A utilização de *deepfakes* no domínio jurídico-penal: uma nova realidade?

JOSÉ MARQUES MOREIRA ([1])

RESUMO: Os avanços científicos dos últimos anos no domínio da inteligência artificial, comportaram seguramente vantagens para os seus utilizadores. Contudo, a par desses avanços, verificou-se um crescimento na utilização destes *softwares* para a prática de ilícitos criminais, em particular nas situações de *phishing* e *deepfakes*. Procuramos, neste pequeno ensaio e sem quaisquer pretensões de completude, analisar um desses casos à luz do ordenamento jurídico português, debater as soluções ao dispor do Estado para combater o fenómeno e, a final, refletir sobre a necessidade de efetuar alterações legislativas no contexto jurídico-penal para acompanhar a evolução científica desta tecnologia.

PALAVRAS-CHAVE: inteligência artificial; *deepfakes*; *phishing*; burla; falsificação; CEO; cibercrime.

[1] Doutorando em Direito pela Escola de Direito da Universidade Católica Portuguesa — Centro Regional do Porto. Mestre em Direito (2019) e Licenciado em Direito (2015) pela Escola de Direito da Universidade Católica Portuguesa — Centro Regional do Porto. Advogado Sénior na empresa Continental GmbH, com especialização nas áreas de *Governance* e *Compliance* de Inteligência Artificial na Europa.

1. Contexto e enquadramento legal dos *deepfakes*

§ Nas últimas décadas, os avanços científicos no domínio da inteligência artificial — "**IA**" — têm vindo a revolucionar diversos setores de atividade, oferecendo soluções tecnológicas diversas e transformando as sociedades modernas num mundo mais digital. Pensamos, por hipótese, nos algoritmos de reconhecimento de imagem e de emoções, nos algoritmos desenvolvidos no campo da medicina ([2]), designadamente no diagnóstico e tratamento de determinadas patologias, nos algoritmos utilizados para permitir uma maior eficiência ambiental nas cidades ([3]), outros utilizados no campo da educação, ou até mesmo nas organizações empresariais através de soluções que aumentam a eficácia das tarefas do dia a dia dos profissionais. Estas tecnologias, de uma forma ou de outra, recorrem à IA e a algoritmos de aprendizagem ([4]).

No entanto, esta tecnologia, quando utilizada de forma atípica, comporta certos desafios no domínio do Direito Penal. São exemplos os designados *deepfakes* ([5]), que nada mais são do que criações digitais manipuladas que utilizam IA, especificamente GAN's (*Generative Adversarial Network*), capazes de replicar vozes, rostos, ou movimentos humanos com um elevado grau de realismo. Aproveitando-se da forma astuciosa como um determinado comportamento humano facilmente é mimetizado, os

---

[2] Relativamente à importância da IA no setor da medicina, *cfr*. o relatório da OCDE sobre o uso da IA e possíveis benefícios da sua utilização. No entendimento da OCDE, será possível os prestadores de serviços prestarem cuidados de saúde em tempo real aos pacientes, através de diagnósticos preventivos capazes de detetar anomalias e facilitando uma ação preventiva por parte dos médicos e enfermeiros. *sic* OECD Artificial Intelligence Papers, *Assessing Potential Future Artificial Benefits and Policy Imperatives*, n.º 27, de Novembro 2024, pg. 15.

[3] Veja-se o exemplo do Japão, que tem estado a desenvolver esta tecnologia em algumas das suas cidades. As designadas *smart cities* são modelos estruturados com base em tecnologias de informação e de comunicação, que têm por objetivo promover práticas de desenvolvimento e crescimento sustentável. As *smart cities* assentam numa rede de dispositivos e de infraestruturas inteligadas entre si, capazes de transmitir dados, onde aplicações baseadas em IoT recolhem e analisam esses dados. Desta forma os recursos utilizados são mais racionados e a sua utilização é mais ponderada. *cfr. Japan's Smart Cities, Solving Global Issues such as the SDGs, etc*. Through Japan's Society 5.0, *in* https://www.kantei.go.jp/jp/singi/keikyou/pdf/Japan's_Smart_Cities-1(Main_Report).pdf.

[4] Para uma perspetiva técnica da IA e informação sobre os diversos tipos de algoritmos atualmente existentes, *cfr*. DOMINGOS, Pedro, *A revolução do algoritmo mestre, Como a aprendizagem automática está a mudar o mundo*, 5.ª Edição, Manuscrito, 2017.

[5] Esta tecnologia começou a ser desenvolvida no ano de 2014, tendo a sua utilização sido exponenciada nas áreas do cinema e do entretenimento. A título de exemplo, *cfr*. Rogue One: a Star Wars Story, 2016, quando a personagem Grand Moff Tarkin foi protagonizada pelo ator britânico Peter Cushing, que tinha falecido no ano de 1994.

deepfakes têm vindo a ser utilizados, um pouco por todo o mundo, para a prática de ilícitos criminais.

§ É possível também afirmar que a utilização de *deepfakes* no contexto criminal consubstancia uma forma de *phishing*. Podemos definir este conceito ([6]) como uma técnica enganosa utilizada pelos agentes que praticam o ilícito criminal, para que os lesados forneçam informações confidenciais, ou realizem ações que resultem em prejuízo para si, geralmente por meio de emails, contactos telefónicos (*"vishing"*) ou mensagens falsas (*"smishing"*). Os agentes que praticam o ato enganam os lesados através da criação de uma identidade falsa, socorrendo-se da confiança no presumido interlocutor, para levar a que o lesado realize determinadas ações, que, por via de regra, resultam num prejuízo patrimonial para si ou para terceiros. Enquanto no *phishing* convencional são utilizados texto ou emails fraudulentos, os *deepfakes* utilizam áudio ou vídeo altamente realistas, sintetizando a voz e a imagem, tornando o engano ainda mais convincente.

