li, ‘The Internet of Things: A Security Point of View’, Internet Res., 2016, doi: 10.1108/intr-07-2014-0173.

T. Bovaird, ‘Public–Private Partnerships: From Contested Concepts to Prevalent Practice’, Int. Rev. Adm. Sci., 2004, doi: 10.1177/0020852304044250.

T. G. Calderon and L. Gao, ‘Cybersecurity Risks Disclosure and Implied Audit Risks: Evidence From Audit Fees’, Int. J. Audit., 2020, doi: 10.1111/ijau.12209.

T. Limba, T. Plėta, K. Agafonov, and M. Damkus, ‘Cyber Security Management Model for Critical Infrastructure’, J. Entrep. Sustain. Issues, 2017, doi: 10.9770/jesi.2017.4.4(12).

T. Wu, J. F. P. Disso, K. Jones, and A. I. Campos, ‘Towards a SCADA Forensics Architecture’, 2013, doi: 10.14236/ewic/icscsr2013.2.

V. D. Savin, ‘Cyber-Security in the New Era of Integrated Operational – Informational Technology Systems’, Bus. Excell. Manag., 2021, doi: 10.24818/beman/2021.11.1-05.

V. Mancuso, A. J. Strang, G. J. Funke, and V. Finomore, ‘Human Factors of Cyber Attacks’, Proc. Hum. Factors Ergon. Soc. Annu. Meet., 2014, doi: 10.1177/1541931214581091.

X. Wang, Y. Han, C. Wang, Q. Zhao, C. Xu, and M. Chen, ‘In-Edge AI: Intelligentizing Mobile Edge Computing, Caching and Communication by Federated Learning’, Ieee Netw., 2019, doi: 10.1109/mnet.2019.1800286.

Z. Masood, M. A. Z. Raja, N. I. Chaudhary, K. M. Cheema, and A. H. Milyani, ‘Fractional Dynamics of Stuxnet Virus Propagation in Industrial Control Systems’, Mathematics, 2021, doi: 10.3390/math9172160.