CYBERLAW

by CIJIC

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente.***

CYBERLAW

by CIJIC

EDIÇÃO N.º X – SETEMBRO DE 2020

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

NOTAS DO EDITOR:

Os últimos tempos, assim e porque não os vindouros, sobressaltam-nos com três complexidades *esdrúxulas*: acesso universal e aberto à Rede e democratização desta; capacitação humana numa era de diluvio informacional; a relação da tecnologia, do digital, ao serviço das organizações e/ou Estado com a pessoa humana.

É inegável que o acesso à Rede é um direito fundamental da pessoa humana. Da mesma forma que a liberdade, a inclusão e democratização do espaço físico possibilitou uma dinamização de valor acrescentado ao elevador social, é já hoje mais do que óbvio, que a inclusão digital trará idênticos efeitos. Quantas mais pessoas acederem à Rede, melhor. E tudo gira em torno de uma característica universal da pessoa humana: o ser social que somos. É, pois, essencial determinarmos, enquanto ente coletivo, a necessidade da prossecução, por via da pólis, de um acesso universal e aberto à Rede. É tema de agenda política.

Preocupam-nos, com efeito, as questões supranacionais que envolvem, desde logo o 5G. O tabuleiro político mundial, neste momento, está partido ao meio. E tal como Harari referiu – ainda que a propósito do combate à pandemia -, é imperioso que saibamos "*criar princípios éticos globais e restaurar a cooperação internacional* (…).". Obviamente, tudo se resume às escolhas que fizermos, *Ie, "(…) Depende das escolhas que fazemos no presente. Os países podem optar por competir por recursos escassos e prosseguir uma política egoísta e*

isolacionista, ou podem escolher ajudarem-se mutuamente através de um espírito de solidariedade global."[1].

Assim, nem *a great firewall* chinesa, uma agenda económica protecionista e isolacionista, ou a pressão e separatismo estaduais servem a humanidade. Não será sobre esta toada *belicista* que a humanidade produzirá ganhos conjuntos. Se é que os almeja produzir. O espírito de solidariedade internacional tem-se perdido na espuma dos dias.

Curiosamente, na era de dilúvio informacional, parece-nos comprometida a capacitação humana. Severa, a incompreensão de que a pessoa humana não pode ser um objeto. Sendo-o, emerge do *trade-off* entre o acesso a um serviço "*free*" e a quantidade de dados pessoais que liberta, não só para lhe aceder como depois no usufruir desse serviço.

Zuboff[2] alerta-nos para o *direct and personal targeting*, um assombro de *direct emotional manipulation* , em que sobressai o modelo de negócio das *big tech trendy* de sempre: o parcelamento informacional da pessoa, vendido a outras corporações como ponto de dados; métricas, perfis, com o intuito de retornar (ao titular dos dados) sob a forma de bem ou comodidade (que julga querer adquirir). Qual rato de laboratório. Uma pirâmide financeira suportada à conta da pessoa titular dos dados pessoais, por esta e para esta.

O resultado concreto, analítico, sob a forma de capitalização bolsista, demonstra-nos que a era da informação, na verdade, não está a funcionar para as massas. Pelo contrário. Erige-se num paradoxo: empobrece as suas (nossas) vidas, quer pelos dados pessoais que *capta* quer pelos bens/comodidades que impinge, e enriquece o pecúlio dos (*famosos*) 1%. A robustez financeira acumulada por tais 1%, por sua vez, demonstra uma capacidade, por si só, de manipulação de pilares fundamentais dos estados de direito democrático: a capacidade para atingir diretamente o núcleo legislativo internacional. Com acesso a leis-fato (à medida), só o Direito poderá colocar travão a esta distopia.

Infelizmente, a erosão, de direitos fundamentais humanos, não fica sustida apenas no aspeto mercantil em que opera a redução da pessoa humana a uma objetificação pronunciada. Intrometida e diligentemente, o próprio Estado passou a focar a pessoa como um "*asset*", como um meio, rasgando os pilares fundacionais de toda a doutrina kantiana.

---

1 Harari @ https://en.unesco.org/courier/2020-3/yuval-noah-harari-every-crisis-also-opportunity (ultimo acesso setembro 2020).
2 *The age of surveillance capitalism: the fight for a human future at the new Frontier of power*.

A observação da realidade presente, ainda comprometida pela atualidade da pandemia, não olvida que, à semelhança do *surveillance capitalism*, aqui converge a dualidade relacional humano/tecnologia (digital). Se o Estado se comporta como um ente egoísta, usando as pessoas como mero valor, ponto de dados, métrica ou perfil, miríade informacional para prosseguir determinadas agendas (quais?), o que o distinguirá das organizações privadas que procuram o lucro por todos e quaisquer meios?

Note-se, por exemplo, no caso de Portugal – sendo que é uma prática participada por uma maioria de países democráticos deveras preocupante –, o "estado de vigilância" começa, geralmente, como demonstrando ter um propósito justificado por um "*objetivo*" publicamente aceitável. Daqui deriva para uma moção rotineira, *ie*, uma vez implementado – mesmo que *"a título experimental*" –, passa a fazer parte da rotina diária de todos os cidadãos, planeado e executado de acordo com um cronograma racional, não aleatório, seguindo diretrizes perfeitamente concretas, focado em detalhes, como agregação e armazenamento de *dados*[3].

A justificação, para esta aceitação passiva e obediente, por parte do cidadão, reduz-se a uma vacuidade: "*eu não tenho nada a esconder*…". Contudo, o *estado de vigilância* (à semelhança do homónimo capitalismo) serve quem? O quê? Para quê?

Aquiesçamos, um *estado de vigilância* é um que contempla a vigilância como a solução para a esmagadora maioria das questões sociais complexas. Um *estado de vigilância* é respaldo da incompetência, manifestação de uma viciação por tecnologias (criadas por quem?) e dados (para quê? para quem?), com as limitações aí inerentes.

Tal como na problemática do *surveillance capitalism*, o *estado de vigilância* aparece-nos pressuposto no equilíbrio entre as suas necessidades (quais, porque não são coletivamente sufragadas) e desejos/ansias individuais egoístas. Neste jogo de soma zero para o cidadão - ainda que negociado como uma troca de soma não nula -, a propósito de segurança (ou saúde) prometidos pelo estado, este cede, no todo ou em partes, a sua individualidade. Uma vez tal cedência concretizada, a superioridade informacional granjeada, detida pelo *estado de vigilância,* tende a exaurir os mecanismos democráticos de supervisão do próprio estado, na

3 Podemos trazer à colação, para melhor percebermos, desde logo, os sistemas de videovigilância municipal já implementados. De igual forma, podemos pensar sobre a *vigilância*, embora míope quando o cidadão contribuinte tem uma riqueza pessoal assinalável – e tal miopia poderá explicar a constância de acesso de tais cidadãos a regime excecionais de regularização tributaria - exercida pela Autoridade tributária. Recentemente, uma *novidade*, a *app* stayawaycovid.
Entre reconhecimento facial, pelas cameras de videovigilância; rastreamento através do cartão Mb – incentivado o seu uso massivo também a propósito da pandemia, sendo o *contactless* qual "sabão azul" nas medidas de mitigação da propagação da doença – não só através da localização como também do perfil de consumo, entre outros; à coleta de dados de saúde que a *app* permite, bem como o rastreio geolocalizado; de tudo temos experimentado. Os propósitos são "*claros*": segurança, combate ao crime e saúde. Aliciantes…

medida em que o monopólio do conhecimento lhe permite controlar tudo o que pode ser divulgado. Bem coordenado com uma assinalável retórica de medo, tal *estado* passa a dispor da faculdade de usar os seus poderes para propósitos indiferentes à origem e finalidades registadas aos *baby-step* da sua implementação. Distopia? Sim. E já representada nas nossas vidas.

Urge, pois, contrariar as pulsões totalitaristas de *estados de vigilância*, promotores de exclusão e discriminação, sob pena de o nosso futuro, enquanto ente coletivo, ser irreparavelmente composto por cidadãos desprovidos da sua individualidade intrínseca.

Tal distopia estadual não serve à pessoa humana. A luta convoca-nos a todos.

O núcleo não pode, em momento algum, ser desfocado da sua essência: Estado ao serviço da pessoa. Tecnologia ao serviço da pessoa. É pela pessoa que o Estado se materializa. É para a pessoa que o Estado se organiza numa comunhão de direito democrático. É por um Estado que promove e prossegue o cardápio de direitos, liberdades e garantias fundamentais da pessoa que cumpre lutar. De igual forma, o recurso à ferramenta de auxílio – a tecnologia (digital) – pode e deve ser feito sempre que a finalidade seja construir um ente coletivo em que a pessoa é e sempre, também pela sua individualidade intrínseca, um fim em si mesmo. É por tal *futuro por design*, na disponibilidade da pessoa e pela pessoa humana que devemos concentrar o nosso esforço coletivo.

Nesta nova edição da Cyberlaw by CIJIC, perseguidos por tais inquietações, tivemos o ensejo de provocar os autores participantes à procura de juízos sobre a realidade desafiante que convoca a sociedade atual. E futura. Entre a inteligência artificial e a *algocracia* e os desafios que estas convocam ao Direito (e aos juristas); passando pelo crime de violência domestica num contexto de abuso (mais uma forma de abuso) através das redes sociais e a proteção jurídico-penal que a vida privada exigem; à utilização de *benware* como meio de neutralização das técnicas e medidas antiforenses que os criminosos usam; à engenharia do "direito penal sobre rodas" e ao agente inteligente automóvel num contexto de um certo desarranjo terminológico - todos escritos em língua portuguesa - e ante as responsabilidades – que já demos conta oportunamente – impondo-se-nos a difusão de conteúdo em inglês escrito, juntamos três temas desafiantes: *State surveillance; fake news & social networks; open banking*.

Como era expectável, *ab initio*, os temas são desafiantes. Para todos. São, como sempre, abertos a colaboração múltipla e, de preferência, participada. A prova foi, quer-nos parecer, superada com mestria.

Entretanto abre-se a janela da próxima edição, para Março de 2021. Não sem antes sublinhar que, nos próximos tempos, ante os critérios definidos pelo corpo diretivo e pelo editor, em parceria com a Associação académica da faculdade de direito de lisboa, passaremos a dispor de um número da revista, anualmente, em formato de papel.

Resta-me, por fim, agradecer a todos quantos contribuíram para mais esta nova edição da Revista, pelo esforço, pela disponibilidade, pela obra, endereçando a todos, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um merecidíssimo: - Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 29 de Setembro de 2020

Nuno Teixeira Castro

A INTELIGÊNCIA ARTIFICIAL NA ERA GLOBAL DIGITAL DESAFIA O DIREITO E RESPONSABILIZA OS JURISTAS

IN THE DIGITAL GLOBAL AGE ARTIFICIAL INTELLIGENCE CHALLENGES THE RULE OF LAW SUMMONING JURISTS TO IT

MARCO ANTÓNIO MARQUES DA SILVA *

EDUARDO VERA-CRUZ PINTO *

* *Marco Antonio Marques da Silva*. Pontifícia Universidade Católica de São Paulo (PUC-SP), Brasil
* *Eduardo Vera-Cruz Pinto.* Universidade de Lisboa (UL), Portugal

RESUMO

Será eficaz a resistência jurídica à invasão tecnológica globalizada que sustenta o tecno-capitalismo numérico?

A tecnologia digital e a Inteligência Artificial (IA), quando aplicadas em benefício da pessoa humana, trazem ganhos e vantagens para a Humanidade nunca alcançados. Por outro lado, a mesma tecnologia compreende efeitos devastadores na nossa forma de estarmos com os outros e de nos preocuparmos com o próximo. Afeta o nosso modo de viver em sociedade e facilita a manipulação da informação com apropriação do conhecimento de massas capaz de destruir o que foi erguido como marco civilizacional na Democracia e na civilidade jurídica.

Diminuir os maus efeitos da tecnologia digital passa por democratizar o acesso a esta e à IA. A tecnologia é imprescindível para a evolução, todavia, não é neutra e nem todos os avanços tecnológicos são benéficos ao ser humano. O Algoritmo vai criando sociedades diferentes daquelas que o Direito construiu para as pessoas humanas. Educar o nosso cérebro para resistir, como humano, às propostas comodistas que o diminuem em racionalidade, inteligência e discernimento é um dos maiores desafios do presente.

Os algoritmos devem ser utilizados nos limites que definirmos para que não sejamos removidos dos processos de decisão. A tecnologia tem de estar ao serviço da sociedade - construída sobre as bases de harmonia, justiça, igualdade e solidariedade - e não o inverso, *ie*, a sociedade não pode estar subserviente à tecnologia e à IA.

A revolução digital mudou definitivamente a pessoa humana, a vida em sociedade e a economia. Poderá o Direito ser a resposta humana para aquilo a que se intitula de *algocracia*?

***Palavras-Chave**: tecnologia e* revolução tecnológica; algoritmo; inteligência artificial; Direito; *algocracia*.

ABSTRACT

Can legal resistance to the globalized technological invasion, that underlies numerical techno-capitalism, be effective?

Digital technology and Artificial Intelligence (AI), when applied for the benefit of the human person bring gains and advantages for Humanity as never before. On the other hand, the same technology has devastating effects on the way we relate to others and worry about them or about each one another. It affects our way of living in society and helps to manipulate information with appropriation of mass knowledge enabling the destruction of what was erected as a civilizational landmark in Democracy and its legal civility.

Reducing the bad effects of digital technology implies democratizing access to it and AI. Technology is essential for evolution, however, it is neither neutral nor all technological advances are beneficial to human beings

The Algorithm creates societies different from those that Law has built for human people. One of the greatest challenges in the present is to educate our brain to resist, as a human, to the comfortable proposals that diminish us in rationality, intelligence and insight and judgment. Algorithms must be used within the limits that we define it so that we are not removed from the decision-making process. Technology must always be at the service of society - built on the foundations of harmony, justice, equality and solidarity - and not the other way around: society must not be subservient to technology and AI.

Digital revolution has definitely changed the human person, life in society and our economy. Could Law be the human answer to what is called *algocracy*?

Key words: technological and digital revolution; algorithm; artificial intelligence; Law; *algocracy*.

Mudamos de época histórica, pois já estamos em plena Era Digital, e não nos apercebemos. Por isso, devemos colocar as questões essenciais para o contexto em que o Direito vai ser criado e aplicado nesta *nova Era*: a despersonalização da inteligência pelo algoritmo será o futuro? A desumanização da pessoa ficará como regra inscrita nas leis? Será eficaz a resistência jurídica à invasão tecnológica globalizada que sustenta o tecno-capitalismo numérico como ideologia de Estado? A quase totalidade da população mundial terá acesso à conectividade móvel, à banda larga em interligação no momento e à internet das coisas (com substituição da *cloud* pela *edge computing* ou computação de borda). Essa será uma consequência da diminuição do contacto social na normalização da vida com o vírus Covid-19? A revolução digital mudou definitivamente a pessoa humana, a vida em sociedade e a economia. Quem ainda não sabe isso? Como viver ignorando isso? Como reagiremos, enquanto sociedade global, a esse fenómeno?

A respeito do assunto, tivemos a oportunidade de apontar anteriormente:

"*Nesse novo tempo, a explosão de informações de todo e qualquer conteúdo, de forma irrestrita e ilimitada, não só pelos meios de comunicação de massa, como rádio e televisão, mas também e principalmente pelas redes sociais e demais veículos da internet, com transmissão de dados e velocidade em proporções muitas vezes incomensuráveis, traz consequências de toda ordem, com reflexos políticos, religiosos, sociais, antropológicos, econômicos, fundamentais e etc.*"[1].

Nessa toada de indagações, observa-se que a tecnologia digital e a Inteligência Artificial (IA), quando aplicadas em benefício da pessoa humana, trouxeram ganhos e vantagens para a Humanidade nunca alcançados.

Por outro lado, a tecnologia tem efeitos devastadores na nossa forma de estarmos com os outros e de nos preocuparmos com o próximo. Afeta o modo de viver em sociedade e facilita a manipulação da informação (notícias falsas)[2] com apropriação do conhecimento

1 SILVA, Marco Antonio Marques da. Direito ao Esquecimento - Posicionamento Jurisprudencial Brasileiro. *In*: PINTO, Eduardo Vera-Cruz; SILVA, Marco Antonio Marques da; CICCO, Maria Cristina de (coordenação). Direito à Verdade, à Memória, ao Esquecimento. Lisboa: AAFDL, 2018, p. 183.
2 MORGAN, Susan. Fake news, disinformation, manipulation and online tactics to undermine democracy, in *Journal of Cyber Policy*, 3:1, 2018, pp. 39-43, DOI: 10.1080/23738871.2018.1462395.

de massas que pode destruir o que foi erguido como marco civilizacional na Democracia e na civilidade jurídica.

Inicialmente, é importante definir inteligência artificial, inclusive distingui-la de programação. A inteligência artificial é um conceito originário da informática e a ideia principal é permitir que computadores possam "*emular a inteligência humana ao realizar determinadas tarefas*". O pesquisador de Stanford, John McCarthy, cunhou o termo em 1956 (durante a Conferência de Dartmouth), considerando que "*um programa de computador poderia ser considerado AI se fosse capaz de fazer algo que normalmente atrelamos à inteligência de seres humanos*"[3].

A inteligência artificial pode ser compreendida como "*a capacidade de dispositivos eletrônicos funcionar de uma maneira que lembra o pensamento humano. Isso implica em perceber variáveis, tomar decisões e resolver problemas (...) sem a interferência humana*"[4]. A IA faz a análise de dados e pode trazer soluções para múltiplas questões apresentadas, mesmo que não tenham previamente sido "ensinadas" à IA.

Todavia, a programação pode ser apenas programar *software* para realizar determinadas tarefas previamente estabelecidas, enquanto a IA tem todo um conhecimento parecido com o funcionamento neural humano, podendo ter treinamento para que o algoritmo possa resolver novas tarefas com o aprendizado anterior – como o *machine learning*[5].

Por sua vez, a IA é distinta de *software*. Este é o local onde a inteligência artificial se desenvolve, dando soluções aliadas a análise de dados para execução do *hardware*. Em analogia ao corpo humano, o *hardware* seria a musculatura humana e o software o cérebro[6].

Assim, o uso da IA no exercício das profissões jurídicas, nomeadamente da advocacia[7], vai mudar muito a realidade judiciária e o Direito da Cibersegurança passará a ser uma exigência horizontal para todas elas. O modo de criar, interpretar e aplicar as regras jurídicas vai sofrer grandes alterações. Uma IA regulada pelo Direito pode ser a chave para

3 MAGRANI, Eduardo. *Entre Dados e Robôs.* Ética e privacidade na era da hiperconectividade. Porto Alegre: Arquipélago Editorial, 2019, p. 51.
4 FIA. *Inteligência Artificial:* o que é, como funciona e exemplos. Disponível em: https://fia.com.br/blog/inteligencia- artificial/. Acesso em 19.08.2020.
5 CONECTANDO NET. Diferença entre inteligência artificial e aprendizado de máquina. Disponível em:https://conectandonet.com.br/blog/diferenca-entre-inteligencia-artificial-e-aprendizado-de-maquina/ . Acesso em 19.08.2020.
6 Idem, ibidem.
7 ALARIE, Benjamin; NIBLETT, Anthony; YOON, Albert H. How artificial intelligence will affect the practice of law. *University of Toronto Law Journal*, v. 68, n. supplement 1, p. 106-124, 2018.

o futuro da Humanidade. Este é um dos principais desafios políticos e culturais da União Europeia.

Hoje, a economia carbonizada é a melhor justificação para a impunidade na quarta revolução industrial que tem uma produção "invisível". Os negócios são executados eletronicamente e em ambiente exclusivamente digital, muitos sem intervenção humana, quase todos sem regulação eficaz.