§ Neste pequeno ensaio pretendemos analisar o contexto jurídico-penal da utilização dos *deepfakes* através de um caso ocorrido numa sucursal no Reino Unido de uma empresa alemã, que determinou um prejuízo patrimonial para a empresa lesada ([7]).

---

[6] Com maior detalhe sobre a definição do conceito de *phishing cfr*. COSTA, Almeida, *A burla no Código Penal Português*, 2020, Almedina, pg. 103. Ainda o acórdão do Tribunal da Relação de Lisboa, proferido no processo n.º 1063/12.1TVLSB.L1-1, de 15 de março de 2016, Relator Juiz Desembargador RIJO FERREIRA, disponível em: https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/9e97f8bfa975299480257f95002b666e?OpenDocument. Por fim "Phishing e Money Mules", Nota Prática do Ministério Público n.º 27/2024, de 20 de novembro de 2024 *in* https://cibercrime.ministeriopublico.pt/sites/default/files/2024-11/2024.11.20-nota-pratica-27-phishing-e-money-mules.pdf.

[7] Sem prejuízo da análise que iremos efetuar a este caso concreto, a verdade é que temos vindo a assistir a uma crescente utilização deste tipo de técnicas criminais elaboradas com recurso à IA. Exemplo disso foi o caso ocorrido em 2024 com a empresa de engenharia ARUP, que foi vítima de um crime de burla após um funcionário, que trabalhava numa sucursal da empresa em Hong Kong, ter sido convencido a enviar 20M£ em virtude da receção de uma videochamada gerada por IA. *sic UK engineering firm Arup falls victim to £20m deepfake scam*, publicado por Dan Milmo *in* The Guardian, maio de 2024 através do link https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video. Outro exemplo semelhante, mas onde não chegou a ocorrer um dano efetivo, ocorreu com a WPP, empresa de publicidade, ao ter sido criada uma conta de WhatsApp com uma imagem do CEO, onde, através dessa conta, foi agendada uma reunião via Microsoft Teams. Nessa reunião estariam presentes o CEO e outro executivo da empresa. Durante a reunião foi implantado um *deepfake* da voz do CEO, onde era solicitada a criação de um novo negócio na tentativa de solicitar dinheiro e dados pessoais de colaboradores da empresa. *cfr*. *CEO of world's biggest ad firm targeted by deepfake scam*, publicado por Nick Robins-Early *in* The Guardian, maio de 2024 através do link https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam. Também os órgãos de Estado têm sido afetados, como foi o caso da Primeira-Ministra tailandesa que recebeu um contacto de outro chefe de governo, a solicitar o envio de fundos visto ser o único país da Associação das Nações do Sudeste Asiático que ainda não o teria feito. *sic Even world leaders receive scam calls. Just ask Thailand's prime minister*, publicado por Jay Ganglani e Kocha Olarn *in* CNN, janeiro de 2025 através do

E, atenta a dinâmica factual, pretendemos apreciar o evento à luz do Direito Penal português, para, em função das conclusões a que chegarmos, contribuir para o estudo do fenómeno e verificar se os meios ao dispor permitem a sociedade combater este tipo de práticas.

2. O *deepfake* criminal — apreciação do caso *sub judice*

2.1 A matéria de facto

§ Em março de 2019, um gestor financeiro de uma empresa (que trabalhava numa subsidiária no Reino Unido) recebeu uma chamada através de um *deepfake* de voz que imitava o CEO da empresa mãe sediada na Alemanha ([8]). Nessa chamada, o alegado CEO solicitava a realização de uma transferência bancária, sensivelmente no montante de €220.000,00, para uma conta bancária na Hungria, alegando tratar-se de um pagamento necessário e urgente a realizar a um fornecedor estratégico. Durante o telefonema foi garantido que o valor seria reembolsado pela empresa mãe à subsidiária no Reino Unido. O gestor financeiro, confiando na genuinidade da chamada e na autenticidade do interlocutor, realizou a transferência para a conta bancária indicada pelo alegado CEO. Após a transferência bancária realizada pelo gestor, o dinheiro foi reenviado para uma conta no México e subsequentemente para outras localizações geográficas. Mais tarde, recorrendo ao mesmo *modus operandi*, o agente infrator tentou convencer novamente o gestor financeiro a realizar uma outra transferência bancária, o que não viria a suceder visto não ter existido reembolso da primeira transferência por parte da empresa mãe para a sucursal britânica. Em virtude da impossibilidade de rastreabilidade do dinheiro e atenta a conduta do agente infrator, a empresa foi lesada num prejuízo patrimonial elevado, mediante a utilização de uma técnica de IA enganosa, vulgo um *deepfake*.

---

link https://edition.cnn.com/2025/01/16/asia/thailand-prime-minister-scam-call-intl-hnk/index.html. Cremos, no entanto, que face à análise que iremos efetuar neste ensaio ao caso concreto, a mesma pode ser replicada *mutatis mutandis* aos demais casos referidos, atenta a similaridade da matéria de facto e da conduta do agente.

[8] Para maior detalhe *cfr. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case*, *Scams using artificial intelligence are a new challenge for companies*, publicado por Catherine Stupp *in* Wall Street Journal, agosto de 2019 através do link https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.