Logo é uma economia sem fisicalidade, sem regras (desregulada), sem resistências. A economia virtual dos algoritmos instala-se lentamente, prescindido das pessoas em benefício de poderosos e de abusadores. A Inteligência Artificial, que aqui é a desculpa e o meio, não pode servir para isto. O Direito pode ser a melhor (a única?) resposta humana[8] para a que se denomina de *algocracia*[9]. A União Europeia está a fazer os primeiros ensaios jurídico-legais nesse sentido.

A título exemplificativo das inovações tecnológicas e suas aplicações, na União Europeia foi criado o Observatório Europeu para o 5G para acompanhar a comercialização da tecnologia móvel de quinta geração (5G) nos Estados-membros. Inclusive alguns Estados estão a investir na tecnologia de *blockchain* para reduzir ou mesmo eliminar os intermediários económicos realizando transações comerciais diretas (*peer to peer*) entre quem produz e quem compra e realizar atos públicos sem passar por um funcionário que "*só cria dificuldades para obter uma vantagem*" (pagamento de uma comissão, uma gorjeta, uma prenda). Pode ser esta uma forma de, usando a IA, reduzir margens ilegítimas de lucro e assim reduzir as desigualdades criadas pela economia digital. Ou pode funcionar exatamente ao contrário? Não sabemos. É preciso ousar, experimentar, criticar, analisar e depois agir, decidir com base no conhecimento adquirido e colocando a pessoa humana acima de tudo e de todos.

Um primeiro consenso a que se chegou na União Europeia foi que a forma de diminuir os maus efeitos da economia digital é democratizar o acesso às tecnologias e à IA, para que não sirvam apenas uma pequena elite empresarial que enriquece com essa vantagem competitiva ou por uma elite política governamental que adquire, por esse meio, mais poder

8 CHINEN, M. *Law and autonomous machines the co-evolution of legal responsibility and technology.* Cheltenham: Edward Elgar Publishing, 2019.
9 DANAHER, John. The Threat of Algocracy: Reality, Resistance and Accommodation https://philpapers:org/archive/DANTTO-13:pdf.

menos controlado. Os avultados investimentos públicos em IA têm de ser universalizados nos seus efeitos.

A maioria dos parlamentos europeus legisla para que a utilidade social das inovações tecnológicas e do uso da IA tenha de ser garantida por regras jurídicas positivadas como normas legais, que as impeçam de ficar retidas nas empresas com capacidade para as produzir além da justa remuneração do investimento feito e do risco que correram com tais projetos. A pessoa humana aumentou imenso o seu conhecimento, mas não conseguiu manter a inteligência necessária para a usar consigo e para si[10].

Importante salientar que para a criação das novas tecnologias inteligentes artificialmente, contribuíram também cientistas formados nas universidades públicas. Para tal criação, as empresas receberam financiamento público para esses projetos e, atualmente, estão em situação de monopólio ou cartel no mercado digital. As entidades reguladoras têm de ter uma base legal para poderem atuar em defesa da difusão das inovações tecnológicas que usam a IA pela economia e a comunidade tem de ser muito exigente em relação à sua eficácia coletiva e ao compromisso de justiça social.

Nesse ideia de justiça social pelo uso da tecnologia de código aberto, foi criada a primeira criptomoeda, denominada *bitcoin*. O *idealizador*, Satoshi Nakamoto, compreendeu que ao abrir o código e descentralizá-lo, permitiria que qualquer pessoa, indiscriminadamente, sem qualquer análise prévia de crédito, desde que possua computador e o conhecimento, que foi passado, possa adquirir e transacionar valores, independente de um terceiro que seria o banco, pouco importando qualquer condição, normalmente exigida por um banco. Nas palavras de Fernando Ulrich, "*o Bitcoin também tem o potencial de melhorar a qualidade de vida dos mais pobres no mundo. Aumentar o acesso a serviços financeiros básicos é uma técnica antipobreza promissora (...) O Bitcoin, dessa forma, proporciona uma válvula de escape para pessoas que almejam uma alternativa à moeda depreciada de seu país ou a mercados de capitais estrangulados. (...) Experiências recentes com governos despóticos sugerem que cidadãos oprimidos se beneficiaram altamente da possibilidade de realizar transações privadas, livres das garras de tiranos. O Bitcoin*

10 A sociobiologia procura compreender se os avanços tecnológicos terão superado as capacidades naturais do cérebro humano, sobretudo no uso das redes neuronais (Edward O. Wilson).

oferece algo de privacidade como a que tem sido tradicionalmente permitida pelo uso de dinheiro vivo – com a conveniência adicional de transferência digital"[11].

As máquinas aprendem sozinhas (*machine learning*) e mais do que nós lhes ensinamos.[12] Haja vista o emblemático caso em que, os robôs inteligentes artificialmente desenvolvidos pelo Facebook tiveram de ser desligados depois que criaram uma linguagem entre si, a partir de simples negociação simulada. Veja que essa nova linguagem criada pelas máquinas, sem qualquer programação prévia, acabou de certa forma assustando os desenvolvedores, que preferiram desligar e postergar tal desenvolvimento.

Assim, a criação de uma inteligência não humana, de difícil controle pelas pessoas, mudará a noção de privacidade e de segurança (cibersegurança). As máquinas passam a fazer operações autónomas de associação (inteligência associativa). Trata-se de uma fonte de ação inteligente, não apenas de automação ou internet das coisas. As máquinas e os algoritmos substituem os humanos e o que eles sabem fazer. Num mundo assim, o que significa ser (ou manter-se) humano?

A vigilância total como meta política é sempre uma ameaça à privacidade e à intimidade necessárias ao *quantum humano* das pessoas. O recurso intensivo ao reconhecimento facial como instrumento de segurança pública[13] tem um impacto devastador na proteção jurídica de dados pessoais[14]. Inclusive em Portugal a restrição ao uso destas técnicas está positivada e a aplicação das normas legais é seguida de perto pela Comissão nacional de Proteção de dados (CNPD)pessoais[15].

Acerca da inovação dessa revolução que é a internet das coisas, há alguns pontos que devem ser observados, ressaltados por Jenny Judge e Julia Powles, possivelmente, com a inovação da internet das coisas haverá desculpa para o aumento do consumismo, além de

11 ULRICH, Fernando. *Bitcoin: o que é como funciona.* São Paulo: Instituto Ludwing von Mises Brasil, 2014, livro digital p. 15.
12 GRIFFIN, Andrew. *Facebook´s Artificial Intelligence Robots Shut Down after they start talking to each other in their own language.* Independent. Disponível em: <https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-artificial-intelligence-ai-chatbot-new-language-research-openai-google-a7869706.html >. Acesso em 13.08.2020.
13 Afonso de Freitas Dantas e Manuel Poêjo Torres, "State Surveillance: how is face-recognition technology impacting the politico-juridical landscape?", in Review CIJIC/IURIS-FDUL, número especial, 2020.
14 COTINO HUESO, Lorenzo. *Big data e inteligencia artificial.* Una aproximación a su tratamiento jurídico desde los derechos fundamentales. In: Dilemata – Revista Internacional de Éticas Aplicadas, 2017, nº 24, p. 136.
15 Comissão Nacional de Proteção de Dados, Parecer/2019/92, Processo PAR/2019/61; Comissão Nacional de Proteção de Dados, Parecer/2019/93, Processo PAR/2019/62; Concurso Público N.º 235/19/DCP/GACD/Software de Reconhecimento Facial e Deteção de Vida. *in* Diário da República, Anúncio de procedimento n.º 13672/2019, Série II de 2019-12-10.

que os objetos domésticos diários possam virar *espiões inimigos*[16], sob constante vigilância, observados em todo momento, passíveis de manipulação pelos dados gerados por nós, e a solução proposta pelas autoras é a de que as pessoas tenham controle dos dados e que estes sejam usados de forma inteligente:

"*A internet das coisas é outra desculpa para consumismo desenfreado, qual a única contribuição será abarrotar o porão com ainda mais tralha desnecessária. Mas no pior, objetos domésticos de uso diário serão transformados em espiões inimigos, mantendo-nos em constante vigilância. Nós somos cutucados e manipulados todos os momentos. Nossas vidas e posses serão perpetuamente expostas aos hackers. A internet das coisas irá preencher nossas casas com objetos adequados, mas esses objetos são longe de serem encantados – eles são amaldiçoados. (...) A saída é contraintuitiva. Em um curto período, nós necessitaremos esquecer sobre as coisas. Nós precisamos parar com a obsessão de ter mais objetos "inteligentes", e começar a pensar na inteligência das pessoas*"[17] (tradução livre).

Nesse sentido, a educação nunca se fez tão presente e necessária, sob pena de mais uma vez a população ser manipulável, pois como informa Sérgio Czajkowski Júnior[18], a tecnologia é imprescindível para a evolução, todavia, não é neutra e nem todos os avanços tecnológicos são benéficos ao ser humano.

Por isso, os menos preparados (crianças, adolescentes e idosos) estão expostos à pressão social *online* e ao *ciberbulling* até ao limite da sua saúde mental. A solidão partilhada em comunidades insulares *online* aumenta o discurso do ódio, as teorias da conspiração e o radicalismo extremista das opiniões *tweetadas*. O Algoritmo vai criando sociedades diferentes daquelas que o Direito construiu para as pessoas humanas.

16 JUDGE, Jenny. POWLES, Julia. Forget the internet of things: we need an internet of People. *The Guardian*, 25.05.2015. Disponível em: <https://www.theguardian.com/technology/2015/may/25/forget-internet-of-things-people >. Acesso em 16.08.2020.

17 "the internet of things is just another excuse for rampant consumerism, whose only contribution will be to clog basements with yet more unnecessary junk. But at worst, everyday household objects will be turned into enemy spies, placing us under constant surveillance. We will be nudged and manipulated at every moment. Our lives and possessions will be perpetually exposed to hackers. The internet of things will fill our homes with objects all right, but those objects are far from enchanted – they are cursed. (…) The way out is counterintuitive. In short, we need to forget about the things. We need to stop obsessing over "smart" objects, and start thinking smart about people".

18 CZAJKOWSKI JR., Sérgio apud Karasinski, Lucas. O que é tecnologia? *Tecnomundo*, 29.07.2013. Disponível em: < https://www.tecmundo.com.br/tecnologia/42523-o-que-e-tecnologia-.htm >. Acesso em 16.08.2020.

Educar o nosso cérebro para resistir, como humano, às propostas da tecnologia que o diminuem em racionalidade, inteligência e discernimento é um dos maiores desafios das sociedades de hoje. Assim, circula como informação o que é opinião editada num discurso que, ou confirma as minhas crenças ou não interessa e é considerado como falso. Presos na circularidade daquilo que nos é dado (ou que nós procuramos) perdemos a vontade de inovar, a capacidade crítica sem hipercriticismo e a possibilidade de nos adaptarmos para viver como pessoas humanas em ambientes tecnológicos claustrofóbicos que nos aprisionam a humanidade. Sim, viver porque, como no lema dos sobreviventes de Estação Onze, de Emily St John Mandel: "sobreviver não é suficiente".

Observa-se que as sociedades estão cada vez mais divididas, distópicas e as posições mais extremadas. A adesão emotiva a causas por que "são boas" e dos "bons" contra os "maus" planta a semente da intolerância e da ditadura com discursos a contrário de inclusão e de democracia. Nas seitas da *net* cada vez é mais difícil separar o facto da ficção, o real do inventado, o verdadeiro do falso. A tecnologia, assim usada, é desagregadora, torna-nos solitários, violentos e predadores, divide-nos e incapacita-nos para (re)agir coletivamente e apela ao que de mais animal e primário existe na condição humana, diminuindo a sua dimensão de pessoa. Por isso, se as plataformas digitais continuarem a ser usadas pelas multinacionais do ciberespaço como estão a ser, a nossa humanidade pode correr perigo.

Além da necessidade aceitar com crítica as informações veiculadas hoje, pois muitas podem ser resultado de *fake news*, é imprescindível atermo-nos aos parâmetros iniciais inseridos nos algoritmos de IA, para que também não se caia na tentação de rotular e discriminar, uma vez que preconceitos humanos também podem ser refletidos na programação computacional, pela possibilidade dos valores humanos do programador reproduzirem preconceitos[19].

Basta verificar a criação do software para a Polícia Norte Americana com a finalidade de prevenir a criminalidade. Referido programa não trouxe qualquer nova informação que a Polícia não soubesse. Além disso, tinha base de dados preconceituosa, pois apontava para

19 POLLO, Luiza. *Inteligência Artificial genérica pode colocar máquinas contra humanos.* UOL, 22.08.2019. Disponível em: < https://tab.uol.com.br/noticias/redacao/2019/08/22/inteligencia-artificial-generica-pode-colocar-maquinas-contra-humanos.htm >. Acesso em 16.08.2020.

latinos e negros para pessoas mais propensas a cometer crimes, voltando a superadas teorias do criminoso[20].

Pode tornar-se realidade a ficção de serem as pessoas humanas substituídas por robôs, sob a forma de algoritmos e de sistemas de análise preditiva ("a realidade é muito abusadora" – Mário de Carvalho)? Depende de nós. Os algoritmos devem ser utilizados nos limites que definirmos para que os humanos não sejam removidos dos processos de decisão[21].

O algoritmo processa informação e é frio, totalmente objetivo e aplica aquilo que é mais rentável (otimiza). O automatismo decisório da máquina pode dar soluções ótimas, mas incompatíveis com a nossa imprescindível subjetividade, as nossas regras de vida em sociedade e os valores inerentes à defesa da pessoa humana e dos seus direitos e liberdades (Hannah Fry, Hello World). Só o compreenderemos se formos lá atrás ao luditismo (movimento popular que partia as máquinas na Revolução industrial) e à crítica da técnica e da maquinação feita por Charles Chaplin e por Duchamp e pela sua normalização artística com Miguel Palma.

Cruzados estes algoritmos na IA para resolver, com base nos dados disponíveis, problemas complexos cuja solução requer a "*mão da pessoa humana*" é um problema. Isso porque o algoritmo não trabalha com exceções às regras que lhe foram dadas (muitas delas só identificáveis após a aplicação da regra que conduz a uma solução injusta). Nega assim a possibilidade de justiça que só existe onde a regra pode ser excecionada.

A regra jurídica não é um dogma e ainda menos um determinismo que não se pode afastar. A aplicação da regra depende sempre da boa e possível solução (logo justa e eficaz) do caso concreto. Por isso, o Direito é uma criação humana que só as pessoas humanas podem aplicar, sendo imprescindível à vida em sociedade. Daí que, antes de avançar para soluções técnico-legais em matéria de IA, importa conhecer a natureza humana e os limites do Jurídico. Precisamos usar a nossa inteligência natural para compreender o que separa o

20 UOL. *Inteligência artificial promete prevenir crimes, mas fracassa*. Disponível em: < https://tab.uol.com.br/noticias/redacao/2019/07/11/inteligencia-artificial-promete-prevenir-crimes-mas-fracassa.htm >. Acesso em 11/07/2019.

21 O algoritmo (nome com origem em al-Khwarizmi, pai da álgebra) ao resolver diversas equações matemáticas com passos firmes, simples e de forma sistemática permite solucionar um problema do mundo real. A boa solução otimiza os recursos e dá celeridade e, assim, todos ganhamos com isso.

nosso cérebro da tecnologia por ele criada e o que é incompatível entre os produtos tecnológicos e a nossa humanidade.

Para isso, é preciso: dinheiro, obtido através de uma fiscalidade adequada e eficaz para garantir a transferência do capital do lucro para a ética; uma política que institua um sistema de redistribuição que ligue as verbas assim obtidas ao investimento em educação digital e em comunicação social sobre estas matérias[22]; políticas públicas que reforcem o combate contra conteúdos virais mal-intencionados e as *deepfakes* (adulteração tecnológica de vídeos produzidos e manipulados pela IA para parecerem verdadeiros), por entidades estaduais competentes e eficazes.

Nesse sentido, o dinheiro para investir nesse conhecimento sobre os limites a fixar à tecnologia para que permaneçamos humanos - um conhecimento sobre as nossas possibilidades e os nossos limites - deve vir das empresas que têm como negócio ultralucrativo a nossa degradação humana pela via digital ("gigantes tecnológicos"). Não basta a doação – sempre anunciada como publicidade – das empresas beneficiadas para esse fim.

E mais, precisamos de um sistema de impostos sobre essas empresas e de taxas sobre os serviços e bens que vendem e sobre o seu património. Um sistema que desenvolva legislação que criminalize os comportamentos abusivos e lesivos da humanidade das pessoas, com pesadas multas pecuniárias e cancelamento de licenças para o exercício da sua atividade. A UE tem procurado seguir esse caminho com oposição muito firme e eficaz dos EUA (sobretudo na era nacional-protecionista em que está).

No que diz respeito à educação, implica investir em educação presencial e em grupos de confiança em torno de objetivos comuns retirando tempo das pessoas que estão hoje disponíveis para se sentarem à frente do computador e tentarem criar consensos sobre o modo de usar telemóveis e computadores em sala de aula e em ambiente escolar. Ligando as políticas de educação digital aos escalões etários; e definir os casos, situações e matérias onde o uso de instrumentos digitais constitui instrumento de apoio didático e restringir o seu uso na obtenção de informação a tais casos. Elaborar programas disciplinares obrigatórios de formação digital sobre o uso adequado das tecnologias e da internet.

22 Um sistema que financie a criação de plataformas digitais que incentivem a solidariedade entre as pessoas e promovam atitudes e ideias características da humanidade da pessoa e da personalidade do humano.

A pandemia de covid-19 tornou urgente a responsabilização dos juristas numa intervenção profissional e cívica em defesa da pessoa humana face ao mau uso da IA. Precisamos de estar atentos à normalização de situações que se justificavam em Estado de exceção por causa da contenção do contágio e que não podem perdurar fora dele. O recurso às novas tecnologias para desenvolver instrumentos eficazes para a vigilância de cidadãos com rastreamento de contactos[23] e a sua identificação facial em lugares públicos para instituir um sistema que cruza esses elementos com outros constantes em bases de dados pessoais tem de ser, mais que controlado, destruído[24].

A par disso tudo, a literatura ficcional (Zamiatine, Nós. Obra que inspirou 1984 de Georges Orwell) não pode ser superada pela realidade que se pretende normalizar em Estados controladores da sua população ao ponto dos direitos pessoais e familiares estarem totalmente submetidos àquilo que os poderes instituídos entendem por "*interesse geral*" ou "*bem comum*". A ficção corporizou em filmes a superioridade dos animais sobre os humanos (O Planeta dos Macacos) e das máquinas sobre as pessoas (Wall. E) como avisos (que tornam reais as possibilidades) sobre as nossas escolhas e descasos.

Uma das utilizações positivas das tecnologias digitais e da IA é o combate ao crime organizado (as máfias) que aproveitará o mundo pós-pandemia para expandir os seus negócios ilícitos.

Importante salientar que o crime organizado não é um problema de polícia e de tribunais. É um problema político sério, pois o seu êxito depende das fragilidades sociais e da fraqueza dos Estados. Se a sua tecnologia para praticar crimes for mais desenvolvida e eficaz que a do Estado para os combater, a batalha pela Justiça através do Direito no Estado está perdida.

Inclusive, estas máfias são indiferentes ao sofrimento, sem tabus morais e tudo sacrificando ao lucro fácil obtido com o crime, ocuparão todos os vazios, preencherão todas as necessidades, utilizarão todas as fragilidades das leis (conquistando legalmente sectores

23 Nomeadamente, o uso das tecnologias de *contact tracing* como medida de apoio às atividades de contenção da epidemia do novo coronavírus. "TechDispatch #1/2020: Contact Tracing with Mobile Applications", de 7 de maio de 2020, da Autoridade Européia de Proteção de Dados (AEPD).

24 De acordo com a recomendação do Comitê Europeu de Proteção de Dados quando escreve "a atual crise sanitária não deve ser utilizada como uma oportunidade para conferir mandatos desproporcionados para efeitos de conservação de dados. A limitação da conservação deve ter em consideração as verdadeiras necessidades e a pertinência médica (que pode incluir considerações epidemiológicas como o período de incubação, etc.), devendo os dados pessoais ser mantidos apenas durante a crise da COVID-19". Em "Diretrizes 4/202 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19", de 21 de abril de 2020.

económicos inteiros), ampliarão as suas "bases sociais de apoio" e usarão a violência com aceitação social quando for preciso, se nada mais a travar, lembrando que a tecnologia também pode ser usada a esse propósito.

A União Europeia procura apoiar os Estados mais fragilizados pela pandemia no uso adequado da tecnologia digital como modo de prevenção e repressão do crime organizado e dos movimentos antidemocráticos que aproveitam a situação[25], usando a IA como instrumento de eficácia da Democracia submetendo a sua utilização às regras de Direito.

É preciso que a tecnologia utilizada por regimes autoritários em Democracia formal (a caminho de totalitarismos disfarçados na retórica dos seus proponentes) para restringir direitos mostrando eficácia no combate à epidemia não sirvam para os legitimar e que as democracias saibam colocar esses meios ao serviço do mesmo combate com eficácia, mas usando-os para reforçar a garantia dos direitos das pessoas contra os abusos coletivos.

A demagogia social-nacionalista (populismo é um nome para muita coisa, a evitar) e dos movimentos sociais apoiados por partidos intolerantes e proibicionistas espreita sempre uma oportunidade para a deriva autoritária e a tomada do poder a médio prazo. A União Europeia tem políticos preparados para enfrentar os "novos fascismos" de direita e de esquerda (Josef Joffre para o negar só analisa o curto prazo). A ter êxito, nesse caminho de juridicização das tecnologias digitais, a IA será um dos principais instrumentos de *rehumanização* da pessoa humana.

Não há dúvidas de que a inteligência artificial será a nova tendência dos próximos anos em todas as áreas e na sociedade como um todo. Porém, será importante aplicá-la em situações responsáveis com a sociedade, tendo sempre como linha guia de seu algoritmo o supraprincípio da dignidade da pessoa humana, lembrando que a tecnologia trabalha para a sociedade construída nas bases de harmonia, justiça, igualdade e solidariedade, e não o inverso, a sociedade não trabalha para a IA.

Em conclusão, é dever dos juristas apontar e delinear as circunstâncias em que a Inteligência Artificial funcionará, de modo a não se sobrepor ao ser humano em sua dignidade humana, constituindo invento que deve agregar no sentido humano, e não apenas tecnológico.

25 PINTO, Eduardo Vera-Cruz. O Direito após a pandemia de COVID- 19: os binómios Fundamentais. (Law after the COVID- 19 pandemic: the fundamental binomials), *In Revista da Faculdade de Direito da Universidade de Lisboa*, 2020.

BIBLIOGRAFIA

ALARIE, Benjamin; NIBLETT, Anthony; YOON, Albert H. How artificial intelligence will affect the practice of law. *University of Toronto Law Journal*, v. 68, n. supplement 1, p. 106-124, 2018.

ASHLEY, Kevin; BRANTING, K.; MARGOLIS, H. & SUNSTEIN, C. R. Legal *Reasoning and Artificial Intelligence: How Computers" Think" Like Lawyers*. University of Chicago Law School Roundtable, v. 8, n. 1, p. 1-28, 2001.

BAIÃO, Kelly Sampaio. GONÇALVES, Kalline Carvalho. *A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana*. Civilistica.com. Rio de Janeiro, a. 3, n. 2, jul.-dez./2014. Disponível em:http://civilistica.com/wp-content/uploads/2015/02/Baião-e-Gonçalves-civilistica.com-a.3.n.2.2014.pdf .acesso em 15 de Julho 2020.

BARTON, Benjamin H. *Glass half full: The decline and rebirth of the legal profession.* Oxford University Press, USA, 2015.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BOOS, Tobias. G*eographies of Cyberspace: Internet, Community, Space, and Place* [em linha]. In Inhabiting Cyberspace and Emerging Cyberplaces: The Case of Siena, Italy. 1ª Ed. [s.l.]: Palgrave Macmillan, 2017. pp. 13 a 38. Disponível em: https://www.springer.com/cda/content/document/cda_downloaddocument/9783319584539-c2.pdf?SGWID=0-0-45-1625321-p180850642 .

BUCHANAN, Bruce G. *A (very) brief history of artificial intelligence*. Ai Magazine, v. 26, n. 4, p. 53-53, 2005.

CHINEN, M. *Law and autonomous machines the co-evolution of legal responsibility and technology*. Cheltenham: Edward Elgar Publishing, 2019.

COHEN, Saul Bernard. *Geopolitics, the Geography of International Relations.* Rowman and Littlefield Publishers, 2009; European Union Agency for Fundamental Rights. Facial recognition technology: fundamental rights considerations in the context of law enforcement. Publications Office of the European Union, 2020.

CONECTANDO NET. *Diferença entre inteligência artificial e aprendizado de máquina*.

Disponível em: <https://conectandonet.com.br/blog/diferenca-entre-inteligencia-artificial-e-aprendizado-de-maquina/ >. Acesso em 19.08.2020.

COTINO HUESO, Lorenzo. *Big data e inteligencia artificial.* Una aproximación a su tratamiento jurídico desde los derechos fundamentales. In: Dilemata – Revista Internacional de Éticas Aplicadas, 2017, nº 24.

DANAHER, John. *The Threat of Algocracy: Reality, Resistance and Accommodation*. Disponível em: < https://philpapers:org/archive/DANTTO-13:pdf >.

DANTAS, Afonso de Freitas. TORRES, Manuel Poêjo. State Surveillance: how is face-recognition technology impacting the politico-juridical landscape?, *In:* Review CIJIC/IURIS-FDUL, número especial, 2020.

DONEDA, Danilo et al. *Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal*. Pensar: Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018.

FIA. *Inteligência Artificial:* o que é, como funciona e exemplos. Disponível em: < https://fia.com.br/blog/inteligencia-artificial. Acesso em 19.08.2020.

FLORIDI, L. et al. Artificial Intelligence and the 'Good Society': the US, EU, and UK approach. Science and Engineering Ethics. Springer, 2017.

GASSER, Hans-Peter. *Acts of terror, 'terrorism' and international humanitarian law.* International Review of the Red Cross, Vol. 84, No. 847, September 2002.

GOLDSMITH, Jack e WU, Tim – Who Controls the Net? Illusions of Borderless World [em linha]. Nova Iorque (NY): Oxford University Press, 2006. Disponível em: http://cryptome.org/2013/01/aaron-swartz/Who-Controls-Net.pdf.

GOODENOUGH, Oliver. The State of the Art of Legal Technology Circa 2015. Keynote speech at Codex Future Law, 2015, Available in: https://conferences.law.stanford.edu/futurelaw2015/ Accessed May 23, 2019.

GOUVEIA, Jorge Bacelar. *Direito da Segurança - Cidadania, Soberania e Cosmopolitismo*. Almedina, 2018.

GRIFFIN, Andrew. *Facebook´s Artificial Intelligence Robots Shut Down after they start talking to each other in their own language.* Independent. Disponível em:

<https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-artificial-intelligence-ai-chatbot-new-language-research-openai-google-a7869706.html. Acesso em 13.08.2020.

GROVE, William M.; MEEHL, Paul E. *Comparative efficiency of informal (subjective, impressionistic) and formal (mechanical, algorithmic) prediction procedures: The clinical–statistical controversy*. Psychology, public policy, and law, v. 2, n. 2, p. 293, 1996.

GUERREIRO, Alexandre, *International Law and the Fight Against Terrorism and Cyberterrorism.* in AA. VV. O Direito Internacional e o Uso da Força no Século XXI, AAFDL Editora, 2018.

HARTZOG, Woodrow. SELINGER, Evan Selinger. *The Inconsentability Of Facial Surveillance*. Loyola Law Review, vol. 66, no. 101, 2019.

HILDEBRANDT, Mireille. Law as computation in the era of artificial legal intelligence: Speaking law to the power of statistics. University of Toronto Law Journal, v. 68, n. supplement 1, p. 12-35, 2018.

JUDGE, Jenny. POWLES, Julia. Forget the internet of things: we need an internet of People. *The Guardian*, 25.05.2015. Disponível em: <https://www.theguardian.com/technology/2015/may/25/forget-internet-of-things-people >. Acesso em 16.08.2020.

KAPLAN, Jerry. Artificial Intelligence: What everyone needs to know. Oxford University Press, 2016.

KARASINSKI, Lucas. O que é tecnologia? *Tecnomundo*, 29.07.2013. Disponível em: < https://www.tecmundo.com.br/tecnologia/42523-o-que-e-tecnologia-.htm >. Acesso em 16.08.2020.

KATZ, Daniel Martin. *Quantitative legal prediction-or-how i learned to stop worrying and start preparing for the data-driven future of the legal services industry*. Emory LJ, v. 62, p. 909, 2012.

KLEINBERG, Jon et al. Human decisions and machine predictions. *The quarterly journal of economics*, v. 133, n. 1, p. 237-293, 2017.

KRUECKEBERG, Jennifer et al. Face Off, the lawless growth of face recognition in the UK policing. Big Brother Watch, May 2018, bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf. Acesso em 14.08. 2020.

MAGRANI, Eduardo. *Entre Dados e Robôs.* Ética e privacidade na era da hiperconectividade. Porto Alegre: Arquipélogo Editorial, 2019.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data: A revolution that will transform how we live, work, and think.* Houghton Mifflin Harcourt, 2013.

MCCORDUCK, Pamela. *Machines who Think:* A Personal Inquiry Into the History and Prospects of Artificial Intelligence: [25th Anniversary Update]. AK Peters, 2004.

MCGINNIS, John O.; PEARCE, Russell G. *The great disruption:* How machine intelligence will transform the role of lawyers in the delivery of legal services. Fordham L. Rev., v. 82, p. 3041, 2013.

MORGAN, Susan. Fake news, disinformation, manipulation and online tactics to undermine democracy, in *Journal of Cyber Policy*, 3:1, 2018, pp. 39-43, DOI: 10.1080/23738871.2018.1462395.

NABEEL, Fahad. *Regulating Facial Recognition Technology in Public Places*. Centre for Strategic and Contemporary Research, 2019. Disponível em: https://www.academia.edu/39871139/Regulating_Facial_Recognition_Technology_in_Public_Places. Acesso em: 20 jul. 2020.

NEGRI, Sergio Marcos Carvalho de Ávila. OLIVEIRA, Samuel Rodrigues de. COSTA, Ramon Silva. *O uso de Tecnologias de Reconhecimento Facial Baseadas em Inteligência Artificial e o Direito à Proteção de dados"* in Revista de Direito Público, Universidade Federal de Juiz de Fora.

PINTO, Eduardo Vera-Cruz. O Direito após a pandemia de COVID- 19: os binómios Fundamentais. (Law after the COVID- 19 pandemic: the fundamental binomials), *In*: *Revista da Faculdade de Direito da Universidade de Lisboa*, 2020.

POLLO, Luiza. *Inteligência Artificial genérica pode colocar máquinas contra humanos.*
UOL,22.08.2019.Disponível:https://tab.uol.com.br/noticias/redacao/2019/08/22/inteligencia-artificial-generica-pode-colocar-maquinas-contra-humanos.htm >. Acesso em 16.08.2020.

POST, David. *Governing Cyberspace: Law*. Santa Clara High Technology Law Journal [em linha]. Vol. 24, nº4, Artigo 5 (2008): pp. 883 a 913. Disponível em: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1466&context=chtlj.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, v. 10, n. 1, p. 40-81, 2018.

SILVA, Marco Antonio Marques da. Direito ao Esquecimento - Posicionamento Jurisprudencial Brasileiro. *In*: PINTO, Eduardo Vera-Cruz; SILVA, Marco Antonio Marques da; CICCO, Maria Cristina de (coordenação). *Direito à Verdade, à Memória, ao Esquecimento*. Lisboa: AAFDL, 2018.

SOARES, Marcelo Negri. KAUFFMAN, Marcos Eduardo. CHAO, Kuo-Ming. *Inteligência Artificial: impactos no Direito e na Advocacia,* in Revista de Direito Público, Universidade Federal de Juiz de Fora.

SOUZA, Renato Rocha. "Sobre a Ética Humana e a Ética dos Algoritmos". *In*: Magrani, Eduardo. (Org.). Horizonte presente: Debates de tecnologia e sociedade. 1ed. Rio de Janeiro: Letramento, 2019, v. 1.

SPROWL, James A. Computer-Assisted Legal Research: Westlaw and Lexis. ABAJ, v. 62, 1976.

ULRICH, Fernando. *Bitcoin: o que é como funciona.* São Paulo: Instituto Ludwing von Mises Brasil, 2014.

UOL. *Inteligência artificial promete prevenir crimes, mas fracassa*. Disponível em: < https://tab.uol.com.br/noticias/redacao/2019/07/11/inteligencia-artificial-promete-prevenir-crimes-mas-fracassa.htm >. Acesso em 11/07/2019.

VIOLÊNCIA DOMÉSTICA E REDES SOCIAIS
A PROTEÇÃO JURÍDICO-PENAL DA VIDA PRIVADA NA INTERNET

DOMESTIC VIOLENCE AND SOCIAL NETWORKS
THE LEGAL-CRIMINAL PROTECTION OF PRIVATE LIFE ON THE INTERNET

NUNO POIARES *

* Investigador Integrado do ICPOL e professor do Instituto Superior de Ciências Policiais e Segurança Interna. Professor convidado do Instituto Politécnico de Beja, da Faculdade de Direito da Universidade Lusófona de Lisboa; e tem colaborado, no âmbito da formação avançada em Direito do Ciberespaço, com o Instituto de Ciências Jurídico-políticas e o CIJIC da Faculdade de Direito da Universidade de Lisboa. ORCID ID: https://orcid.org/0000-0002-9325-0206.

RESUMO

No presente artigo pretendemos contribuir para a compreensão da relação entre o crime de violência doméstica e as redes sociais, em particular a proteção jurídico-penal da vida privada na internet. Para atingir uma resposta ao ponto de partida desenvolveu-se um diálogo argumentativo e fundamentado nas questões do direito penal contemporâneo com base no método jurídico, um raciocínio lógico-dedutivo assente na triangulação da jurisprudência portuguesa e do Tribunal Europeu dos Direitos Humanos, na doutrina (nacional e estrangeira) e na legislação, com destaque para a Lei do Cibercrime, o direito penal primário e a lei civil; a par da Constituição da República Portuguesa e a Convenção Europeia dos Direitos Humanos. Nessa senda foram analisadas diversas questões de natureza material à luz do dispositivo vertido na al. b), n.º 2 do art.º. 152.º do CP, para percebermos o tipo legal que é preenchido quando o agente difunde, sem o consentimento da vítima, uma imagem relativa à intimidade da vida privada nas redes sociais. A vocação humanista e de equilíbrio social do direito penal impeliu-nos a avançar para o tema em discussão, contribuindo para a estruturação de uma reflexão assente em três capítulos. Nas conclusões sugerimos, à luz da jurisprudência e da doutrina, que o crime de VD é um tipo específico impróprio ou impuro e de perigo abstrato que pode criar uma relação de concurso aparente de normas com outros tipos penais, como a devassa da vida privada, p. e p. no art.º. 192.º, nº 1. al. b) ou as gravações e fotografias ilícitas, p. e p. no art.º. 199.º, n.º 2, al. b), do CP, punindo-se o agente pelo crime mais grave, *in casu* a violência doméstica, pois existe uma relação de subsidiariedade entre os tipos legais em concreto.

Palavras-Chave: Internet; violência doméstica; cibercrime; redes sociais; devassa da vida privada.

ABSTRACT

In this paper we intend to contribute to the understanding of the dialectic between the crime of domestic violence and social networks, the legal and penal protection of private life on the internet. To reach this starting point, an argumentative dialogue based on the issues of contemporary criminal law was developed based on the legal method, a logical-deductive reasoning based on the triangulation of Portuguese jurisprudence and the European Court of Human Rights, in the doctrine (national and foreign) and in the ordinary national civil-law and criminal law, with particular emphasis on the Cybercrime Law; alongside the Portuguese Republic Constitution and the European Convention on Human Rights. In this path, several questions of a material nature were analyzed in the light of the device poured in al. b) of no. 2 of article 152 of the CP, in order to understand what legal type is fulfilled when the agent disseminates, without the victim's consent, an image related to the privacy of private life on social networks. The humanist vocation and the social balance of criminal law impelled us to move forward to the topic under discussion, contributing to the structuring of a reflection based on three chapters. In the conclusions we suggest, in the light of jurisprudence and doctrine, that the crime of domestic violence is a specific improper or impure type and of abstract danger that can create a relationship of apparent competition of norms with other criminal types, such as the wanton of private life (art. 192, no. 1, al. b) and illegal recordings and photographs (art. 199, no. 2, al. b), of the Criminal Code, punishing the agent for the most serious crime, as there is a subsidiarity relationship between the specific legal types.

Keywords: Internet; domestic violence; cybercrime; social network; wanton of private life

Sumário: Introdução; 1. Da proteção da intimidade da vida privada; 1.1. À luz da Convenção Europeia dos Direitos Humanos; 1.2. À luz da Constituição da República Portuguesa; 1.3. À luz do direito ordinário nacional; 2. A violência doméstica em Portugal; 2.1. Enquadramento histórico-sociológico; 2.2. Abordagem jurídico-penal da violência doméstica; 2.3. Violência doméstica e operadores da prática jurídica; 3. Violência doméstica, vida privada e internet; 3.1. Internet e crime; 3.2. Violência doméstica e difusão de imagens nas redes sociais; 3.3. Violência doméstica e devassa da vida privada; Conclusão; Referências.

INTRODUÇÃO

É lugar comum referir que vivemos numa sociedade de risco global[1], em rede[2], info-orientada[3], em suma, numa sociedade da informação[4]. As distâncias físicas são uma realidade em revisão porque deixaram de fazer sentido[5] a partir do momento que Marshall McLuhan formulou o conceito de aldeia global e previu uma sociedade tomada pelos meios de comunicação que atuariam por via eletrónica[6]. Hoje as redes de comunicação tornaram a Internet uma realidade omnipresente[7], inclusivamente no espaço doméstico. Anthony Giddens entende que o lar é o lugar mais perigoso nas sociedades modernas, na medida em que há maior probabilidade de uma pessoa ser agredida no interior da sua casa do que na rua[8], desde logo porque a revolução digital pôs em crise os fundamentos da ordem jurídica da era analógica, em especial direitos fundamentais como o direito ao respeito pela vida privada[9],

1 Beck, 2015.
2 Para Castells (2004: 15-16) a rede é um conjunto de nós interligados, formas muito antigas da atividade humana, mas atualmente essas redes ganham uma nova vida, ao converterem-se em redes de informação impulsionadas pela Internet. As redes têm enormes vantagens como ferramentas organizativas, graças à sua flexibilidade e adaptabilidade, caraterísticas fundamentais para prosperar num contexto de mudança permanente. Contudo, atualmente a introdução de novas tecnologias de informação e de comunicação de base informática e, em especial da Internet, permite que as redes desdobrem a sua flexibilidade e adaptabilidade, permitindo a coordenação de tarefas, a gestão da complexidade e o desenvolvimento de uma forma organizacional superior da atividade humana. A este propósito *vide* ainda Castells, 2002.
3 Aguiar, 2017: 44.
4 Pinheiro, 2015: 94-107.
5 Verdelho, 2009b: 410.
6 McLuhan, 1964; Georgiadou, 1995; Leite, 2016: 3.
7 Verdelho, 2009a: 717.
8 Giddens: 2001: 193; Ferreira, 2005: 21.
9 Pereira, 2019: 1469.

realidade particularmente sensível à luz da violência doméstica. Na linha de pensamento de Paulo Sousa Mendes e David Silva Ramalho, verificamos uma deslocação da criminalidade típica do mundo *offline* para o ambiente digital e crimes como a violência doméstica (doravante VD) são cometidos cada vez mais *online* - nas redes sociais, por exemplo -, utilizando o *smartphone* ou outro *device* como instrumentos do crime[10].