§ Na verdade, o agente infrator terá tido acesso a *samples* públicos da voz do CEO da empresa, através de vídeos partilhados online, o que terá contribuído para o treino do algoritmo subjacente ao *deepfake* e criado a convicção de que se tratava efetivamente da pessoa em questão. Não obstante a factualidade não se ter verificado em Portugal, assume particular relevo analisar este caso de acordo com o quadro normativo jurídico-penal português, visto que, em virtude da tecnologia em crise, é possível que o tecido empresarial português possa vir a ser afetado no futuro com este tipo de condutas. E, nessa medida, as questões que a nosso ver se impõe são: **i)** a conduta do agente preenche o tipo legal de que norma(s)? **ii)** a utilização deste meio de IA enganoso, vulgo *deepfake*, uma vez que se materializa num caso de *phishing*, deverá ser punida? **iii)** a utilização de uma identidade de terceiro determina, por si só, a prática de um ilícito criminal? Vejamos.

2.2 Enquadramento jurídico-penal ao abrigo do Direito Português

§ No n.º 1 do artigo 217.º do Código Penal **— "CP" —** o legislador português determinou que: *"Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, por meio de erro ou engano sobre factos que astuciosamente provocou, determinar outrem à prática de actos que lhe causem, ou causem a outra pessoa, prejuízo patrimonial é punido com pena de prisão até três anos ou com pena de multa."* ([9]). Este ilícito criminal depende de queixa, sendo, portanto, um crime semipúblico e o bem jurídico tutelado pela norma é o *património, globalmente considerado* ([10]).

No que concerne à sua caracterização, podemos afirmar que o ilícito previsto no artigo 217.º é um crime de dano, na medida em que pressupõe um prejuízo patrimonial para o sujeito passivo, um crime de forma vinculada, uma vez que o legislador descreveu de forma detalhada o modo da sua consumação e é um crime de resultado, uma vez que se consuma com a saída do bem da esfera jurídica do sujeito passivo ([11]-[12]).

---

[9] Sobre o conceito de engano astucioso previsto pelo legislador português no artigo 217.º do CP, *cfr*. COSTA ANDRADE, Tiago, *O Crime de Burla, Bem Jurídico e Imputação Objetiva*, Almedina, 2019, pgs. 61 e seguintes.

[10] *sic* COSTA, Almeida, *Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, artigos 202.º a 307.º*, dirigido por Jorge de Figueiredo Dias, Coimbra Editora, anotação ao artigo 217.º do Código Penal, pg. 275.

[11] *cfr.* acórdão do Tribunal da Relação de Lisboa, proferido no processo n.º 430/07.7JDLSB-A.L2-9, de 03 de setembro de 2013, Relator Juiz Desembargador TRIGO MESQUITA, disponível em: https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/876588deba66185180257be20038ecb5?OpenDocument.

[12] *sic* COSTA, Almeida, *Comentário Conimbricense do Código Penal op. cit.* pgs. 276 e 277.

Socorrendo-nos das palavras de ALMEIDA COSTA ([13]), *"**A burla recobre situações em que o agente**, com a intenção de conseguir enriquecimento ilegítimo (próprio ou alheio), **induz outra pessoa em erro, fazendo com que a última, por esse motivo, pratique actos que causam a si mesma (ou a terceiro), prejuízos de caracter patrimonial**."*. Podemos, portanto, afirmar, nas palavras do autor, que *"*[A] *burla integra um delito de execução vinculada, em que a lesão do bem jurídico tem de ocorrer como consequência de uma muito particular forma de comportamento. Traduz-se ela na **utilização de um meio enganoso tendente a induzir outra pessoa** n**m erro que, por seu turno, a leva a praticar actos de que resultam prejuízos patrimoniais** próprios ou alheios."* (negrito nosso).

Analisando de perto a jurisprudência nacional, ainda no que concerne ainda à caracterização do ilícito, verificamos que o Tribunal da Relação do Porto, manifestado no processo n.º 1314/09.0PAVNG.P1, de 11 de dezembro de 2013, Relator Juíza Desembargadora MARIA MANUELA PAUPÉRIO ([14]) reconheceu que *"*[...] *Os elementos que preenchem e enformam a tipicidade do crime de burla são; **o uso de erro ou engano sobre factos, astuciosamente provocados** (1) para **determinar outrem à prática de actos que lhe causem**, ou a terceiro, **prejuízo patrimonial**, (2) **com intenção de obter para o agente ou para terceiro um enriquecimento ilegítimo** (3)"* (negrito nosso).

§ Ora, na conduta descrita no subcapítulo que antecede verificamos que: **i)** o agente tinha a intenção de obter para si — ou para terceiro, desconhecemos — um enriquecimento ilegítimo, **ii)** foi utilizado um engano sobre factos que astuciosamente provocou, através do treino e utilização do *deepfake* da voz do CEO, e que **iii)** o agente determinou ao gestor financeiro a prática de atos que causaram um prejuízo patrimonial à empresa. Atenta a factualidade descrita, cremos que podemos afirmar que a previsão normativa, *maxime* o tipo objetivo do ilícito criminal do crime de burla, se encontra preenchido.

No entanto, atento o montante do prejuízo patrimonial causado à empresa lesada, sensivelmente €220.000,00 o tipo de ilícito em causa sofre um agravamento. Isto porque

---

[13] *sic* COSTA, Almeida, *Comentário Conimbricense do Código Penal op. cit.* pg. 275.
[14] *sic* acórdão do Tribunal da Relação do Porto, proferido no processo n.º 1314/09.0PAVNG.P1, datado de 11 de dezembro de 2013, Relator Juíza Desembargadora MARIA MANUELA PAUPÉRIO, disponível em: https://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/b5fb581c97643f0180257c590050c0b4?OpenDocument.

nos termos da alínea a) do n.º 2 do artigo 218.º, conjugada com o artigo 202.º, ambos do CP, se trata de um prejuízo patrimonial de *"valor consideravelmente elevado"* e, por força disso mesmo, o agente seria punido com uma pena de prisão agravada de 2 a 8 anos. Em suma, no caso concreto estas duas normas — arts. 217.º e 218.º do CP — deverão ser conjugadas por forma a compor o quadro normativo aplicável ao agente.

§ Como tal, no nosso entendimento, a utilização de *deepfakes* poderá ser enquadrada nos artigos 217.º e 218.º do CP — este último artigo para os casos previstos na norma —, nos casos em que a utilização da tecnologia é meramente uma ferramenta concretizadora do dano, conquanto que estejam reunidos os demais requisitos do tipo, o que, na nossa opinião, parece ser o caso. Nessa medida, encontram-se preenchidos os elementos do tipo objetivo do crime de burla qualificada, pelo que, caso a factualidade se tivesse verificado em Portugal, esta solução normativa seria perfeitamente justificada perante a conduta descrita.

Por fim, resulta da factualidade que o agente infrator, num momento posterior, tentou convencer o gestor financeiro a realizar uma nova transferência. Nessa medida, cremos que esta conduta poderá ser enquadrada no n.º 2 do artigo 217.º do CP, no que concerne, nomeadamente, à tentativa da prática de um novo ilícito. E assim, a acrescer à consumação ocorrida num primeiro momento, deverá ser englobada a tentativa do agente no momento posterior, para efeitos de subsunção dos factos à conduta jurídico-penal do agente.

2.3 Outros potenciais ilícitos em crise

§ A análise de outros tipos de ilícitos criminais que nos permitam enquadrar a situação fáctica reveste particular relevância neste ensaio, visto que, podendo a conduta ser preenchida em mais do que uma norma, é possível estarmos perante um concurso de crimes. Nessa medida, decidimos analisar a conduta do agente à luz de três tipos de ilícito, visto se tratarem daqueles que, a nosso ver, poderão ter uma maior conexão com o caso concreto: **i)** o disposto no artigo 221.º do CP respeitante ao crime de Burla Informática e nas Comunicações, **ii)** o disposto no artigo 225.º do CP respeitante ao crime de Abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, bem como **iii)** o crime

de Falsidade Informática p. e p. *ex vi* art. 3.º da Lei n.º 109/2009, de 15 de Setembro — **"Lei do Cibercrime" —**.

§ No que respeita ao crime de Burla Informática e nas Comunicações, o legislador português definiu no artigo 221.º do CP que *"Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, mediante interferência no resultado de tratamento de dados, 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."*. Ora, quanto à sua caracterização, este é também um crime semipúblico, uma vez que depende de queixa — n.º 4 do artigo 221.º —, integra um crime de dano, de execução vinculada porquanto a lesão do património do lesado se materializa através da intromissão nos sistemas e da utilização de certos meios informáticos, bem como é um crime de resultado, exigindo que seja produzido um prejuízo patrimonial no património do lesado ([15]-[16]). O bem jurídico protegido pela norma é essencialmente o património ([17]).

A burla informática consiste num comportamento que se materializa num engano consciente, mediante a manipulação de um sistema de dados ou de aplicações informáticas, ou utilização abusiva de dados. Dito de outro modo, para que o tipo legal esteja preenchido, o agente deverá praticar atos tendentes a enganar o sistema informático que, por sua vez, será utilizado para provocar o evento lesivo na esfera do lesado — contrariamente ao que sucede no crime de burla, onde o erro, ou o engano, operam por afetação direta no lesado —.

---

[15] *cfr.* COSTA, Almeida, *Comentário Conimbricense do Código Penal op. cit.* pg. 329; *cfr*. COSTA, Almeida, *A burla no Código Penal Português*, *op. cit.*, pg. 96.

[16] *cfr*. acórdão do Tribunal da Relação de Évora, proferido no processo n.º 264/06.6GBPSR.E1, de 26 de junho de 2012, Relator Juiz Desembargador MARTINHO CARDOSO, disponível em: https://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/9e4d23e33c93144580257de10056f883?OpenDocument.

[17] *cfr.* COSTA, Almeida, *Comentário Conimbricense do Código Penal op. cit.* pg. 329.

São exemplos deste tipo de ilícito as burlas levadas a cabo através do sistema informático MB WAY ([18]), ou, *no passado*, a utilização de cartões bancários nos sistemas informáticos ATM sem a devida autorização do seu titular ([19]-[20]).

Contudo, é importante dar nota que se afigura uma diferença essencial do tipo objetivo previsto no artigo 221.º em comparação com o tipo previsto no artigo 217.º. Invocando as palavras de ALMEIDA COSTA ([21])*"No que concerne ao aspecto a que vem de aludir-se, a infracção do n.º 1 do art. 221.º assume uma estrutura diversa do delito fundamental de burla do art. 217.º. Como se assinalou, neste último o agente cria no sujeito passivo um estado de erro que o leva à prática de actos de diminuição patrimonial (própria ou alheia), deparando-se com um iter criminis que comporta, nos termos expostos, um duplo nexo de imputação objectiva. Ao invés, a denominada "burla informática" concretiza-se num* ***atentado directo ao património****, i. e.,* ***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****."* (sublinhado nosso). Ou seja, na hipótese prevista no art. 221.º, o dano patrimonial produz-se através da interferência direta no sistema

---

[18] A título de exemplo *cfr*. acórdão do Tribunal da Relação de Coimbra, proferido no processo n.º 84/20.5GBPMS.C1, datado de 24 de maio de 2023, Relator Juiz Desembargador PAULO GUERRA, disponível em: https://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/7a1946bd59cc69cd802589c9003fdf28?OpenDocument.