É neste quadro que surge o presente estudo, onde procurámos compreender o tipo legal de crime que é preenchido quando o agente difunde, sem o consentimento da vítima, uma imagem relativa à intimidade da vida privada nas redes sociais. Para esse efeito foi analisada a relação entre os operadores do direito, as vítimas e a sociedade, materializada em políticas públicas, como os Planos Nacionais contra a VD que foram emanados desde 1999[11], a par de uma abordagem à evolução do quadro legal da VD e uma análise jurisprudencial quanto aos pressupostos para a materialização deste tipo legal revestido de uma tutela penal especial reforçada, baseada na dignidade humana.

O presente estudo está estruturado em três capítulos: num primeiro momento analisamos a proteção da intimidade da vida privada à luz da Convenção Europeia dos Direitos Humanos (doravante CEDH), da Constituição da República Portuguesa (doravante CRP) e do direito ordinário nacional. No segundo capítulo analisamos o crime de VD, com base numa abordagem histórica e sociológica, seguindo-se uma análise jurídico-penal e a relação entre o objeto de estudo e os operadores do direito. Por fim, no terceiro capítulo, articulamos os conceitos de Internet, crime, VD, difusão de imagens, redes sociais e devassa da vida privada, procurando uma resposta à pergunta de partida. Nas conclusões sugerimos que o crime de VD é um tipo específico impróprio ou impuro e de perigo abstrato que pode criar uma relação de concurso aparente de normas com outros tipos penais, como a devassa da vida privada.

10 Moreira, 2019: 30.

11 I PNCVD (1999-2002) aprovado pela Resolução do Conselho de Ministros n.º 55/99, 15 de junho; II PNCVD (2003-06) aprovado pela RCM n.º 55/99, 15 de junho; III PNCVD (2007-10), aprovado pela RCM n.º 83/2007, 22 de junho; IV PNCVD (2011-13), aprovado pela RCM n.º 100/2010, 17 de dezembro; e V PNCVD (2014-17), aprovado pela RCM n.º 102/2013, 31 de dezembro.

I. DA PROTEÇÃO DA INTIMIDADE DA VIDA PRIVADA

No presente capítulo é desenvolvida uma análise lógico-dedutiva da proteção jurídica dada à intimidade da vida privada, pela CEDH e a CRP, culminando no direito ordinário nacional, o que permite uma visão holística do tema *sub judice*.

1.1. À luz da Convenção Europeia dos Direitos Humanos

O Conselho da Europa foi criado após a Segunda Guerra Mundial[12] com o objetivo de proteger os direitos humanos e as liberdades fundamentais e promover uma maior unidade entre os Estados-membros, materializando a CEDH em 1950, e consagrando no artigo 8.º o direito ao respeito pela vida privada e familiar, incluindo o domicílio e a correspondência, o que significou um progresso, já que a Declaração Universal dos Direitos Humanos (doravante DUDH) reconhecia apenas o direito à reserva da vida privada, constituindo igualmente um avanço ao distinguir a proteção da vida privada da honra, garantindo a proteção jurídica dos dados pessoais, fundada no direito ao respeito pela vida privada proclamado no art. 12.º da DUDH e consagrado no art. 8.º da CEDH. Curiosamente, a CEDH tem uma relevância reforçada em alguns ordenamentos jurídicos: *e.g.* a Constituição Holandesa desempenha um papel limitado na legislação e no processo penal. E isso deve-se ao facto de não existir um tribunal constitucional. Em vez disso, o legislador e os tribunais concentram-se mais na CEDH como o principal instrumento norteador da proteção dos direitos fundamentais[13]. Em 1948 a Assembleia-Geral das Nações Unidas proclamou a DUDH, estabelecendo no art. 10.º que ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra ou reputação[14]. O art. 8.º da CEDH estipula, ainda, nos termos do n.º 2, a legitimidade de ingerências de autoridades públicas no exercício do respeito pela vida privada, sob a condição de serem previstas por lei e desde que sejam necessárias numa sociedade democrática[15], o que coloca em destaque os conceitos de identidade informacional e a proteção de dados pessoais.

A identidade informacional trata-se de um núcleo de direitos relacionados com a identidade pessoal, a proteção de dados pessoais e o desenvolvimento da personalidade[16],

12 Em 1949. A este propósito *vide* Moreira, 2019: 1473.
13 Pereira, 2019: 1456-1457.
14 Pereira, 2019: 1451. Apesar de a CEDH se ter inspirado na DUDH existem diferenças como, por exemplo, o facto de a CEDH estar dotada de obrigatoriedade de um tratado internacional, enquanto que a DUDH não a tem (Moreira, 2019: 1473-1474).
15 Moreira, 2019: 1474; art. 8.º, n.º 2 da CEDH.
16 Pinheiro, 2019: 1438.

direito do indivíduo, enquanto pessoa singular e física, previsto no art. 6.º da DUDH[17]. Contudo, essa proteção teve de ser alargada para o ciberespaço apesar de os autores da CEDH não terem previsto, *a priori*, o impacto que as tecnologias digitais assumiriam na vida privada com o desenvolvimento da informática[18], o que veio a ser mitigado quando a Organização das Nações Unidas votou em 4 de julho de 2018 várias resoluções sobre a promoção, proteção e gozo dos direitos humanos na Internet[19].

A melhor forma de compreender o alcance do artigo 8.º da CEDH, considerada como o mais bem-sucedido sistema para a proteção internacional dos direitos humanos[20], consiste em analisar a riquíssima jurisprudência produzida pelo TEDH[21], que trata a vida privada em articulação com a informação pessoal[22]. A jurisprudência do TEDH vai no sentido de dar razão aos demandantes, invocando a violação do art. 8.º da CEDH, quando se verifica que existiu uma ingerência das autoridades públicas, quando vão para além do necessário para alcançar o objetivo legítimo ou quando essa ingerência não está prevista na lei, cf. o n.º 2 do art. 8.º da CEDH, em linha com o teor vertido no n.º 4 do art. 34.º da CRP[23]. A liberdade de expressão e de informação é outro domínio em que o tribunal tem sido chamado a encontrar um ponto de equilíbrio entre o direito à vida privada e outros direitos fundamentais, em especial no ambiente digital, em paralelo com temas como os poderes de vigilância em massa e a vigilância digital no local de trabalho[24], de forma a garantir este direito e a sua delimitação, enquanto direito que pertence à categoria dos direitos de personalidade[25]. Importa, contudo, saber se as políticas de privacidade das entidades públicas e privadas passam no teste de conformidade com o direito à vida privada nos termos da Convenção, mesmo que sejam certificados por organismos de certificação de dados à luz do Regulamento Geral da Proteção de Dados (doravante RGPD), tendo em consideração o conceito de *interesse legítimo* que pode justificar tratamentos sem o consentimento do titular de dados[26].

17 Veríssimo, 2007: 39.
18 Pereira, 2019: 1451.
19 *UN Human Rights Council (2018), Resolutions on the "Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development"* (Van Der Wilk, 2018: 12).
20 Morrison, 1981 *cit in* Pereira, 2019: 1458.
21 Pinheiro, 2019: 1450. O TEHD é o único tribunal internacional que decide sobre casos concretos mediante queixa apresentada por parte de qualquer pessoa singular, ONG ou grupo de particulares que se considere vítima de violação de direitos humanos, cf. artigo 34.º da CEDH, devendo, estando os Estados-membros obrigados a dar execução às condenações emanadas pelo TEDH (Mendes, 2019: 1058-1059).
22 Pinheiro, 2019: 1439.
23 *E.g.* sentença Carlos Trabajo Rueda contra o Reino de Espanha (30 de maio de 2017); Robathin contra Áustria (3 de outubro de 2012); Ivashchenko contra a Rússia (13 de fevereiro de 2018), todas do TEDH.
24 Pereira, 2019: 1462-1469.
25 Moreira: 2019: 1475.
26 Pereira, 2019: 1470.

1.2. À luz da Constituição da República Portuguesa

A autonomia individual constitui uma expressão, do ponto de vista jurídico, da liberdade pessoal e o reconhecimento da dignidade humana tendo emanações constitucionais como a liberdade de deslocação, de fixação do domicílio, emigração e imigração, de expressão e de informação, religiosa, de ensino, cultural, etc.[27], que vinculam as entidades públicas e privadas[28] pois, nos termos do art. 18.º da Constituição, os preceitos constitucionais respeitantes aos direitos, liberdades e garantias, são diretamente aplicáveis e vinculam as entidades públicas e privadas; e a lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na CRP, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos. Nessa senda, a luta contra a violência doméstica surge como uma decorrência da igual dignidade da pessoa humana[29] prevista no art. 1.º da CRP, sendo a pessoa humana um *prius*, em qualquer dos géneros, masculino ou feminino[30], eliminando-se desigualdades do passado[31].

O direito ao respeito pela vida privada integra o catálogo constitucional de direitos e liberdades fundamentais. Os instrumentos internacionais que consagram o direito à vida privada consideram-se abrangidos pela cláusula geral de receção automática prevista no art. 8.º, n.º 1 da CRP[32]. O art. 34.º da CRP, à semelhança do disposto no art. 10.º da Constituição alemã, garante a inviolabilidade do domicílio e da correspondência, uma das formas de tutela do direito à reserva da vida privada, consagrado no art. 26.º da CRP[33], garantindo que qualquer pessoa que estabeleça uma comunicação, tenha a segurança que esta permanece fechada no circuito dos sujeitos da relação comunicacional, proibindo-se ingerências por parte de autoridades públicas ou entidades privadas[34]. O art. 26.°, n.º 1, da CRP, sede do direito geral de personalidade e expressão direta do postulado da dignidade humana vertido no art. 1.º da Constituição, assegura que a todos são reconhecidos os direitos à identidade pessoal[35], ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom

27 González, 2019: 1420-1421.
28 Pinto, 2005: 75-76 *cit in* Pereira, 2019: 1454.
29 A igualdade vertida no art. 13.º da CRP é a igualdade perante a (*na*) lei, dita por vezes igualmente jurídico-formal (Miranda e Medeiros, 2005: 120-124).
30 Miranda e Medeiros, 2005: 53-55.
31 Pereira, 2005: 18.
32 Miranda e Medeiros, 2005: 88; Canotilho e Moreira, 2007: 254.
33 Segundo Miranda e Medeiros o sentido de domicílio é muito mais amplo do que o conceito civilístico (arts. 82.º a 88.º do CC), abrangendo todo o local em que a pessoa habita, quer se trate de residência ou local de trabalho, habitual ou ocasional, permanente ou eventual, estável ou precário (Miranda e Medeiros, 2005: 372).
34 Aguiar, 2017: 48.
35 Miranda e Medeiros, 2005: 282-285.

nome e reputação, à imagem[36], à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação, consagrando o direito à identidade pessoal, abrangendo, além do direito ao nome, um direito à historicidade pessoal[37]. Consagra, assim, o direito de reserva da intimidade na vida privada e familiar, um dos que tem maior alcance prático e com maior índice de conflitualidade possível de antecipar com base nas normas que se referem à inviolabilidade do domicílio e da correspondência (art. 34.º), à liberdade de expressão e comunicação (arts. 37.º e 38.º), ao direito de informação e ao princípio do *arquivo aberto* da administração (art. 268.º, n.ºs 1 e 2) e a atuação da polícia (art. 272.º, n.º 2), *máxime* os problemas que se levantam quando a realização da justiça exige uma intromissão na reserva da intimidade da vida privada[38].

A preocupação com a privacidade dos cidadãos espelhou-se na versão original da CRP de 1976 que, no seu artigo 35.º, consagrou a proteção de pessoas contra o tratamento informático de dados pessoais, reconhecendo o direito à proibição do tratamento informático de certos tipos de dados pessoais; o direito ao conhecimento e acesso das pessoas aos seus próprios dados pessoais integrados em registos informáticos; e a proibição de atribuição de um número nacional único aos cidadãos. As quatro revisões constitucionais que se seguiram ampliaram a extensão deste artigo, quanto à proibição da interconexão de dados pessoais informatizados e seu acesso por terceiros[39]. No art. 35.º da CRP está consagrada a proteção dos dados pessoais, podendo ser classificado como um especial direito de personalidade, uma vez que tem o objetivo de proteger o cidadão dos perigos que o uso da informática pode causar em sua privacidade[40]. Assim, tem de existir consentimento do titular dos dados para utilização pela informática, prevenindo o tratamento abusivo de dados informáticos de natureza pessoal, ou seja, aqueles que dizem respeito ao cidadão, conceito abrangente à semelhança da definição vertida na Lei da Proteção de Dados Pessoais[41], atual Lei n.º 58/2019, de 8 agosto.

1.3. À luz do direito ordinário interno

O Código Civil consagra, desde 1966, enquanto direito especial de personalidade, a reserva sobre a intimidade da vida privada no artigo 80.º[42], facto que nos remete ao artigo *The*

36 O direito à imagem é uma expressão típica da autonomia e da identidade pessoal, um direito à autodeterminação exterior, contrariada pela jurisprudência apenas em determinadas circunstâncias (Miranda e Medeiros, 2005: 289-290).
37 Canotilho e Moreira, 2007: 462.
38 Miranda e Medeiros, 2005: 290-295.
39 Venâncio, 2011: 13.
40 Sawaris, 2017: 128.
41 Miranda e Medeiros, 2005: 379.
42 Pereira, 2019: 1457.

right to privacy (1890), que conduziu ao reconhecimento do direito à privacidade na generalidade dos sistemas jurídicos europeus[43]. Contudo, no nosso ordenamento jurídico o sentido do direito à privacidade não corresponde ao conceito anglo-saxónico enquanto *right to be let alone*[44]. Ao contrário do *right to privacy*, o direito à reserva da intimidade da vida privada surge como um direito que considera que a pessoa representa *convivência e solidariedade*[45].

Este direito especial tem servido de base para o debate moderno quanto a quem caberá o domínio do corpo humano[46]. Sabemos que o nascimento completo e com vida marca o início da existência jurídica (art. 66.º, n.º do Código Civil, doravante CC) e cessa com a morte (art. 68.º, n.º 1 do CC). Mas será concebível um senhorio sobre o corpo humano, ou partes que dele hajam sido destacadas, no sentido definido pelo art. 1305.º do CC?[47]. De acordo com a doutrina portuguesa a autodeterminação implica todas as possibilidades de *facere*, de uma liberdade comunicacional, sem nunca perder a defesa contra a intrusão indevida na esfera da personalidade do indivíduo[48]. É verdade que, se a personalidade do ser humano cessa com a sua morte (art. 68.º do CC), e tendo em conta que, juridicamente, o que não for pessoa só pode ser objeto, o cadáver tem a natureza de *res*; e, por isso, é possível doar o corpo, para estudo, às faculdades de medicina. Daqui resulta que cada pessoa exerce uma autoridade sobre o seu corpo e que ela se apresenta como um pressuposto de diversas manifestações (*v.g.*, integridade pessoal, imagem, voz, saúde, liberdade de movimentação, etc.)[49].

A Lei n.º 44/2018, de 9 de agosto, procedeu à 46.ª alteração ao Código Penal (doravante CP), e veio reforçar a proteção jurídico-penal da intimidade da vida privada na internet quando passou a punir com pena de prisão de dois a cinco anos o agente que difundir através da internet ou de outros meios de difusão pública generalizada, dados pessoais, designadamente imagem ou som, relativos à intimidade da vida privada de uma vítima sem o seu consentimento, cf. a al. b), n.º 2 do art. 152.º do CP. Acresce que, quem, sem consentimento e com intenção de devassar a vida privada de uma pessoa, designadamente a intimidade da vida familiar ou sexual, divulgar imagem das pessoas ou de objetos ou espaços íntimos, incorre no crime de devassa da vida privada p. e p. pelo art. 192.º do CP, o que suscita dúvidas relativamente ao alcance do dispositivo vertido no art. 152.º do CP, *máxime* o tipo

43 Na *Harvard Law Review* cf. Warren e Brandeis, 1890: 193-220.
44 Ascensão, 1996: 118-121.
45 Aguiar, 2017: 45.
46 González, 2019: 1390.
47 González, 2019: 1391.
48 Pinheiro, 2019: 1439.
49 González, 2019: 1406-1421.

legal preenchido com a difusão de imagens sem consentimento, nas redes sociais, relativas à intimidade. Em 2018 o legislador agravou as penas de prisão para quem divulgasse na Internet imagens ou vídeos da intimidade de outras pessoas sem a autorização destas, designada como pornografia de vingança.

O CP já previa penas pela devassa da vida privada ou pela divulgação de imagens ou gravações sem autorização, mas passou a incluir a referência ao meio (internet). E se essa difusão for feita num quadro de VD a pena de prisão prevista é agravada para um mínimo de dois anos até aos cinco anos. O que significa que ficaram abrangidas as imagens e vídeos da intimidade de cônjuges ou ex-cônjuges, de pessoas com quem o agressor mantenha (ou tenha mantido) relação amorosa, do pai ou mãe dos filhos, e de pessoas particularmente indefesas que com ele coabitem (em função da idade, deficiência, saúde, gravidez ou dependência económica). Importa, ainda, referir que a Lei do Cibercrime considera como crime informático só aquele que é praticado para atingir bens, sistemas ou dados informáticos, e não aquele que é praticado por meios informáticos, como a devassa por meio de informática, p. e p. no art. 193.º do CP.

II. A VIOLÊNCIA DOMÉSTICA EM PORTUGAL

2.1. Enquadramento histórico-sociológico

Uma abordagem holística do objeto *sub judice* conduz-nos a uma análise histórica e sociológica para compreender a evolução do ordenamento jurídico português, porque a visão jurídica não representa, tipicamente, mais do que a simples transposição da perspetiva social[50], uma proteção de valores considerados essenciais numa determinada comunidade histórico-socialmente enquadrada[51].

No pós-25 de abril de 1974 a mulher ascendeu à condição de cidadã de pleno direito e no reconhecimento legal de iguais direitos, comparativamente ao homem[52]. Até aos anos 80 do séc. XX vivíamos numa sociedade patriarcal, em que a mulher passava do domínio do pai para o domínio do marido, em que o bem superior da família e dos filhos justificava a continuidade dos casamentos numa sociedade profundamente católica, em que a Igreja não admitia o divórcio[53].

No entanto importa não confundir a violência contra as mulheres com a VD, a violência conjugal e os maus tratos[54]. Nelson Lourenço[55] já referia, antes da Reforma Penal de 2007, que se falava com uma excessiva sobreposição em relação a duas realidades distintas: a violência doméstica e a violência contra a mulher (*máxime* a violência conjugal[56] e a violência de género com uma prevalência de vitimização no género feminino[57]), defendendo que a violência doméstica é uma realidade mais vasta do que a violência contra a mulher e que há outras dimensões que têm sido descuradas no âmbito das políticas sociais, como a violência contra as crianças, os idosos e os deficientes[58]. Para Giddens a VD é um abuso físico de um membro da família em relação a outros membros[59], a expressão da falta de interiorização dos direitos fundamentais no seio das relações familiares e interpessoais do tipo privado[60], que envolve, geralmente, mais do que uma forma de violência: emocional, psicológica, sexual,

50 González, 2019: 1408.
51 Costa, 2007b: 68-69.
52 Ferreira, 2005: 43.
53 Ferreira, 2005: 29. Para aprofundamento sociológico da influência da Igreja Católica no Direito Penal oitocentista *vide* Poiares e Dias, 2019d: 311-329.
54 CEJ, 2016: 21.
55 Professor catedrático jubilado da Universidade Nova de Lisboa.
56 Ferreira, 2005: 217.
57 Leite: 2020: 32-35.
58 Lourenço, 2005: 27.
59 Giddens, 2009: 196.
60 Palma, 2019: 55.

física, social e económica[61]. A VD, em especial o espancamento da mulher é, segundo a ONU (2000), a forma mais generalizada de violência contra as mulheres e, em diversos países, 20% das mulheres foram vítimas de maus tratos por parte dos homens com quem vivem[62].