[19] *cfr*. acórdão do Tribunal da Relação de Évora, proferido no processo n.º 264/06.6GBPSR.E1, datado de 26 de junho de 2012, Relator Juiz Desembargador MARTINHO CARDOSO, disponível em: https://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/9e4d23e33c93144580257de10056f883?OpenDocument; acórdão do Tribunal da Relação de Évora, proferido no processo n.º 90/11.0GCLLE.E1, de 20 de janeiro de 2015, Relator Juiz Desembargador JOÃO AMARO, disponível em: https://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/737b074e63612dc880257de100582533?OpenDocument; acórdão do Tribunal da Relação de Évora, proferido no processo n.º 133/13.3GBODM.E1, de 19 de novembro de 2015, Relator Juiz Desembargador CARLOS JORGE BERGUETE, disponível em: https://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/1f4d4f4321f0a37580257f23003f6522?OpenDocument; acórdão do Tribunal da Relação do Porto, proferido no processo n.º 676/08.0GBFLG.P1, datado de 05 de junho de 2013, Relator Juiz Desembargador JOAQUIM GOMES, disponível em: https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/60a14d338f50f74880257b8f003bd8de?OpenDocument; acórdão do Tribunal da Relação de Guimarães, proferido no processo n.º 541/10.GAPTB.G1, datado de 18 de dezembro de 2012, Relator Juíza Desembargadora ANA TEIXEIRA, disponível em: https://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/e6bae9c7ac50111d80257af3004e537d?OpenDocument.

[20] Aos dias de hoje, a utilização de cartões bancários sem autorização é punida nos termos do disposto no artigo 225.º do CP conforme veremos adiante, atenta a alteração legislativa levada a cabo em 2021, mais concretamente com a transposição da Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário.

[21] *cfr.* COSTA, Almeida, *Comentário Conimbricense do Código Penal op. cit.* pg. 330.

informático, não sendo necessário que o sujeito passivo seja colocado em estado de erro nos termos previstos no art. 217.º. E, nessa medida, o tipo objetivo não comporta o *"duplo nexo de imputação objetiva"* conforme referido pelo autor.

§ Cremos, portanto, que a conduta do agente não preenche o tipo legal previsto no artigo 221.º do CP, uma vez que o agente não manipulou, ou praticou um erro, mediante a interferência direta no sistema informático, tendo em vista enganar o lesado. Neste caso foi utilizado, de forma lícita, um determinado *software* (*deepfake*), tendo em vista a prática de atos ilícitos (*phishing*) através desse mesmo programa informático. Nessa medida, cremos que o tipo legal aqui em análise não será o mais adequado para enquadrar a conduta tipo na previsão jurídico-penal.

§ Já no que concerne ao tipo objetivo previsto no artigo 225.º do CP, este foi alterado em 2021 em virtude da transposição da Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário. Nessa medida, o legislador passou a prever no n.º 1 do artigo em análise que *"Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, usar: a) Cartão de garantia; b) Cartão de pagamento; c) Qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou a meio de pagamento; d) Dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou a meio de pagamento; determinando o depósito, a transferência, o levantamento ou, por qualquer outra forma, o pagamento de moeda, incluindo a escritural, a eletrónica ou a virtual, e causar, desse modo, prejuízo patrimonial a outra pessoa, é punido com pena de prisão até 3 anos ou com pena de multa."*. Em virtude da alteração legislativa, passa agora a prever-se, por exemplo, que as condutas típicas relativas ao uso fraudulento de dados de cartões bancários de pagamento — que antes eram punidas pelo artigo 3.º da Lei do Cibercrime, e pelo artigo 221.º, n.º 1, do CP — passam a estar unificadas no tipo de crime previsto na alínea d) do n.º 1 do artigo 225.º do CP ([22]). De outra banda, por via da alteração legislativa passou a

[22] Neste sentido *cfr*. acórdão do Tribunal da Relação de Guimarães, proferido no processo n.º 625/20.8PCBRG.G1, de 14 de novembro de 2023, Relator Juiz Desembargador BRÁULIO MARTINS e disponível em: https://www.dgsi.pt/jtrg.nsf/c3fb530030ea1c61802568d9005cd5bb/133758bb63c0816080258a77004e1b43;

incluir-se neste tipo de crimes, todo o uso abusivo — além de cartões — de dispositivos e meios de pagamento, que não em numerário e ainda o uso abusivo de dados — autênticos — de cartões de pagamento, quando não esteja em causa a presença física do cartão. Passam, portanto, a punir-se nos termos do artigo 225.º do Código Penal todos os comportamentos ilícitos relacionados com o uso abusivo de cartões de pagamento de todas as naturezas ([23]).

O intuito do quadro normativo previsto no artigo 225.º é o de concentrar no CP a punição do abuso de cartões de pagamento autênticos. Será, designadamente, o caso de um cartão utilizado de forma ilegítima pelo agente infrator, por exemplo, presencialmente num estabelecimento comercial. Mas também será o caso da utilização abusiva e não autorizada dos dados do cartão, por exemplo, em compras à distância com recurso à internet. O abuso de cartão, ou de outros meios de pagamento, é um mero uso de algo autêntico, mas não autorizado pelo seu titular, ou ilegítimo ([24]).

§ Atento o quadro normativo em questão, não se nos afigura possível enquadrar a conduta do agente na previsão normativa deste novo artigo 225.º do CP, uma vez que o agente não acedeu a qualquer sistema de pagamento do lesado de forma fraudulenta ou enganosa, nem tampouco utilizou dados ou dispositivos corpóreos ou incorpóreos, para aceder ao sistema ou meio de pagamento. O engano provocado pelo agente infrator manifestou-se na relação direta entre o alegado CEO, *maxime* o interlocutor, e o gestor financeiro, *maxime* destinatário, tendo este último, de forma perfeitamente legítima e lícita, efetuado uma transferência bancária e, com isso, provocado o evento lesivo. Como tal, não nos parece que a norma em estudo possa ser enquadrada na conduta tipo do agente.

§ Por fim, no que respeita ao crime de Falsificação, previsto no artigo 3.º da Lei do Cibercrime, o legislador determinou que *"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*

[23] *sic* Abuso e Contrafação de cartões e outros dispositivos de pagamento, Nota Prática do Ministério Público n.º 24/2021, de 13 de dezembro de 2021 *in* https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_24_novos_crimes_na_lei_cibercrime_2.pdf, pg. 5.
[24] *sic* Abuso e Contrafação de cartões e outros dispositivos de pagamento *op. cit.* pg. 6.

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.". Já no art. 2.º definiu dados informáticos como "[q]*ualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função.".* No que concerne à sua caracterização, trata-se de um crime público e o bem jurídico tutelado pela norma é a a *integridade dos sistemas de informação*, *através da qual se pretende impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas de redes e dados* ([25]). Nas palavras de PEDRO DIAS VENÂNCIO, é *"*[u]*m crime que visa proteger a segurança das relações jurídicas enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar."* ([26]).

São exemplos da conduta tipo prevista na norma, os casos em que **i)** é criada uma conta de perfil não genuína numa plataforma informática (*e.g. Facebook*) , através da utilização dos seus dados pessoais, onde, simulando ser o legítimo titular dos dados, são introduzidas informações que não correspondem à realidade, são divulgadas informações de cariz íntimo da vida pessoal, provocando engano e causando prejuízo à honra e à imagem da pessoa ([27]), ou **ii)** a introdução num sistema informático de dados falsos, como a realização de cirurgias num sistema informático de um hospital, realizadas em regime de ambulatório como se tivessem sido levadas a cabo em regime de internamento ([28]).

§ Ora, efetuando a exegese normativa do artigo 3.º, verificamos que, sem prejuízo de se verificarem os requisitos do engano nas relações jurídicas e da interferência no tratamento informático dos dados, a verdade é que temos dúvidas em afirmar que, atenta

---

[25] *cfr*. acórdão do Tribunal da Relação de Lisboa, proferido no processo n.º 189/09.3JASTB.L1-5, datado de 30 de junho de 2011, Relator Juíza Desembargadora FILOMENA LIMA, disponível em: https://diariodarepublica.pt/dr/detalhe/acordao/189-2011-98772075; ainda uma decisão mais recente proferida no acórdão do Tribunal da Relação de Coimbra, proferido no processo n.º 1158/19.0T9CTB.C1, datado de 11 de outubro de 2023, Relator Juíza Desembargadora ALEXANDRA GUINÉ, disponível em: https://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/72f384c9c2f6cfe880258a5200320bcc?OpenDocument.

[26] *sic* VENÂNCIO, Pedro Dias, *Lei do Cibercrime anotada e comentada,* Coimbra Editora, pg. 38.

[27] *cfr*. acórdão do Tribunal da Relação do Porto, proferido no processo n.º 585/11.6PAOVR.P1, datado de 24 de abril de 2013, Relator Juíza Desembargadora FÁTIMA FURTADO, disponível em: https://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/872f3063233d8de480257b78003e60f3?OpenDocument.

[28] *cfr*. acórdão do Tribunal da Relação do Porto, proferido no processo n.º 35/07.2JACBR.P1, datado de 26 de maio de 2015, Relator Juíza Desembargadora MARIA LUÍSA ARANTES, disponível em: https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/aa9d0fb297dcca7880257e62003a86e4?OpenDocument.

a conduta do agente infrator, se tenham produzido dados ou quaisquer documentos, com a intenção de que estes fossem considerados para finalidades juridicamente relevantes. Isto porque, a conduta do agente em apreciação no presente ensaio, não revelou a criação de qualquer conteúdo, dado informático ou documento, capaz de promover o engano no sujeito passivo ([29]). O agente apenas terá treinado o algoritmo com dados do seu verdadeiro titular, como a voz, o sotaque e até maneirismos, através de vídeos do CEO que se encontravam no domínio público, e gizado um plano para entrar em contacto com o gestor financeiro da empresa e convencê-lo a realizar uma transferência bancária. Ou seja, o único conteúdo gerado foi o *deepfake*, que, conforme veremos, não integra, por si só, a prática de qualquer ilícito criminal. Como tal, ao não ter sido gerado qualquer documento, ou dado, não genuíno, temos dúvidas de que esta norma possa ter aplicação no caso *sub judice*.