Mas, apesar de todo o esforço de prevenção e combate a este problema social, os direitos humanos continuam a estar em causa em vários pontos do planeta, desde logo devido às fragilidades dos ordenamentos jurídicos face à realidade tecnológica, verificando-se uma desconsideração pela dignidade humana em quase todos os países[63], com elevados custos sociais e económicos (*e.g.*, a probabilidade dos filhos adoecerem entre as mulheres vítimas é 90% maior do que nas não vítimas; e a probabilidade de haver dificuldades em arranjar emprego é 70% maior nas primeiras, assim como 103% a procura de psicólogos ou psiquiatras[64]).

A isto acrescem alguns preconceitos e mitos, enraizados na nossa sociedade, que continuam a dificultar a denúncia de situações de VD e a dificultar a intervenção neste domínio[65]. O preconceito e o estigma dirigido, *v.g.*, às pessoas LGBTIQAP+[66] é ainda uma realidade transversal na sociedade portuguesa. Continuam a persistir oposições de estigmatização ou discriminação, assim como preconceitos e desinformação sobre a homossexualidade, bissexualidade e transexualidade, com consequências que podem afetar a prática profissional em diversos domínios, incluindo no apoio a vítimas de violência doméstica[67].

Para as vítimas de VD, as respostas da polícia (*v.g.*, atendimento, aconselhamento, mediação, detenção) revestem-se de grande simbolismo, pois podem revelar o nível de tolerância social relativamente a uma conduta, considerando-a como criminosa ou não, justificando uma atuação em conformidade[68]. Por isso, a intervenção neste âmbito exige uma articulação entre as componentes jurídica, policial, logística, económica, saúde, educação, social e cultural[69], obrigando uma formação interdisciplinar não só dos polícias, mas também dos procuradores, juízes e técnicos de intervenção social[70]. Nessa senda, foram emanados recentemente (maio de 2020) novos instrumentos de combate à VD, como o manual de

61 CEJ, 2016: 31-33.
62 CEJ, 2016: 24.
63 Tomar e Dwivedi, 2014.
64 Lisboa, 2005: 48-49; AA.VV., 2003; Moura, 2016.
65 CEJ, 2016: 34-36.
66 Sigla para Lésbicas, Gays, Bissexuais, Travestis, Transsexuais, *Queer*/Questionando, Intersexo, Assexuais, Pan/Poli e mais.
67 AA.VV., 2016: 11-12; ILGA Portugal 2015.
68 Brown, 1984; Gracia, 2004; Holder, 2001 cit. in Sani e Morais, 2015: 7; Poiares, 2014 e 2019a.
69 Lisboa, 2005: 9.
70 Palma: 2019: 56; Poiares, 2014 e 2019a; Sani e Morais, 2015.

atuação funcional a adotar pelos OPC nas 72 horas subsequentes à apresentação de denúncia por maus-tratos em contexto de VD; um guia de Intervenção integrada junto de crianças ou jovens vítimas de VD; um plano anual de formação conjunta e um guia de requisitos mínimos para programas e projetos de prevenção primária para a violência contra as mulheres e VD[71].

2.2. Abordagem jurídico-penal da violência doméstica

A ressonância que o CP adquire no seio da comunidade advém-lhe do impacto que a Parte Especial provoca na consciência coletiva[72], apresentando, no domínio da VD, uma proteção jus-social, na medida em que as necessidades do sistema social levam a solicitar aos tribunais, ao Ministério Público (doravante MP) e às polícias, uma intervenção social de cariz misto, *i.e.*, apoio social e comunicação da autoridade do Estado[73].

O atual CP Português, aprovado na sua versão original pelo Decreto-Lei n.º 400/82, de 3 de setembro, introduziu o crime de "Maus-tratos ou sobrecarga de menores e de subordinados ou entre cônjuges", constituindo a primeira designação mais aproximada do tipo previsto no art. 152.º em vigor. Foi Eduardo Correia quem propôs a autonomização do crime de maus tratos nos artigos 166.º e 167.º do Projeto do CP sem, no entanto, prever os maus tratos entre cônjuges, ilícito que veio a ser introduzido na redação do CP pela Comissão Revisora, ficando a constar do n.º 3 do art. 153.º[74]. Em 1995, o CP, através do Decreto-Lei n.º 48/95, de 15 de março, passou a prever a aplicação de pena de prisão aos crimes de maus-tratos físicos ou psíquicos infligidos pelo cônjuge ou quem com ele conviver em condições análogas às dos cônjuges no crime designado de "Maus-tratos ou sobrecarga de menores, de incapazes ou do cônjuge". Com a Lei n.º 7/2000, de 27 de maio, que procede à quinta alteração do Decreto-Lei acima mencionado, alterou a natureza do crime, agora denominado de "Maus-tratos e infração de regras de segurança", para pública, passando a prever o alargamento ao progenitor de ascendente comum em 1.º grau[75]. A modificação da natureza do crime permitiu ao Estado acionar a ação penal sem o consentimento da vítima. A partir deste momento, de acordo com o artigo 244.º do Código de Processo Penal (doravante CPP), qualquer pessoa que tenha conhecimento do crime, pode denunciá-lo ao MP, a outra autoridade judiciária ou aos Órgãos de Polícia Criminal (doravante OPC), sendo a denúncia do crime obrigatória para as entidades policiais e para os funcionários, na aceção do artigo

71 XXII Governo Constitucional, 2020a, 2020b, 2020c e 2020d.
72 Costa, 2007a: 13.
73 Palma: 2019: 56.
74 Nunes e Mota, 2010: 133.
75 Morais, 2019: 38.

386.º do CP, se tomarem conhecimento do crime no exercício das suas funções e por causa delas, sendo que o MP tem legitimidade para promover o processo penal, independentemente da vontade da vítima, de acordo com o art. 48.º do CPP[76]. Ao constituir-se como crime público é dado mais um passo no reconhecimento da importância deste problema social, intensificando-se a ação do Estado na esfera privada da família, adquirindo outra visibilidade[77].

Em 2007 ocorreu a décima quinta alteração ao CPP e foram reforçadas as medidas de proteção da vítima[78] e, com a reforma penal introduzida pela Lei n.º 59/2007, de 4 de setembro, a epígrafe do artigo 152.º passou a designar-se violência doméstica. Este crime corresponde a qualquer ato, conduta ou omissão que sirva para infligir, de modo reiterado ou não, sofrimentos físicos, sexuais, mentais ou económicos, de modo direto ou indireto (*v.g.* castigos corporais, privações da liberdade e ofensas sexuais), a qualquer pessoa que habite no mesmo agregado doméstico privado. O arguido, ainda que não habite no mesmo agregado doméstico privado que a vítima, passa a ser punido se infligir os maus-tratos a cônjuge ou ex-cônjuge, a pessoa que mantenha ou tenha mantido uma relação de namoro ou análoga à dos cônjuges e a progenitor de descendente comum em 1.º grau. Relativamente às pessoas particularmente indefesas, em razão da idade, deficiência, doença, gravidez ou dependência económica, estas têm de coabitar com o mesmo de acordo com a al. d), n.º 1, do art. 152.º do CP. As relações de namoro ou relações análogas às dos cônjuges, foram incluídas em 2013, com a 29.ª alteração ao CP, por força da Lei n.º 19/2013, de 21 de fevereiro. A 45.ª alteração ao CP, aprovada pela Lei n.º 16/2018, de 27 de março, passou a integrar na previsão de qualificação do homicídio os crimes cometidos no âmbito de uma relação de namoro.

Foram ainda emanados diversos diplomas e diretivas, como a Lei n.º 61/91, de 13 de agosto, que reforçou a proteção legal das vítimas, ou os Planos Nacionais contra a VD[79], onde os conselhos municipais de segurança também assumiram a prevenção da VD[80]. A Lei n.º 130/2015 de 4 de setembro procedeu à vigésima terceira alteração ao CPP e aprovou o

76 Lemos, 2019.
77 Lourenço e Carvalho, 2000: 58; Poiares, 2020.
78 Mendes, 2018: 41-43.
79 I Plano Nacional contra a Violência Doméstica (doravante PNCVD) - 1999-2002, aprovado pela Resolução do Conselho de Ministros (doravante RCM) n.º 55/99, de 15 de junho; II PNCVD (2003-06) aprovado pela RCM n.º 55/99, de 15 de junho; III PNCVD (2007-10), aprovado pela RCM n.º 83/2007, de 22 de junho; IV PNCVD (2011-13), aprovado pela RCM n.º 100/2010, 17 de dezembro; V PNCVD (2014-17), aprovado pela RCM n.º 102/2013, de 31 de dezembro.
80 Lei n.º 33/98, de 18 de julho, alterada pelo Decreto-Lei n.º 32/2019, de 4 de março, em conjugação com Decreto-Lei n.º 101/2018, de 29 de novembro.

Estatuto da Vítima[81], transpondo a Diretiva 2012/29/UE do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, que estabelece normas relativas aos direitos, ao apoio e à proteção das vítimas da criminalidade e que substitui a Decisão-Quadro 2001/220/JAI do Conselho, de 15 de março de 2001. Mais recentemente, a Lei de Política Criminal para o biénio de 2017-2019, identificou a VD como um fenómeno criminal de prevenção prioritária[82], estando em vigor um ciclo programático alinhado com a Agenda 2018-2030 para o Desenvolvimento Sustentável (ONU), assente em três planos nacionais de ação, com objetivos em matéria de igualdade entre mulheres e homens, prevenção e combate à violência contra as mulheres e VD e combate à discriminação em razão da orientação sexual, identidade de género e características sexuais[83]. Em 2019 a PGR estabeleceu procedimentos uniformizadores a observar pelo MP na área da violência doméstica, através da Diretiva n.º 5/2019, de 4 de dezembro.

Este esforço concertado visa, em primeira linha, a prevenção especial e a proteção das vítimas[84] que desconhecem a dimensão criminal dos atos exercidos contra si e os seus direitos ou não se identificam como vítimas e não procuram ajuda[85]. No domínio do cibercrime, o silêncio prende-se, por vezes, com o desconhecimento do sujeito passivo, de que foi alvo de um ataque, ou simplesmente a descrença na investigação policial e o sentimento de impunidade destes crimes[86]. Acresce que muitas vítimas e, por vezes, os operadores do direito, desconhecem o alcance do conceito de VD, inclusive quanto aos factos que preenchem o tipo legal[87].

O bem jurídico protegido pelo crime de VD é plural e complexo, visando a defesa da integridade pessoal, nas suas vertentes física, psíquica e mental, e a proteção da dignidade humana no âmbito de uma relação interpessoal. Embora o tipo legal abranja ações típicas que já encontram previsão noutros tipos legais, o seu fundamento deve ser encontrado na proteção de quem, no âmbito de uma relação interpessoal, vê a sua integridade pessoal, liberdade e segurança ameaçadas com tais condutas, sendo o enfoque colocado na situação relacional existente entre agressor e vítima. O verdadeiro traço distintivo deste crime relativamente aos

81 Nos termos do artigo 1.º o Estatuto da Vítima contém um conjunto de medidas que visam assegurar a proteção e a promoção dos direitos das vítimas da criminalidade, transpondo para a ordem jurídica interna a Diretiva 2012/29/EU do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, que estabelece normas relativas aos direitos, ao apoio e à proteção das vítimas da criminalidade e que substitui a Decisão-Quadro 2001/220/JAI do Conselho, de 15 de março de 2001.
82 Cf. al. f) do art. 2.º da Lei n.º 96/2017, de 23 de agosto.
83 *In* https://nacoesunidas.org/pos2015/agenda2030/ (consultado em 11.06.2020).
84 Palma, 2019: 54.
85 CEJ, 2016: 43.
86 Aguiar, 2017: 25.
87 Poiares, 2014, 2020.

demais onde igualmente se protege a integridade física, a honra ou a liberdade sexual, reside no facto de o tipo legal prever e punir condutas perpetradas por quem afirme e atue um domínio sobre a vítima, sobre a sua vida, sobre a sua honra ou(e) sobre a sua liberdade e que a reconduz a uma vivência de medo, de subjugação[88]; é um crime de resultado que pode ser cometido por omissão, traduzida na não prestação dos cuidados necessários de que a vítima carece e que leva à verificação do resultado típico (infligir maus tratos) e é um crime de perigo abstrato pois é a própria ação em si que é considerada perigosa, considerando-se apta a produzir efeitos danosos, mas não é necessário que esse perigo se materialize, já que não está previsto como efeito da ação típica. Assim, o bem jurídico protegido pela incriminação abrange o bem-estar necessário à vida pessoal, traduzido na manutenção de um ambiente propício a um salutar e digno modo de vida[89]. A delimitação dos casos de VD daqueles em que a ação apenas preenche a previsão de outros tipos de crime, como a ofensa à integridade física, a injúria, a ameaça ou o sequestro, deve fazer-se com recurso ao conceito de maus tratos quando, em face do comportamento demonstrado, for possível formular o juízo de que o agente manifestou desejo de humilhar ou especial desconsideração pela vítima[90].

Até ao ano de 2007 a tipificação do crime de VD pressupunha, no entendimento da maioria da jurisprudência, uma conduta reiterada por parte do agente, algo que passou a ser irrelevante face à nova letra do art. 152.º do CP. No entanto, a jurisprudência mais recente tem demonstrado que nem todo o ato singular pode ser enquadrado como VD, por não ser atendível como uma ofensa à dignidade humana, o que tem suscitado dúvidas nos mandatos profissionais, desde logo aquando da atuação policial que, face à incapacidade de objetivar legalmente determinados comportamentos jurídico-penais, tendem a tipificar os mesmos como VD, ainda que, mais tarde, o MP venha a ter entendimento diverso[91]. Face à nova redação dada ao artigo 152.º, n.º 1, o crime pode ser cometido mesmo que não haja reiteração de condutas, embora só em situações excecionais o comportamento violento único, pela gravidade intrínseca do mesmo, preencha o tipo de ilícito[92]. É assim um problema controverso, o de saber se em ordem de afirmarmos que estamos perante a VD devemos

88 *In* Acórdão de 4 de junho de 2018 do TRG, proc.º n.º 121/15.5GAVFL.G1.
89 *In* Acórdão de 12 de outubro de 2016 do TRP, proc.º n.º 2255/15.7T9PRT.P1.
90 *In* Acórdão de 15 de outubro de 2012 do TRG, proc.º n.º 639/08.6GBFLG.G1.
91 Estas dúvidas são partilhadas pelo MP, como se depreende do ponto 4 da diretiva da PGR n.º 5/2019, de 4 de dezembro, que refere o seguinte: sempre que, aquando do registo de inquérito, se suscita dúvida quanto à qualificação como violência doméstica da factualidade subjacente, deve aquela prevalecer, mantendo-se a mesma até ao momento em que seja inequívoco enquadramento diverso.
92 *In* Acórdão de 24 de abril de 2006 do STJ, proc.º n.º 06P975; e Ferreira, 2005: 106-107.

atender à sazonalidade ou repetição no desenvolvimento de condutas violentas por parte do agressor[93].

O critério da reiteração deu lugar a uma divergência doutrinária e jurisprudencial[94], aspeto juridicamente relevante quando estamos perante um comportamento isolado à luz do crime de devassa da vida privada nas redes sociais. O segmento *de modo reiterado ou não* introduzido no n.º 1 do art. 152.º do CP, é unívoco no sentido de que pode bastar só um comportamento para a condenação[95], pois visa proteger, não apenas a saúde mas a integridade pessoal, prevista no art. 25.º da CRP[96], ligado à defesa da dignidade da pessoa humana. O crime de VD não exige a prática reiterada dos atos objetivos previstos no mesmo por parte do agente, mas exige que os mesmos se traduzam na humilhação da vítima ou numa especial desconsideração pela mesma[97], ou seja, admite-se, que basta um singular comportamento para integrar o crime quando assuma uma dimensão manifestamente ofensiva da dignidade pessoal do cônjuge[98] se um único ato ofensivo se revelar de tal modo intenso que ao nível do desvalor (quer da ação quer do resultado) seja apto a lesar em grau elevado o bem jurídico pondo em causa a dignidade da pessoa humana[99]. O crime de VD exige, assim, que alguém, de modo reiterado ou não, inflija maus tratos no âmbito de um relacionamento conjugal, ou análogo, e que, por força das lesões verificadas, se entenda que tenha ofendido a dignidade da vítima[100].

A *pedra de toque* da distinção entre o tipo legal de VD e os tipos de crime que especificamente tutelam os bens pessoais nele visados concretiza-se pela apreciação de que a conduta constitui um atentado à dignidade pessoal aí protegida[101], pois tutela-se, não a comunidade familiar e conjugal, mas sim a pessoa individual na sua dignidade humana, abarcando, por isso, os comportamentos que lesam a dignidade da vítima. O que releva é saber se a conduta do agente é suscetível de se classificar como maus tratos, o que se deverá concluir quando for possível formular o juízo de que o agente manifestou desprezo, desejo de humilhar, ou especial desconsideração pela vítima[102]. Com a Reforma de 1995, os maus tratos psíquicos passaram a estar contemplados com um leque mais alargado de condutas, como humilhações, provocações, ameaças, insultos, privações ou limitações arbitrárias da liberdade

93 Ferreira, 2005: 26; Poiares, 2020.
94 Cruz, 2017: 81; Poiares, 2020.
95 *In* Acórdão de 20 de janeiro de 2015 do TRE, proc.º n.º 228/13.3TASTR.E1.
96 Nos termos do n.º 1 do art.º 25.º da CRP, a integridade moral e física dos cidadãos é inviolável.
97 *In* Acórdão de 1 de junho 2017 do TRL, proc.º n.º 3/16.0PAPST.L1-9.
98 *In* Acórdão de 10 de setembro de 2012 do TRG, proc.º n.º 1011/11.6GBBCL.G1.
99 *In* Acórdão de 10 de setembro de 2014 do TRP, proc.º n.º 648/12.0PIVNG.P1.
100 *In* Acórdão de 29 de janeiro de 2014 do TRC, proc.º n.º 1290/12.1PBAVR.C1.
101 *In* Acórdão de 3 de julho de 2012 do TRE, proc.º n.º 53/10.3GDFTR.E1.
102 *In* Acórdão de 8 de maio de 2017 do TRG, proc.º n.º 669//16.4JABRG.G1

de movimentos, ou seja, condutas que revelam desprezo pela condição humana do parceiro, podendo provocar sentimentos de culpa ou de fraqueza mas não, necessariamente, um sofrimento psicológico. O relevante é que os maus-tratos psíquicos estejam associados à posição de controlo ou de dominação que o agressor pretenda exercer sobre a vítima, de que decorre uma maior vulnerabilidade desta[103].

O crime de VD visa proteger muito mais do que a soma dos diversos ilícitos típicos que o podem preencher, como ofensas à integridade física, injúrias ou ameaças. Está em causa a dignidade humana da vítima, a sua saúde física e psíquica, a sua liberdade de determinação, que são ofendidas, não apenas através de ofensas, ameaças ou injúrias, mas através de um clima de medo, angústia, insegurança e humilhação. O bem jurídico tutelado com a incriminação das condutas abrangidas no n.º 2 do art.º 152.º CP, é diferente daqueles que são protegidos por outras incriminações que a conduta do agente pode, eventualmente, também ter preenchido, como a integridade física e diferentes dimensões da liberdade. Integram o crime de VD todas as condutas do agente que, revestindo-se da gravidade prevista na descrição do artigo 152.º do CP, não a excedem de forma particular, de modo a permitir destacar uma ou mais das ações integradoras daquele ilícito penal para efeitos de punição autónoma. Consequentemente, tendo o crime de VD agravado, p. e p. pelo art. 152.º, n.ºs 1, al. a), e 2, do CP, um âmbito de proteção mais abrangente do que o de coação, ocorre entre ambos uma relação de concurso aparente, sendo o segundo ilícito consumido pelo primeiro[104].

Existem ainda outros factos enquadráveis no tipo legal *sub judice*: *e.g.*, o agente, casado com outra mulher, com quem vive, mas que mantém, paralelamente, um relacionamento amoroso com a vítima, ainda que sem coabitação, consubstancia com esta uma relação análoga à dos cônjuges e por essa razão suscetível de integrar o núcleo das vítimas de VD[105]. Nos factos integradores do crime de VD e de violação, entre cônjuges e, apesar dos factos integradores deste último revestirem autonomia, indo para além do ambiente de VD até aí existente, existe uma relação de subsidiariedade entre ambos, devendo o agente ser punido, pelo crime de violação, por ser o mais grave[106]. O mesmo sucede numa relação de namoro que, no âmbito da VD, não abrange uma relação de natureza exclusivamente sexual. A prática de atos sexuais, mantidos apenas sob violência e ameaça, depois de haver terminado uma

103 *In* Acórdão de 29 de fevereiro de 2012 do TRP, proc.º n.º 368/09.3PQPRT.P1.
104 *In* Acórdão de 6 de fevereiro de 2017 do TRG, proc.º n.º 201/16.06GBBCL.G1; Ac. de 27 de fevereiro de 2008 do TRL, proc. n.º 1702/2008-3; Ac. de 10 de julho de 2014 do TRG, proc.º n.º 591/11.0PBGMR-G1; Acórdão de 10 de janeiro de 2018 do TRC, proc.º n.º 1641/16.0T9VIS.C1; Morais, 2019: 37-55.
105 *In* Acórdão de 27 de fevereiro de 2013 do TRC, proc.º n.º 83/12.0GCGRD.C1; Acórdão de 7 de julho de 2016 do TRP, proc. n.º 18/15.9GAPRD.P1.
106 *In* Acórdão de 27 de setembro de 2017 do TRP, proc.º n.º 1342/16.9JAPRT.

relação extraconjugal, integra apenas o crime de violação do art.º 164.º, n.º 1, al. a) do CP[107]. O alargamento da punição prevista no art. 152.º do CP aos casos em que o crime é praticado por agente que tenha mantido com a vítima relação de namoro, visa a proteção das vítimas contra atos de violência contrários à confiança num comportamento de respeito e abstenção de atos violadores da integridade pessoal do ex-parceiro, incluindo as vítimas de *stalking*, quando um ex-namorado perturba a paz do ex-parceiro[108], cabendo assim, no crime de VD, as condutas e comportamentos que causam, inclusive através do envio de SMS, maus tratos configurados como *stalking*[109].

2.3. Violência doméstica e operadores da prática jurídica

Nesta secção pretendemos refletir sobre o papel dos operadores da prática jurídica (procuradores, juízes, polícias, etc.) no quadro da violência doméstica, sobretudo o seu contributo para o reforço da confiança das vítimas no sistema judicial e policial. Portugal aderiu, desde o final da Segunda Guerra Mundial, a diversos instrumentos de direito internacional, no domínio da defesa dos direitos humanos e de combate à violência contra as mulheres[110]. Desde então, em particular a partir do fim do séc. XX, verificou-se um investimento na formação dos polícias, magistrados e técnicos sociais na perspetiva de desenvolver, de forma concertada, a estratégia nacional contra a VD.

No entanto diversos estudos demonstram que existe um longo caminho a percorrer no campo da formação e na mudança de mentalidades. As atitudes e respostas dos magistrados e dos polícias desempenham um papel importante e contribuem para a satisfação da vítima, cooperando na garantia da sua segurança, fornecendo informação, aconselhamento, suporte e encaminhamento à vítima de violência, ou seja promovendo, a capacitação da vítima para lidar com as situações que motivaram a denúncia[111]. Mas este problema não é apenas português. Nos EUA estima-se que as mulheres relatam à polícia entre 25% a 50% dos ataques que são vítimas, e os homens ainda menos[112]. As mulheres sobreviventes de abusos infligidos por parceiros íntimos encontram ceticismo ou descrença no seu esforço para obter justiça por parte dos diversos operadores do sistema. As suas histórias de abuso são menos valorizadas do que outros tipos legais internamente mais coerentes. Mas a VD, por vezes,

107 *In* Acórdão de 14 de junho de 2017 do TRP, proc.º n.º 16/16.5GAAGD.P1.
108 *In* Acórdão de 26 de setembro de 2017 do TRE, proc.º n.º 518/14.8PCSTB.E1.
109 *In* Acórdão de 8 de outubro de 2014 do TRP, proc.º n.º 956/10.5PJPRT.P1.; Acórdão de 1 de outubro de 2013 do TRE, proc.º n.º 258/11.0GAOLH.E1.
110 Ferreira, 2005: 219.
111 Sani e Morais, 2015: 16; Poiares, 2014 e 2019a.
112 Sampson, 2013: 5-6.

resulta em problemas psicológicos, que podem afetar a memória de uma vítima, culminando numa história sem consistência e pouco plausível. As mulheres sofrem com os estereótipos e a tendência cultural de descrer nas mulheres simplesmente porque são mulheres[113].

Por outro lado, as vítimas que tentam fugir dos agressores procuram frequentemente relocalizar-se em espaços confidenciais (*e.g.* casas-abrigo), alterando o seu nome, morada e identidade para dar início a uma vida sem violência. Mas ajudar essas vítimas representa um problema legal, em particular o conflito entre manter registos e informações acessíveis ao público e permitir endereços e registos confidenciais para vítimas de VD que temem ser encontradas pelo agressor[114], o que reforça a desconfiança das vítimas em relação aos tribunais. Alguns estudos revelam que nos EUA cerca de 60% das ordens judiciais de proteção são violadas pelos agressores anualmente; e aproximadamente 70% das vítimas de VD são assassinadas pelos agressores que estavam sob uma medida de proteção do tribunal. Assim, a principal preocupação nos tribunais diz respeito à privacidade dos dados das vítimas de VD face ao arguido que tem acesso a informação que nem este, nem o público, deviam ter acesso[115]. Em Portugal, não raras vezes, os agressores têm conhecimento da localização das vítimas (*e.g.* em casas-abrigo), o que, por vezes, se deve ao facto de decorrerem processos em simultâneo nos tribunais judiciais e nos tribunais de família e menores e não se garantir em plenitude a segurança da informação.

Alguns autores defendem a institucionalização de tribunais específicos e juízes com formação especializada para julgar os crimes desta natureza, conferindo essa competência aos tribunais de família e menores, por estarem dotados de outra sensibilidade[116]. Existe investigação internacional que sugere que estes tribunais podem desempenhar um papel vital no sentimento de proteção e segurança das vítimas. Os sucessivos governos ingleses têm, desde 2005, estabelecido tribunais especializados em VD em Inglaterra e no País de Gales. As avaliações realizadas à prática nesses tribunais sugerem ganhos significativos desde a sua implementação, pois o número de condenações nos casos de VD aumentou. Acresce que as avaliações independentes sugerem que, quando as vítimas estão envolvidas e apoiadas por profissionais focados dentro destes tribunais, sentem-se mais seguras e os seus casos têm

113 Epstein e Goodman, 2019: 405-406; Leite, 2020: 31-66. Uma abordagem da prática judicial de investigação de paternidade de menores em Portugal permite ancorar uma reflexão sobre a relação das mulheres com os tribunais. O sistema jurídico português ao assumir a defesa das crianças nascidas fora do casamento, pela intervenção em situações que são diferentes do modelo de estrutura familiar dominante faz com que as linguagens e as práticas jurídicas e a administração da lei passem a refletir pressupostos normativos que podemos encontrar em regras informais de regulação das interações sociais em outras esferas (Machado, 2004: 13-26).
114 Driskell, 2008.
115 Hulse, 2010: 5-9.
116 Cardoso, 2014: 113.

maior probabilidade de evoluir para uma acusação. Contudo, os progressos estão em risco pois estes tribunais dependem de parcerias e, nos últimos anos, os cortes orçamentais e o encerramento de vários tribunais têm afetado a sua dinâmica[117].

Mas, apesar desta realidade, a lei não pode retirar ao ofendido o direito de participar no processo que tenha por objeto a ofensa de que foi vítima[118]. Por isso os operadores devem manter os seus mandatos respeitando o princípio da legalidade e criando condições para reforçar o sentimento de segurança das vítimas. Alguns autores propõem que os Estados disponibilizem as suas bases de dados para permitir que indivíduos particulares possam saber se uma determinada pessoa já foi submetida a uma medida preventiva por VD. O objetivo é capacitar as potenciais vítimas com essas informações, para que possam evitar um relacionamento que pode levar a anos de sofrimento e abuso. Aqui, a conceção de privacidade mais relevante é a privacidade informacional em oposição à privacidade decisória. Em vez de ser reativa a atos passados de violência, a proposta é preventiva e visa evitar a violência e o abuso[119]. Por outro lado fala-se na inteligência artificial aplicada aos processos de decisão nos tribunais, por forma a impedir que os preconceitos turvem a objetividade, mitigando a revitimização. É um tema atual que nos leva a questionar em que medida poderá o juiz vir a ser suplantado por um computador, um *robot* ou um juiz-máquina[120].

117 Leite e Morais, 2019: 518.
118 Miranda e Medeiros, 2005: 361.
119 Chiu, 2010: 283-291.
120 Mendes, 2016: 118.

III. VIOLÊNCIA DOMÉSTICA, VIDA PRIVADA E INTERNET

3.1. Internet e crime

Nos finais dos anos 60 do séc. XX surgiram os computadores[121] e, quando apareceu a Internet na década de 80, criou-se um espaço virtual ilimitado para a propagação e venda de ideias, bens e serviços a uma escala global; atividades e ambientes novos no ciberespaço, conceito que não encontra um significado universalmente aceite, tratando-se de um conjunto de redes de comunicação entre computadores[122], que engloba as comunidades intangíveis e o espaço interativo através da internet[123]. O ciberespaço está ligado às ideias de globalização, um universo virtual paralelo ao mundo físico, sem fronteiras, desenvolvimento e impacto da tecnologia nas sociedades hodiernas[124]. Em 2020, para uma população mundial de 7,6 bilhões de pessoas, estima-se que existam 50 bilhões de dispositivos conectados[125].

A Internet, realidade que inclui *hardware*, *software*, infraestruturas técnicas, aplicações e os conteúdos que navegam pelos servidores[126], tornou-se uma realidade omnipresente que viu aumentar exponencialmente os fenómenos criminosos com a implementação de redes de comunicação[127], dificultando a reconstituição do percurso das informações, levando a que cada vez mais pessoas se sintam tentadas a utilizar a Internet para a consumação do crime[128]. Nessa medida, com o aparecimento da criminalidade informática, o pensamento jurídico foi confrontado com duas questões: a delimitação do universo das condutas ofensivas praticadas contra os meios informáticos, ou através deles, que deveriam catalogar-se de crime informático; e a denominação legal (*nomen juris*) mais adequada para os crimes que lesam os bens jurídicos relativos à propriedade, ao uso, à segurança, à funcionalidade dos computadores e equipamentos periféricos (hardware), e ao funcionamento das redes e sistemas de computadores e telecomunicações que neles é possível correr (software)[129]. Estas questões são naturais pois o direito é pensado em função do mundo físico. As caraterísticas da Internet (anónima, global e transnacional), fazem com que seja adversa à atuação do direito, concebido para atuar numa sociedade assente em bens tangíveis, contrariando o

121 Ramos, 2017: 33.
122 Dicionário Priberam cit. in Elias, 2018: 303.
123 Akdeniz, Walker e Wall, 2000: 3.
124 Elias, 2018: 304-305.
125 Evans, 2011: 3.
126 Lança, 2016a: 35.
127 Verdelho, 2009a: 717.
128 Venâncio, 2011: 15.
129 Aguiar, 2017: 19.

alcance territorial dos ordenamentos jurídicos nacionais, levantando o problema de aplicabilidade deste a um campo sem fronteiras[130].

Assim, fomos assistindo à generalização da utilização da Internet e das redes sociais e ao aumento da capacidade e da conectividade dos equipamentos de computação e comunicação, potenciando a divulgação de conteúdos suscetíveis de violarem a honra de outrem, ou a privacidade, ou o direito à imagem de terceiros[131], assim como outros múltiplos tipos legais[132], *e.g.*, a falsidade informática, o dano relativo a programas ou outros dados informáticos[133], a sabotagem informática, interceção ilegítima, reprodução ilegítima de programa protegido[134], o ciberterrorismo, o *cyberstalking*, o tráfico de pessoas, a prostituição, a contrafação, a imitação e uso ilegal de marca, o acesso ilegítimo, o branqueamento de capitais, a associação criminosa[135], a apropriação ilegítima em caso de acessão ou de coisa achada[136], a burla informática e nas comunicações[137], e tipos legais *sensíveis* quando se pensa em públicos mais vulneráveis como as crianças[138] ou os idosos (*v.g.* as ciberburlas *românticas*[139]) que diariamente são vítimas no ciberespaço. Alguns autores resumem as ciberameaças ao ciberterrorismo, ciberespionagem, cibercriminalidade, o *hacking*[140] e o *hacktivismo*[141]; ou classificando o cibercrime em atividades criminosas tradicionais que são expandidas ou aprimoradas pela Internet; atividades criminosas tradicionais que são generalizadas e radicalizadas pela Internet; e atividades criminosas criadas pela Internet[142].

No fim do séc. XX, Grabosky, Wright e Smith (1998) identificaram os nove tipos de crime baseados na tecnologia: interceção ilegal dos sistemas de telecomunicações; a vulnerabilidade ao vandalismo eletrónico e ao terrorismo; *roubo* de serviços de telecomunicações; violação das regras dos direitos de propriedade intelectual (intimidade das telecomunicações); conteúdos ofensivos e a pornografia no ciberespaço; fraudes do telemarketing; transferência de fundos eletrónicos (comércio na Internet e o dinheiro

130 Gonçalves, 2006: 5.
131 Procuradoria-Geral da República, 2017: 13.
132 Em 2011, só em *phishing*, a área da grande Lisboa registou danos que ultrapassam os € 2.000.000, sendo que quase 75% dos cerca de 1.300 inquéritos de criminalidade informática referem-se a esta realidade (segundo a PJ cit. in Teixeira, 2013: 111).
133 Nunes, 2018: 141-165.
134 Verdelho, 2009a: 724-731.
135 Cf. artigo 299.º do Código Penal.
136 Teixeira, 2013.
137 Cf. art. 221.º do Código Penal.
138 Lança, 2016a: 113-189.
139 Guimarães, 2018: 18-21; Poiares, 2019b e 2019c.
140 Para aprofundamento da noção e complexidade do *hacking vide* Ramalho, 2017: 311-352.
141 Elias, 2018: 308.
142 Hinson, Mueller, O'Brien-Milne, Wandera, 2018; *cit in* Der Wilk, 2018: 16.

eletrónico); o branqueamento do dinheiro eletrónico; e a utilização das telecomunicações para *conspirações* criminosas[143]. Mas, desde então, surgiram novos fenómenos, como a computação em nuvem utilizada para efeitos criminosos e o acesso a dados não publicamente acessíveis e sem o consentimento da pessoa legalmente autorizada a divulgá-los[144].

Alguns autores entendem que o cibercrime é todo o ato em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é alvo simbólico desse ato ou em que o computador é objeto de crime[145]; outros inserem o crime informático em categorias diferentes[146], onde o bem jurídico protegido é a informática no conceito de criminalidade-digital em sentido próprio ou puro[147]; ou factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa. O cibercriminoso é aquele que pratica estes crimes; contudo, no âmbito dos agentes de ameaças, esta designação é atribuída àquele que pratica estes crimes com intenções sobretudo económicas[148].

Mas, independentemente desta discussão, não existem dúvidas que têm aumentado as realidades como o *cyberbullying*, o *cyberstalking*[149] ou o assédio cibernético[150], apesar de a maioria dos esforços de pesquisa sobre abuso através da tecnologia estar preocupada com riscos *convencionais*, como o assédio e abuso em plataformas sociais e restrições a dispositivos como *laptops* e telefones. No entanto, têm surgido fenómenos com dispositivos, cameras e brinquedos conectados à Internet que oferecem oportunidades de intimidação e

143 Giddens, 2009: 236-239.
144 Ramalho, 2014: 123-162.
145 Marques e Martins, 2006.
146 *i.e.* crime informático digital próprio/puro ou crime digital impróprio/impuro.
147 Rodrigues, 2009.
148 ENSC 2019-2023 e ENISA, *Threat Landscape Report 2018* cit in CNCS, 2020: 15.
149 O *cyberbullying* é uma forma de assédio cibernético que afeta mais comummente os menores. Consiste em um comportamento on-line agressivo repetido com o objetivo de assustar e prejudicar a autoestima ou a reputação de alguém, o que às vezes empurra os indivíduos para a depressão e o suicídio. Já o *cyberstalking* pode ser perpetrado através dos emails, mensagens de texto (SMS) ou mensagens instantâneas ofensivas ou ameaçadoras; comentários ofensivos postados na internet, fotos ou vídeos íntimos compartilhados na internet ou por telemóvel. Para o preenchimento do tipo exige-se que a conduta seja adequada a provocar medo, inquietação ou prejudicar a sua liberdade de determinação nos termos do artigo 154.º-A do CP (Lança, 2016b: 313). *Stalking* é uma forma de violência relacional caracterizada por assédio permanente, expresso pelo contacto, comunicação, vigilância e monitorização da vítima, comportamentos repetidos, intencionais, não desejados pelo alvo e que induz medo nas suas vítimas ou que é percebido como ameaçador ou atemorizador por uma pessoa razoável (Matos, 2012: 163). Estas condutas podem ser práticas doces, como ofertas de presentes ou envio frequente de SMS ou e-mails ou, por outro lado, insultos, ameaças ou violência física (Lança, 2016b: 288-289).
150 Experiências de assédio sexual de vítimas que envolvem e-mails ou mensagens SMS sexualmente explícitos ofensivos indesejados; avanços ofensivos inapropriados em sites de redes sociais como o Facebook ou em *chats* na Internet (Van Der Wilk, 2018: 14-15). Para aprofundamento das especificidades do correio eletrónico, em particular a prova digital em processo penal, *vide* Ramos, 2017.

manipulação das vítimas. Na peça de teatro *Gas Light* (1938)[151] de Patrick Hamilton, uma mulher é manipulada pelo marido para duvidar da sua perceção do contexto e questionar a sua própria sanidade. Agora, esse comportamento pode ocorrer através do toque de um telemóvel, seja para ajustar a temperatura de uma sala a quilómetros de distância ou para ferver uma panela para lembrar alguém que está a ser observado[152]. Na Europa, uma em cada dez mulheres sofre algum tipo de violência cibernética desde os quinze anos. A ONU, o Conselho da Europa e as instituições da União Europeia reconhecem a violência cibernética e o discurso de ódio *online* contra as mulheres, desde logo porque são uma forma de violência baseada no género[153].