2.4 A utilização do meio enganoso *deepfake* e a sua (falta de) punição

§ Podemos desde já aventar que a utilização do *deepfake*, por si só, não consubstancia a prática de qualquer ilícito criminal. Pelo contrário. Tecnicamente um *deepfake* é um algoritmo de IA caracterizado como um *"General Purpose AI"*, previsto no Regulamento (UE) n.º 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial (designado por Regulamento de Inteligência Artificial — "**AIA**" —), mais precisamente nos artigos 50.º e seguintes do AIA. E, nessa medida, a intenção do legislador Europeu foi a de regular a matéria da transparência deste tipo de sistemas de IA ([30]), tendo, para

---

[29] Requisito esse necessário para o preenchimento da *factispécie* normativa, conforme resulta do acórdão proferido pelo Tribunal da Relação de Évora, no processo n.º 238/12.8PBPTG.E1, de 19 de maio de 2015, relator Juiz Desembargador ANTÓNIO LATAS, onde no aresto se escreve que *"*[O] *tipo objetivo do crime de falsidade informática previsto no n.º 1 do artigo 3.º da Lei nº 109/2009, de 15 de setembro, é integrado, no plano objetivo, pela introdução, modificação, apagamento ou supressão de dados informáticos ou por qualquer outra forma de interferência num tratamento informático de dados, de que resulte a produção de dados ou documentos não genuínos, consumando-se o crime apenas com a produção deste resultado."*.

[30] No que concerne à matéria da transparência dos sistemas e modelos de IA, *cfr*. os considerandos do AIA quando o legislador manifesta que *"Além disso, presente regulamento visa ainda reforçar a eficácia desses direitos e vias de recurso existentes,* ***estabelecendo requisitos e obrigações específicos, nomeadamente no que diz respeito à transparência****, à documentação técnica e à manutenção de registos dos sistemas de IA. [...] Como tal, é necessário proibir determinadas práticas inaceitáveis de IA, estabelecer requisitos aplicáveis aos sistemas de IA de risco elevado e obrigações para os operadores pertinentes, bem como* ***estabelecer obrigações de transparência para determinados sistemas de IA.*** *[...] A transparência significa que os sistemas de IA são desenvolvidos e utilizados de forma a permitir uma rastreabilidade e explicabilidade adequadas,* ***sensibilizando ao mesmo tempo os seres humanos para o facto de estarem a comunicar ou a interagir com um sistema de IA****, informando devidamente os responsáveis pela*

este tipo de casos de *General Purpose AI*, criado o Anexo XII do AIA, que versa precisamente sobre as *"Informações em matéria de transparência a que se refere o artigo 53.º, n.º 1, alínea b) — documentação técnica para os prestadores de modelos de IA de finalidade geral destinada aos prestadores a jusante que integrem o modelo no seu sistema de IA"*. Mais, estabeleceu no artigo 50.º que *"Os prestadores devem assegurar que os sistemas de IA destinados a interagir diretamente com pessoas singulares sejam concebidos e desenvolvidos* ***de maneira que as pessoas singulares em causa sejam informadas de que estão a interagir com um sistema de IA****, salvo se tal for óbvio do ponto de vista de uma pessoa singular razoavelmente informada, atenta e advertida, tendo em conta as circunstâncias e o contexto de utilização."* (sublinhado nosso). Ou seja, a utilização do *deepfake de per si* não consubstancia qualquer prática criminal. O que dá corpo a essa prática é o engano sobre os factos provocados de forma astuciosa pelo agente, que, no caso em apreciação, recorreu a um sistema informático e a dados pessoais de uma determinada pessoa (CEO da empresa) para mimetizar um determinado comportamento e sintetizar a sua voz. Efetuando uma pequena comparação, é o mesmo que sucede, por exemplo, quando é necessário distinguir os delitos em que o sistema informático constitui o simples meio através do qual o agente infrator atenta contra os bens jurídicos — o que nos parece ser o caso *sub judice* —, dos crimes informáticos em sentido estrito, que envolvem uma ofensa aos sistemas informáticos em si mesmo considerados ([31]). Como tal, podemos afirmar que esta técnica informática não merece qualquer reparo na dogmática jurídico-penal, sendo matéria de regulação por parte do legislador no que concerne à sua disponibilização ao público e utilização, podendo, naturalmente, ser utilizada nos termos previstos no AIA e respeitando a demais legislação nacional.

2.5 A utilização de identidade de terceiro e o ilícito criminal

§ Finalmente, o último ponto do nosso ensaio será aferir se ao ter sido utilizada uma identidade falsa de um terceiro na prática de um ilícito criminal, deverá este comportamento, também ele, consubstanciar a prática de um crime. Dito de outro modo,

implantação das capacidades e limitações desse sistema de IA e informando as pessoas afetadas dos direitos que lhes assistem".

[31] Distinção efetuada por COSTA, Almeida, *A burla no Código Penal Português*, *op. cit.*, pg. 97.

consubstancia a prática de algum ilícito criminal autónomo — *e.g.* falsificação de identidade — a utilização da identidade de um terceiro, para a prática de um outro ilícito?

Temos reservas em enquadrar esta questão, grosso modo, na falsificação de identidade. Em primeiro lugar porque, conforme acabamos de referir no subcapítulo anterior, a criação de *deepfakes* não é ilícita. E não esquecendo o facto de um *deepfake* se materializar na mimetização de um comportamento humano com elevado grau de realismo, o mesmo será dizer que, aos dias de hoje e salvo o devido respeito por melhor opinião, será possível efetuar este tipo de conteúdos, desde que em cumprimento das regras de transparência previstas no AIA (artigo 50.º e seguintes e anexo XII) e na legislação nacional (*e.g.* artigo 26.º, n.º 1 da Constituição da República Portuguesa no que concerne ao direito à imagem, à palavra, à reserva da intimidade da vida privada, etc., ou o artigo 80.º do Código Civil sobre o direito à reserva sobre a intimidade da vida privada). Em segundo lugar, em virtude da própria factualidade no caso *sub judice*. Recordemos que não foi gravado e replicado um determinado conteúdo, videograma ou fonograma, de uma qualquer pessoa sem a sua autorização. Foram apenas utilizados *samples* públicos de um terceiro (CEO da empresa), obtidos licitamente, para treinar um determinado algoritmo capaz de mimetizar a sua voz, sotaque e maneirismos com um elevado grau de realismo. E com o auxílio desse *deepfake*, capaz de gerar conteúdos de voz inexistentes e palavras que o lesado não proferiu, foi praticado o ilícito. Ou seja, não se tratou de uma gravação de videograma ou fonograma não autorizada, da publicação de uma imagem sem autorização ([32]), de uma descontextualização de uma gravação pré-existente, ou de manipulação de conteúdo já existente para astuciosamente levar o sujeito passivo a crer que eram verídicas tais palavras. Tratou-se sim de treino de um algoritmo com dados públicos pré-existentes, capaz de gerar conteúdo totalmente novo e original com a aparência de ter sido o seu verdadeiro titular a proferir tais alegações. O mesmo será dizer, pois, que temos dúvidas que a conduta do agente infrator se possa enquadrar nos termos previstos nos artigos 192.º e 199.º do CP ([33]). Questão diferente era, por exemplo, se além de replicar a voz e a imagem do terceiro, replicasse, por exemplo, a sua assinatura num

[32] *cfr*. acórdão do Tribunal da Relação de Évora, proferido no processo n.º 1802/20.7GBABF.E1, datado de 09 de maio de 2023, Relator Juíza Desembargadora MARIA CLARA FIGUEIREDO, disponível em: https://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/674fcb870e4f1ccc802589b9002e2f73?OpenDocument, onde se refere que o arguido após ter tirado fotografias a um terceiro as publicou na rede social *Facebook* sem a autorização do seu titular.

[33] *sic* COSTA, Almeida, *Comentário Conimbricense do Código Penal, Parte Especial, Tomo I, artigos 131.º a 201.º*, dirigido por Jorge de Figueiredo Dias, Coimbra Editora, anotações aos artigos 192.º e 199.º do Código Penal, pgs. 1039 e 1185 e seguintes.

documento. Aí, naturalmente estaria em causa a conduta prevista no artigo 256.º e seguintes do CP. Mas esse não foi o caso. Isto é, para enquadrar a conduta do agente nas hipóteses legais *supra* referidas, a conduta do agente deverá ela própria materializar-se nas previsões normativas lá estabelecidas. E foi precisamente em virtude da ausência de previsão normativa, que países como o Reino Unido ([34]) e a Coreia do Sul ([35]), pretendem agora criminalizar a criação e disseminação de determinados *deepfakes* de cariz íntimo ou pornográfico.

Em suma, excetuando nos casos em que a conduta do agente integra as previsões normativas, por exemplo, dos artigos 192.º, 199.º e 256.º e seguintes do CP, tendemos a crer que, por si só, será difícil aos dias de hoje punir a conduta do agente como um crime autónomo de falsificação de identidade.

Em terceiro e último lugar, porque a obtenção dos dados para treino do algoritmo, *i.e.* dos *samples* públicos de entrevistas do CEO, não foram obtidos de forma ilícita, nomeadamente nos termos dos artigos 192.º e 199.º do CP. Ou seja, a obtenção destes dados foi efetuada de uma forma legítima, dados esses que foram sim utilizados para uma finalidade ilícita. Nessa medida e atenta a licitude na obtenção deste conteúdo digital, também nos parece não podermos enquadrar esta matéria no domínio da falsificação da identidade.

3. Considerandos conclusivos

§ Chegados aqui, parece-nos que os avanços da IA comportam novos desafios à dogmática jurídico-penal, atenta a utilização da tecnologia para a prática de ilícitos criminais. Apesar de algumas dessas práticas serem perfeitamente enquadráveis em tipos de crime já existentes nos diversos ordenamentos jurídicos, entre os quais o português, casos há em que poderá ocorrer um agravamento na criminalização de determinadas condutas de tipos de crime já existentes — atentos os casos em que se verifica uma massificação da conduta tipo —, ou então a criação de tipos legais autónomos que reprovem determinados comportamentos conexos com a manipulação de dados. Cremos, no entanto, que o ónus da adoção de medidas combativas do fenómeno não se deverá

[34] *cfr*. *Britain to make sexually explicit 'deepfakes' a crime*, publicado por Catarina Demony *in* Reuters, janeiro de 2025 através do link https://www.reuters.com/world/uk/britain-make-sexually-explicit-deepfakes-crime-2025-01-07/?utm_source=chatgpt.com.
[35] *cfr*. *South Korea faces deepfake porn 'emergency'*, publicado por Jean Mackenzie e Nick Marsh *in* BBC, agosto de 2024 através do link https://www.bbc.com/news/articles/cg4yerrg451o.

subsumir apenas ao Estado, mas também à sociedade civil. Em primeiro lugar, no domínio empresarial, parece-nos que, em decorrência da evolução tecnológica, as empresas deverão reforçar os seus procedimentos internos de *risk management, governance, cibersecurity*, etc. Seguramente que a existência de uma política interna, definidora dos métodos e requisitos de transferência de fundos entre empresas do mesmo grupo, teria evitado o evento lesivo no caso concreto aqui em discussão. Em segundo lugar, no que toca a medidas preventivas, será importante a criação de programas de educação e literacia digital, por forma a ensinar o cidadão comum a identificar um *deepfake* e a evitar a sua partilha, bem como programas de literacia digital nas escolas sobre a verificação de factos e a identificação da manipulação digital. Por último, deverá ser repensada uma eventual responsabilização das plataformas digitais capazes de criar e disseminar este tipo de conteúdos, nomeadamente definindo políticas de gestão de autenticidade, marcas de água ou até *disclaimers* identificando que o conteúdo foi gerado através de IA.