A estratégia da União Europeia, relativamente à cibersegurança, foi, assim, obrigada a alterar-se significativamente. As abordagens iniciais limitavam-se à proteção online das crianças, e-comércio e cibercrime tendo, em 2013, arrancado com uma estratégia legal mais consolidada[154]. A Lei n.º 109/2009, de 15 de setembro, aprovou a Lei do Cibercrime que veio substituir a Lei da Criminalidade Informática (Lei n.º 109/91, de 17 de agosto), transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adaptou o direito interno à Convenção sobre Cibercrime do Conselho da Europa. A legislação regula ainda a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas, bem como dos dados conexos necessários para identificar o utilizador registado, para fins de investigação, deteção e repressão de crimes graves, transpondo para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março[155].

O relatório de cibersegurança em Portugal (2020) demonstra que as tendências globais andam em torno das tecnologias emergentes (Internet das coisas, 5G, inteligência artificial, computação quântica e plataformas em nuvem), que tendem a aumentar a superfície e os vetores de ataque; a fragmentação e a imprevisibilidade da governabilidade da cibersegurança a nível internacional; e a importância de certas ciberameaças, como *ransomware*, fraude, *phishing* e ataques à cadeia de fornecimento. Neste cenário a pandemia de Covid-19 ameaça alterar as previsões, trazendo consigo novas tendências, como o possível desaceleramento de algumas tecnologias; a ameaça à proteção dos dados pessoais; o aumento dos ciberataques

151 *Vide* https://www.theguardian.com/stage/2019/oct/08/victorian-melodrama-gaslight-love-island-psychological-abuse-patrick-hamilton-play-buzzword (consultado em 22.05.2020).
152 Lopez-Neira, Patel, Parkin, Danezis e Tanczer, 2009: 24.
153 Van Der Wilk, 2018: 10-11.
154 Gercke, 2014: 35.
155 Lei n.º 32/2008 de 17 de julho.

que usam a engenharia social oportunista; ameaça a serviços essenciais e infraestruturas críticas; e o possível uso político da crise económica e social por agentes de desinformação ou de desestabilização sociopolítica[156]. Alguns autores defendem que o futuro passa por equipar as polícias de investigação com mais meios capazes para fazer face ao fenómeno do cibercrime[157], na medida em que os meios disponíveis para a investigação criminal não se têm revelado suficientes[158]. Mas primeiro importa mitigar as fragilidades das competências técnicas e processuais das polícias, no âmbito da prova digital[159] e a prevenção do cibercrime, por via de uma cooperação interinstitucional[160], nacional, internacional e entre entidades governamentais e as grandes empresas ligadas às novas tecnologias, como o *Google* e o *Facebook*[161].

3.2. Violência doméstica e difusão de imagens nas redes sociais

A primeira rede social surgiu em 1977 com a *SixDegrees.com*[162]. Desde então apareceram dezenas de redes sociais *online*, como o *Facebook*[163], o *Twitter*[164], o *LinkedIn*[165], o *Instagram*[166], o *Pinterest*[167] e o *Myspace*[168] que têm contribuído para a socialização no ciberespaço[169], dando aos utilizadores a oportunidade de se encontrarem com velhos e novos amigos, aumentar as redes e socializar sem a necessidade da deslocação física. Mas esta não é uma zona livre de riscos. O maior inconveniente desta forma de socialização é a confiabilidade incerta do amigo virtual. Ao mesmo tempo muitos utilizadores tratam a socialização no ciberespaço como um domínio para superar a sua liberdade de expressão, o que atrai injúrias, difamações, discursos de ódio, ameaças e outros tipos legais de crime[170].

156 CNCS, 2020: 84.
157 Matos, 2019: 81; Simas, 2014: 160.
158 Simas, 2014: 160.
159 Silva, 2018: 53.
160 Amador, 2012: 69-73.
161 Santos, 2015: 222.
162 Prino, 2012: 6-7; Ellison e Boyd *cit in* Lemons, 2011: 4.
163 Para aprofundamento do enquadramento legal da rede social *online* Facebook *vide* Prino, 2012.
164 Rede social *online* para *microblogging* que permite aos usuários enviar e receber atualizações pessoais de outros contactos, com um número de carateres limitado, conhecidos como *tweets*.
165 Rede social *online* que proporciona a troca de informação de experiências profissionais, em que os usuários dão a conhecer o seu *curriculum vitae* para acederem a oportunidades, estabelecerem contactos profissionais e estarem a par do que acontece no mundo do trabalho (Prino, 2012: 7).
166 Rede social *online* que permite a partilha de fotos e vídeos entre os seus usuários.
167 Rede social *online* que permite a partilha de fotos.
168 Rede social *online* mais popular no mundo até 2008, que perdeu todos os conteúdos colocados na rede até 2016 devido a um erro aquando da migração de dados entre servidores. A este propósito *vide* https://observador.pt/2019/03/19/myspace-perdeu-todo-o-conteudo-dos-utilizadores-anterior-a-2016/ (consultado em 12.06.2020).
169 Henriques, 2014: 3.
170 Halder e Karuppannan, 2009: 23; Amador, 2018: 102.

A legislação não tem acompanhado, ao mesmo ritmo e de maneira eficiente, as preocupações com as alterações de privacidade nas redes sociais, desde logo porque a maior limitação à eficácia dos governos, no âmbito da privacidade das redes sociais *online*, é o facto de muitos utilizadores não desenvolverem medidas de proteção mínimas, *e.g.*, ao disponibilizarem dados pessoais, como as datas de nascimento, a naturalidade, residências e números de telefone, permitindo a descoberta dos números da segurança social e, por essa via, permitir a apropriação da identidade[171], conforme se pode depreender após uma análise atenta à jurisprudência quando se conjuga o universo das redes sociais com a privacidade e o direito à imagem.

O direito à imagem configura um bem jurídico-penal autónomo, tutelado em si e de *per si*, independentemente da sua valência do ponto de vista da privacidade, como resulta claro da circunstância de o texto adoptado pelo CP de 1982 ser o de fotografar, filmar ou registar aspetos da vida particular de outrem, expressão que em 1995 seria substituída por fotografar ou filmar outra pessoa. Trata-se de um bem jurídico eminentemente pessoal com a estrutura de uma liberdade fundamental e que reconhece à pessoa o domínio exclusivo sobre a sua própria imagem. E sendo o objeto da proteção legal a imagem física da pessoa, ela abrange todo o corpo[172]. Constitui, assim, um bem jurídico-penal autónomo que abrange dois direitos autónomos: o direito a não ser fotografado e o direito a não ver divulgada a fotografia. Uma pessoa pode autorizar ou consentir que lhe seja tirada uma fotografia e pode não autorizar que essa fotografia seja usada ou divulgada. Por isso, é suscetível de preencher o tipo legal de crime de gravações e fotografias ilícitas, do art. 199.º, n.º 2, do CP, o agente que, contra a vontade do fotografado, utiliza uma fotografia deste, ainda que licitamente obtida e a publicitada numa rede social, *in casu* o *Facebook*[173]. Também constitui o crime p. e p. pelo art. 199.º do CP, a realização de cópias informáticas de fotografias existentes das vítimas e dos filhos e livremente acessíveis no Facebook daqueles e o seu envio posterior aos próprios por e-mail, por ter sido feita contra a vontade de quem elas retratavam[174]. Acresce que, para a verificação do crime, p. e p. pelo art. 199.º, n.º 2, al. b) do CP, não é preciso que a imagem retratada da pessoa a desfavoreça; consumando-se independentemente da impressão que cause nos outros, se a sua divulgação não tiver sido consentida[175]. Por outro lado, sempre que terceiro capte, sem o consentimento dos respetivos proprietários, imagens da sua residência

171 Lemons, 2011: 12-20.
172 *In* Acórdão de 29 de maio de 2012 do TRE, proc.º n.º 253/07.3 JASTB.E1.
173 *In* Acórdão de 5 de junho de 2015 do TRP, proc.º n.º 101/13.5TAMCN.P1.
174 *In* Acórdão de 12 de julho de 2017 do TRP, proc. n.º 47/15.2T9AGD.P1.
175 *In* Acórdão de 29 de maio de 2012 do TRE, proc.º n.º 253/07.3 JASTB.E1.

através de um *drone* que a sobrevoou, passando essas imagens a fazer parte de um vídeo que divulgou nas redes sociais, pratica aquele um facto ilícito (na primeira variante de ilicitude prevista no n.º 1 do art. 483.º do CC), porque violador do mencionado direito absoluto[176].

Mas já não constitui crime a obtenção de imagens, mesmo sem consentimento do visado, sempre que exista justa causa para tal procedimento, designadamente quando sejam enquadradas em lugares públicos, visem a proteção de interesses públicos ou hajam ocorrido publicamente; e não é proibida a prova obtida por sistemas de videovigilância colocados em locais públicos, com a finalidade de proteger a vida, a integridade física, o património dos respetivos proprietários ou dos próprios clientes perante furtos ou roubos[177].

Encontramos ainda diversas decisões judiciais que são elucidativas quanto ao posicionamento do tribunais neste âmbito, surgindo jurisprudência no contexto das relações de namoro, defendendo que a prática de atos sexuais, mantidos sob ameaça de divulgação de vídeos nas redes sociais, caso não continuassem a relação amorosa que até ali tinham mantido, integra o crime de violação p. e p. pelo art.º 164.º, n.º 1, al. a) do CP[178]; e que a criação, numa rede social, de um perfil em nome de outra pessoa, com inclusão de características de utilizador ofensivas da honra e consideração do titular do perfil, constituem um crime de difamação[179]; ou que, em decisão de regulação de responsabilidades parentais, a imposição aos pais do dever de abster-se de divulgar fotografias ou informações que permitam identificar a filha nas redes sociais mostra-se adequada à salvaguarda do direito à reserva da intimidade da vida privada e da proteção dos dados pessoais e, sobretudo, da segurança da menor no ciberespaço[180].

Mas, apesar de todo o esforço desenvolvido pelos tribunais e pelos Estados neste domínio, estamos longe de um controlo eficiente dos comportamentos desviantes nas redes sociais *online*. Há quem sugira que deviam ser adotados mecanismos destinados a assegurar o direito dos utilizadores a revogarem a sua limitação voluntária, nomeadamente, pela obrigação de obtenção de consentimento do titular pelos terceiros que desejem realizar *tags*, *share*, copiar o conteúdo, entre outros[181]. O art. 81.º, n.º 2 do CC estatui que a limitação voluntária, quando legal, é sempre revogável, ainda que com a obrigação de indemnizar os prejuízos causados às legítimas expetativas do titular dos direitos de personalidade[182]. O

176 *In* Acórdão de 11 de abril de 2019 do TRP, proc.º n.º 24733/17.3T8PRT.P1.
177 *In* Acórdão de 16 de janeiro de 2013 do TRP, proc.º n.º 201/10.3GAMCD.P1.
178 *In* Acórdão de 14 de junho de 2017 do TRP, proc.º n.º 16/16.5GAAGD.P1.
179 *In* Acórdão de 18 de março de 2013 do TRG, proc.º n.º 753/09.0JABRG.G1.
180 *In* Acórdão de 25 de junho de 2015 do TRE, proc. n.º 789/13.7TMSTB-B.E1.
181 Henriques, 2014: 48.
182 Sousa, 1995: 409.

problema coloca-se, contudo, ao nível da operacionalização da possibilidade legal de o utilizador da rede social revogar a todo o tempo esta limitação voluntária[183].

3.3. Violência doméstica e devassa da vida privada

O direito à reserva sobre a intimidade da vida privada, enquanto direito fundamental de personalidade, caracteriza-se como inato, inalienável, irrenunciável, impõe-se ao respeito de todas as pessoas[184] e abrange a proteção do nome, a orientação, identidade e a vida sexual, a integridade física e moral, a saúde mental, o direito a estabelecer relações com outras pessoas, a vida familiar (i)legítima, o respeito da correspondência e a proteção dos dados pessoais contra usos indevidos[185]. Esta proteção é difícil de concretizar pois não é possível controlar as cópias armazenadas no ciberespaço, ainda que tenham sido apagadas. A eliminação dos dados nos sítios de origem não garante a inexistência de outras cópias, pois, uma vez disponibilizada uma informação na Internet, não se sabe onde pode estar armazenada, sendo impossível localizar todos os detentores daquela informação para que seja eliminada da rede[186], em particular num quadro de violência doméstica, onde a (ameaça de) publicação de imagens íntimas surgem, muitas das vezes, como uma extensão e um elemento potenciador da relação desigual que persiste no mundo físico. Não foi, por isso, mero acaso que o legislador, através da Lei n.º 44/2018, de 9 de agosto, tenha procedido à 46.ª alteração ao CP, para reforçar a proteção jurídico-penal da intimidade da vida privada na internet quando passou a punir com pena de prisão de dois a cinco anos o agente que difundir através da internet ou de outros meios de difusão pública generalizada, dados pessoais, designadamente imagem ou som, relativos à intimidade da vida privada de uma vítima sem o seu consentimento, cf. a al. b), n.º 2 do art. 152.º do CP.

Neste âmbito a jurisprudência portuguesa tem sido *fértil* em decisões que relacionam a violência doméstica com o direito à reserva sobre a intimidade da vida privada, surgindo como um instrumento para o agente constranger e criar medo, através de comportamentos de (pornografia de) vingança[187] e abuso, com a (ameaça de) difusão de imagens, nas redes sociais, de modo a afetar emocional, psicológica e fisicamente as vítimas. O direito à imagem configura um bem jurídico protegido independentemente da sua valência do ponto de vista

183 Henriques, 2014: 28.
184 In Acórdão de 11 de abril de 2019 do TRP, proc.º n.º 24733/17.3T8PRT.P1.
185 Moreira, 2019: 1478-1479.
186 Sawaris, 2017: 89.
187 A pornografia de vingança consiste em aceder, usar, disseminar conteúdo gráfico ou de vídeo privado sem consentimento ou conhecimento da vítima, afetando-a (Van Der Wilk, 2018: 18).

da privacidade. Assim, para que o crime opere, não se exige que a oposição de vontade seja expressa, pois, para a conduta ser típica bastará que contrarie a vontade presumida do portador concreto do direito à imagem[188]. Acresce que a criminalização da devassa por meio informático decorre do disposto no art. 35.º, n.º 3 da CRP[189], e visa proteger a reserva da vida privada contra atos de discriminação que a utilização de meios informáticos torna exponencialmente perigosos, razão pela qual o procedimento criminal relativamente ao crime previsto no art. 193.º do CP[190] não depende de queixa. No tipo legal da devassa por meio de informática encontramos não só os atos de criação de ficheiros violadores do bem protegido, mas também os atos de conservação e utilização desse ficheiro[191].

Assim, como elementos objetivos do crime de devassa da vida privada, surge a obtenção ou transmissão de informação relativa a conversas, comunicações telefónicas, mensagens de correio eletrónico, ou outras que incidam sobre matérias individualmente consideradas reservadas; a obtenção ou transmissão de imagens de pessoas, objetos ou espaços íntimos ou reservados; a observação ou escuta de terceira pessoa em lugar privado; e a divulgação de factos da vida privada de terceira pessoa[192]. A intenção de devassar a vida privada das pessoas, referida no n.º 1 do art. 192.º do CP[193], enquanto elemento subjetivo típico, não assume uma autonomia específica, tendo apenas como efeito expressar que o crime de devassa da vida privada só admite o dolo direto; que se trata de um crime de dolo específico ou, segundo um outro entendimento, visando apenas afastar a punibilidade com dolo eventual. Assim, comete o crime de devassa da vida privada quem, sem autorização da pessoa visada, e estando ciente do respetivo conteúdo, intencionalmente divulga, *e.g.*, fotografias onde aquela, se encontra retratada despida, em roupa interior e em poses de natureza sexual[194].

188 Andrade, 2012: 821; Acórdão de 20 de setembro de 2017 do TRC, proc.º n.º 2/16.5PAMGR.C1; Acórdão do TRL de 15 de fevereiro de 1989, CJ 1/89; Acórdão do STJ de 24/5/89, BMJ n.º 387.

189 A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

190 Quem criar, mantiver ou utilizar ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.

191 Venâncio, 2006: 9.

192 *In* Acórdão de 10 de abril de 2018 do TRE, proc.º n.º 353/16.9GASSB.E1.

193 Quem, sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual: a) Interceptar, gravar, registar, utilizar, transmitir ou divulgar conversa, comunicação telefónica, mensagens de correio electrónico ou facturação detalhada; b) Captar, fotografar, filmar, registar ou divulgar imagem das pessoas ou de objectos ou espaços íntimos; c) Observar ou escutar às ocultas pessoas que se encontrem em lugar privado; ou d) Divulgar factos relativos à vida privada ou a doença grave de outra pessoa; é punido com pena de prisão até um ano ou com pena de multa até 240 dias.

194 *In* Acórdão de 6 de fevereiro de 2019 do TRP, proc.º n.º 3827/16.8JAPRT.P1.

Por outro lado, o crime de VD pode consubstanciar-se numa multiplicidade de condutas típicas que preenchem simultaneamente outros *crimes-satélite*, trazendo problemas sensíveis de concurso de crimes consigo. O que é determinante na decisão sobre o concurso de crimes são os sentidos sociais de ilicitude típica integrantes do comportamento global do agente. Assim, o crime de VD está numa relação de unidade de lei com os *crimes-satélite*: relativamente aos crimes menos severamente punidos está numa relação de subsidiariedade[195]; quanto aos crimes mais gravemente punidos está numa relação de subsidiariedade expressa. Quanto ao primeiro caso, a pena dos *crimes-satélites* é afastada pela de VD. Já quanto ao segundo caso, devido à cláusula de subsidiariedade expressa (art. 152.º, n.º 1), a pena do agente é a prevista para crime mais gravemente punido, superior à do art. 152.º. Da análise da prática judiciária, verificamos que é recorrente a identificação do concurso de normas e do concurso heterogéneo. No entanto, relativamente ao concurso efetivo homogéneo, a identificação do preenchimento de vários tipos legais efetivamente cometidos é realizada, mas cada tipo é preenchido pela conduta do agente, ficando-se por ali o processo do art. 30.º, n.º 1, do CP não se respeitando o mandado de esgotante apreciação, decorrente do princípio *ne bis in idem*. Regra geral, o agente é condenado apenas pelo crime de VD, independentemente dos contornos e extensão do caso concreto[196].

Assim, quando um agente tem uma relação interpessoal com a vítima, nos termos vertidos no tipo legal da violência doméstica, e se difundir imagens, nas redes sociais, sem o seu consentimento, comete o crime p. e p. no art. 152.º do CP, conforme se depreende da análise de vários acórdãos, em que o agente é punido pelo crime mais grave quando existe uma relação de subsidiariedade entre os tipos legais em concreto; *e.g.*, apesar dos factos integradores de violação, entre cônjuges, revestirem autonomia, indo para além do ambiente de VD até aí existente, o art. 152.º, n.º 1 do CP, criou uma relação de subsidiariedade entre ambos, devendo o agente ser punido, pela globalidade dos factos, apenas pelo crime de violação, por ser o mais grave[197]. O mesmo sucede numa ex-relação de namoro ou extraconjugal, em que a prática de atos sexuais, mantidos sob violência e ameaça, depois de haver terminado uma relação extraconjugal, integra apenas o crime de violação do art.º 164.º, n.º 1, al. a) do CP[198].

195 Significa que a norma penal intervém de forma auxiliar ou subsidiária, quando o facto não é punido por uma outra norma mais grave.
196 Cruz, 2017: 81-82.
197 *In* Acórdão de 27 de setembro de 2017 do TRP, proc.º n.º 1342/16.9JAPRT.
198 *In* Acórdão de 14 de junho de 2017 do TRP, proc.º n.º 16/16.5GAAGD.P1.

Em suma, geralmente deve ser considerada a existência de um concurso de normas, quando, *e.g.*, a filmagem ilícita é feita para permitir a devassa da intimidade, pelo que os crimes estão numa relação de concurso aparente. Quando a filmagem ilícita é efetuada, não para devassar a intimidade da ofendida, mas para lhe extorquir dinheiro, e só porque esta não fez o pagamento pretendido, frustrando a extorsão, é que o filme é publicitado numa rede social, devassando a sua intimidade, deve entender-se, a existência de um concurso real entre o crime de gravações e fotografias ilícitas e o crime de devassa da vida privada[199]. Por outro lado, quando um agente envia à vítima mensagens ameaçadoras, incorre numa conduta que põe em causa não só a integridade física, mas a saúde da pessoa ofendida, atingida no seu bem-estar físico, psíquico e mental. Se, entre os atos suportados pela ofendida, se destaca a ofensa à sua própria autodeterminação sexual, através da introdução pelo agente de um pénis artificial na sua vagina, mostra-se integrada a previsão da al. b, do n.º 1 do art. 164.º do CP, punição mais grave aplicável no caso (art. 152.º, n.º 1). Por outro lado, se a arguida imobilizou a ofendida, estando impossibilitada de resistir, e retirou da carteira da ofendida o cartão de débito e dele se apropriou, estão preenchidos todos os elementos do crime de roubo, p. e p., pelo art. 210.º, n.º 1 do CP[200], punição também mais grave.

Conclui-se, assim, que o crime de violência doméstica é um crime impróprio ou impuro e de perigo abstrato, que pode criar uma relação de concurso aparente de normas com outros tipos penais, designadamente as ofensas à integridade física simples (art. 143.º, n.º 1 do CP), as injúrias (art. 181.º), a difamação (art. 180.º, n.º 1), a coação (art. 154.º), o sequestro simples (art. 158.º, n.º 1), a devassa da vida privada (art. 192.º, n.º 1. al. b) ou as gravações e fotografias ilícitas (art. 199.º, n.º 2, al b)[201], sendo o agente punido pelo crime mais grave, *in casu* a VD[202], quando existe uma relação de subsidiariedade com tipos legais cujas molduras penais são menores.

199 *In* Acórdão de 13 de dezembro de 2017 do TRC, proc.º n.º 269/16.9PCCBR.C1.
200 *In* Acórdão de 6 de novembro de 2018 do TRL, proc.º n.º 329/17.9PALSB.L1-5.
201 *In* Acórdão de 8 de janeiro de 2013 do TRE, proc.º n.º 113/10.0TAVVC.E1; Castilhos, 2014: 182.
202 Quem difundir através da Internet ou de outros meios de difusão pública generalizada, dados pessoais, designadamente imagem ou som, relativos à intimidade da vida privada de uma das vítimas sem o seu consentimento é punido com pena de prisão de dois a cinco anos.

CONCLUSÃO

As novas tecnologias, a internet e o ciberespaço representam desafios securitários múltiplos para os governos, os informáticos, os juristas, os tribunais e as polícias, exigindo respostas multi(inter)disciplinares, supranacionais e interinstitucionais. No presente artigo definimos como objetivo a compreensão da dialética entre o crime de violência doméstica e as redes sociais, em particular a proteção jurídico-penal da vida privada na internet, assente na jurisprudência portuguesa e do TEDH, na doutrina e na legislação, para podermos responder à pergunta de partida, *máxime* o tipo legal que é preenchido quando o agente difunde, sem o consentimento da vítima, uma imagem relativa à intimidade da vida privada nas redes sociais.

Verificámos que o crime de violência doméstica é um crime específico impróprio ou impuro e de perigo abstrato, que abrange ações típicas que encontram previsão noutros tipos legais, com os quais pode criar uma relação de concurso aparente de normas, designadamente, a devassa da vida privada. Por isso, o agente é punido pelo crime mais grave quando existe uma relação de subsidiariedade entre os tipos legais em concreto. Assim, o crime de VD, relativamente aos crimes com uma moldura penal menos *severa*, encontra-se numa relação de subsidiariedade. Por isso, quando o agente, num quadro de violência doméstica, *i.e.*, numa relação interpessoal nos termos vertidos no art. 152.º do CP – *e.g.*, (ex-)cônjuges, (ex-)namorados, relações adúlteras; pessoa particularmente indefesa em razão da idade, deficiência, doença, gravidez ou dependência económica, que coabite com o agente, etc. – comete o crime de devassa da vida privada p. e p. pelo art. 192.º, com uma moldura penal até um ano ou com pena de multa até 240 dias. Mas *in casu*, a pena é afastada pelo tipo legal p. e p. pela al. b), n.º 2 do art. 152.º, na medida em que, quem difundir através da Internet ou de outros meios de difusão pública generalizada, dados pessoais, designadamente imagem ou som, relativos à intimidade da vida privada de uma das vítimas sem o seu consentimento é punido com pena de prisão de dois a cinco anos, ou seja, a moldura penal do segundo tipo legal *afasta* o primeiro.

BIBLIOGRAFIA

AA.VV. (2003), *Os custos sociais e económicos da violência contra as mulheres. Síntese dos resultados do Inquérito Nacional de 2002*, Ditos & Escritos, n.º 27, Lisboa: CIDM.

AA.VV. (2016), *Violência doméstica: boas práticas no apoio a vítimas LGBT para profissionais de estruturas de apoio a vítimas*, Coleção Violência de Género, Lisboa: CIG.

AGUIAR, Tiago L. S. (2017), *O Correio Eletrónico: A Apreensão e a Interceção no Processo Penal Português*, dissertação de mestrado em Ciências Jurídico-Criminais, Coimbra: FDUC.

AKDENIZ, Yaman; WALKER, Clive; WALL, David (2000), *The Internet, Law and Society*, Longman: Pearson Education.

ALBUQUERQUE, Paulo Pinto de (Coord) (2019), *Comentário da CEDH e dos Protocolos Adicionais*, vol. II, Lisboa: Universidade Católica Editora.

AMADOR, Nelson (2012), *Cibercrime em Portugal: Trajetórias e Perspetivas de Futuro*, dissertação de mestrado em Criminologia e Investigação Criminal, Lisboa: ISCPSI.

ANDRADE, Manuel da Costa (2012), "Comentário Conimbricense do Código Penal", *Parte Especial*, *I*, 2.ª edição, Coimbra Editora.

BECK, Ulrich (2015), *Sociedade de risco mundial: em busca da segurança perdida*, Lisboa: edições 70.

CANOTILHO, J. Gomes, MOREIRA, Vital (2007), *Constituição da República Portuguesa Anotada*, volume I, 4.ª edição, Coimbra: Coimbra Editora.

CARDOSO, Feliz Borges (2014), *A (in)eficácia da proteção das vítimas de violência doméstica*, dissertação de mestrado em Direito, Coimbra: ISBB.

CASTELLS, Manuel (2004), *A Galáxia Internet, Reflexões sobre a Internet*, Lisboa: Fundação Calouste Gulbenkian.

CASTELLS, Manuel (2002), *A Era da Informação: Economia, Sociedade e Cultura*, vol. I – A Sociedade em Rede. Lisboa: Fundação Calouste Gulbenkian.

CASTILHOS, Tânia M. S. (2014), *A violência de género nas redes sociais virtuais: a proteção das mulheres na perspetiva dos direitos humanos*, Salamanca: Ed. Universidad Salamanca.

CEJ (2016), *Violência Doméstica: Implicações sociológicas, psicológicas e jurídicas do fenómeno*, Lisboa: CEJ e CIG.

CHIU, Elaine (2010), "That Guy's a Batterer!: A Scarlet Letter Approach to Domestic Violence in the Information Age". *Family Law Quarterly*, vol. 44, p. 255; St. John's Legal Studies Research Paper No. 1895484, Disponível em SSRN: https://ssrn.com/abstract=1895484 (consultado em 11.05.2020).

CNCS (2020), *Relatório Cibersegurança em Portugal: Riscos & Conflitos*, junho, Lisboa: Observatório de Cibersegurança – Centro Nacional de Cibersegurança.

COSTA, José de Faria (2007a), *Direito Penal Especial. Contributo a uma sistematização dos problemas "especiais" da Parte Especial*, Coimbra: Coimbra Editora.

COSTA, José de Faria (2007b), *Noções Fundamentais de Direito Penal. Introdução,* Coimbra: Coimbra Editora.

CRUZ, Joana Carolina R. (2017), *Problemas de concurso na violência doméstica: uma análise da prática judiciária*, dissertação de mestrado em Direito, Lisboa: FDUNL.

DRISKELL, Kristen M. (2008), "Identity Confidentiality for Women Fleeing Domestic Violence", (March 7). *Hastings Women's Law Journal*, Forthcoming. Disponível em SSRN: https://ssrn.com/abstract=1262426 (11.05.2020).

ELIAS, Luís (2018), *Ciências Policiais e Segurança Interna: Desafios e Prospetiva*. Lisboa: ICPOL-ISCPSI.

EPSTEIN, Deborah & GOODMAN, Lisa A. (2019), "Discounting Women: Doubting Domestic Violence Survivors' Credibility and Dismissing Their Experiences", *U. Pennsylvania Law Review*, 167, Georgetown U. Law Center, 399-461. Disp. em SSRN: https://ssrn.com/abstract=3133066 (consultado em 12.05.2020)

EVANS, Dave (2011), *A Internet das Coisas, como a próxima evolução da Internet está mudando tudo*, Cisco Internet Business Solutions Group.

FERREIRA, Maria Elisabete (2005), *Da Intervenção do Estado na Questão da Violência Conjugal em Portugal*, dissertação de mestrado em Direito, FDUCP, Coimbra: Almedina.

GEORGIADOU, Elissavet (1995), *Marshall McLuhan's "global village" and the internet*, Master of Arts in Image Studies, U. of Kent at Canterbury.

GERCKE, Marco (2014), "Content of a Comprehensive Cybersecurity Legal Framework", in: *Computer Law Review*, 15th year, issue 2/2014, pp. 33-64.

GIDDENS, Anthony (2001), *Sociology*, 4.ª edição, Cambridge: Polity Press.

GIDDENS, Anthony (2009), *Sociologia*, 7.ª edição, Lisboa: F. Calouste Gulbenkian.

GONÇALVES, Maria Eduarda (2006), "Internet, Direito e Tribunais", in: *Sub Judice, Justiça e Sociedade*, set., n.º 35, Almedina.

GONZÁLEZ, José (2019), "Direito ao respeito pela integridade física e psíquica", in: *Comentário da CEDH e dos Protocolos Adicionais*, II, Lisboa: U. Católica Editora, 1389-1437.

GRABOSKY, Peter N.; WRIGHT, Paul H.; e SMITH, Russel G. (1998), *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, New Brunswick, N. J.: Transaction publishers.

GUIMARÃES, Filipa (2018), "Os mais velhos e o engodo das ciberburlas românticas", in: *Público*, 4 fev., ano XXVIII, n.º 10.151, edição, Lisboa: jornal Público, pp. 18-21.

HALDER, Debarati and KARUPPANNAN, Jaishankar (2009), "Cyber Socializing and Victimization of Women". *The Journal on Victimization*, Vol. 12, No. 3, Human Rights and Gender, September, 5-26. SSRN: https://ssrn.com/abstract=1561774 (11.05.2020).

HENRIQUES, Ana Festas (2014), *As redes sociais e o direito à reserva sobre a intimidade da vida privada*, dissertação de mestrado forense, Lisboa: FDUCP.

HINSON, L, MUELLER, J., O'BRIEN-MILNE, L., WANDERA N. (2018), "Technology-facilitated gender-based violence: What is it, and how do we measure it?" Washington D.C., International Center for Research on Women.

HULSE, Rebecca (2010), "Privacy and Domestic Violence in Court", *William and Mary Journal of Women and the Law*, Research Paper 09-51. William & Mary Law School.

ILGA Portugal (2015), *Números da violência contra Pessoas LGBT 2014*, Lisboa: Observatório da Discriminação em função da Orientação Sexual e Identidade de Género.

KOOPS, Bert-Jaap (2016), "Criminal investigation and privacy in Dutch law", in: *TILT Law & Technology Working Paper Series*, version 1.0, 11 September, disponível em http://ssrn.com/abstract=2837483 (20.05.2020).

LANÇA, Hugo C. (2016a), *A regulação dos conteúdos disponíveis na internet. A imperatividade de proteger as crianças*. Tese de doutoramento em Direito, FDUP. Lisboa: Chiado Editora.

LANÇA, Hugo C. (2016b), "Só liguei para dizer que te amo… Duzentas e Cinquenta e Duas vezes… A Ontologia do Ciberstalking", *Revista de Ciências Empresariais e Jurídicas*, n. 27, pp. 285-319.

LEITE, André Lamas e MORAIS, Ana (2019), "Violência doméstica: a experiência dos tribunais especializados na Inglaterra e no País de Gales". *Revista da Ordem dos Advogados*, A. 79, nº 3-4, Jul.-Dez., pp. 517-535.

LEITE, Ana Marta (2016), "A problemática da cibersegurança e os seus desafios", in: *CEDIS Working Papers*, 49, Lisboa: FDUNL.

LEITE, Inês Ferreira (2020), "Violência doméstica e violência interpessoal: contributos sob a perspetiva do Direito para a racionalização dos meios de prevenção e proteção", In: *Anatomia do Crime*, n.º 10, Lisboa: IDPCC-FDUL, pp. 31-66.

LEMONS, Robert (2011), "Protecting Our Digital Walls: Regulating the Privacy Policy Changes Made by Social Networking Websites", *Journal of Law and Policy for the Information Society*, v. 6, n. 60. Disponível em: https://ssrn.com/abstract=1952887 (consulta: 23.05.2020).

LEMOS, Inês (2019), *Proteção policial da vítima: avaliação do risco do agressor em cenários de violência doméstica*, dissertação de mestrado em Ciências Policiais, Lisboa: ISCPSI.

LISBOA, Manuel (2005), "Violência doméstica e violência contra as mulheres", *Seminário Prevenção da Violência Doméstica*, Lisboa: EMCVD, pp. 45-49.

LOPES, Tiago L. (2018), *Recolha de prova digital nos processos-crime de violência doméstica*, dissertação de mestrado em Ciências Militares (Segurança). Lisboa: Academia Militar.

LOPEZ-NEIRA, I, PATEL, T., PARKIN, S. DANEZIS, G., & TANCZER, L. (2009), "Internet of Things: How abuse is getting smarter", *Safe – The Domestic Abuse Quarterly*, 63, UK, 22-26. *In* SSRN: https://ssrn.com/abstract=3350615 ou http://dx.doi.org/10.2139/ssrn.3350615 (consultado em 11.05.2020)

LOURENÇO, Nelson e CARVALHO, Maria João Leote (2000), "Violência doméstica: conceito e âmbito. Tipos e espaços de violência – uma primeira aproximação", in: *Violência doméstica*, Lisboa: PGR e Gabinete da Ministra da Igualdade, pp. 25-62.

LOURENÇO, Nelson (2005), "Violência doméstica e violência contra as mulheres", *Seminário Prevenção da Violência Doméstica*, Lisboa: EMCVD, pp. 27-29.

MARQUES, Garcia e MARTINS, Lourenço (2006), *Direito da Informática*, 2.ª edição, refundida e atualizada, Coimbra: Almedina.

MACHADO, Helena (2004), "Cidadania polifónica e a (in)justiça para as mulheres", in: *ex aequo*, 11, Lisboa: APEM, pp. 13-26.

MATOS, Vítor L. G. (2019), *Medidas cautelares de polícia nos crimes praticados por meios informáticos: limites legais de atuação e capacitação da preservação urgente*, dissertação de mestrado em Direito. Lisboa: FDULHT.

MCLUHAN, Herbert Marshall (1994) (1964), *Understanding Media: The Extensions of Man*, Massachusetts: MIT press.

MENDES, Paulo de Sousa (2019), "Processo equitativo e público", in: Albuquerque, Paulo Pinto (Coord.), *Comentário da Convenção Europeia dos Direitos Humanos e dos Protocolos Adicionais*, vol. II, Lisboa: U. Católica Editora, pp. 1058-1068.

MENDES, Paulo de Sousa (2018), *Lições de Direito Processual Penal*, Coimbra Editora.

MENDES, Paulo de Sousa (2016), "Representação do conhecimento jurídico e sistemas periciais de auxílio à decisão judicial", in: *Anatomia do Crime. Revista de Ciências Jurídico-Criminais*, n.º 3, jan-jun., Lisboa: IDPCC-FDUL, pp. 118-127.

MIRANDA, Jorge e MEDEIROS, Rui (2005), *Constituição Portuguesa Anotada*, I, artigos 1.º-79.º, Coimbra Editora.

MORAIS, Teresa (2019), *Violência doméstica: o reconhecimento jurídico da vítima*. Coimbra: Almedina.

MOREIRA, António V. (2019), "A prova digital é o tema mais relevante em processo penal". Entrevista a David S. Ramalho e a Paulo de Sousa Mendes, *Jornal Económico*, p. 30, 26 jul., in: https://www.mlgts.pt/xms/files/site_2018/Imprensa/2019/Jornal_Economico_DSR_A_prova_digital_e_o_tema_mais_relevante_em_processo_penal_26JUL.pdf (consultado em 13.04.2020).

MOREIRA, Teresa Coelho (2019), "Direito ao respeito pela vida privada no âmbito das relações laborais", in: *Comentário da CEDH e dos Protocolos Adicionais*, II, Lisboa: U. Católica Editora, pp. 1473-1492.

MOURA, Cátia D. (2016), *Custo económico para o Estado Português do crime de homicídio em contexto de VD*, dissertação de mestrado, Lisboa: ISCPSI.

NUNES, Carlos Casimiro e MOTA, Maria Raquel (2010), "O crime de violência doméstica: a alínea b) do n.º 1 do art.º 152º do Código Penal", in: *Revista do Ministério Público*, n.º 122, abril-junho, pp. 133 e ss.

NUNES, Duarte Alberto (2018), "O crime de dano relativo a programas ou outros dados informáticos", in: *Revista do Ministério Público*, 153, Janeiro-Março, pp. 141-165.

PALMA, Maria Fernanda (2019), "O problema do sistema e o sistema imposto pelo problema na violência doméstica", in: *Anatomia do Crime. Revista de Ciências Jurídico-Criminais*, n.º 9, Lisboa: IDPCC-FDUL, pp. 53-57.

PEREIRA, Alexandre Dias (2019), "Direito ao respeito pela vida privada digital", in: *Comentário da Convenção Europeia dos Direitos Humanos e dos Protocolos Adicionais*, vol. II, Lisboa: Universidade Católica Editora, pp. 1451-1472.

PEREIRA, Rui (2005), "A violência doméstica e a reforma penal", in: *Prevenção da Violência Doméstica*, Lisboa: EMCVD, pp. 17-20.

PINHEIRO, Alexandre S. (2019), "Direito ao respeito pela identidade informacional", in: Albuquerque, P. P. (Coord), *Comentário da Convenção Europeia dos Direitos Humanos e dos Protocolos Adicionais*, vol. II, Lisboa: U. Católica Editora, 2019, pp. 1438-1450.

PINHEIRO, Alexandre S. (2015), *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, Lisboa: AAFDL Editora, pp. 94-107.

PINTO, Paulo Mota (2001), "A limitação voluntária do direito à reserva sobre a intimidade da vida privada", in: *Estudos em homenagem a Cunha Rodrigues*, v. II, Coimbra: Coimbra Editora.

POIARES, Nuno (2020), "O crime de violência doméstica: ato reiterado ou não, eis a questão", *Revista Eletrónica do Curso de Direito da UFSM*, Santa Maria, RS, v. 15, n. 1, e42646, ISSN 1981-3694.

POIARES, Nuno (2019a), "Violência doméstica e atividade policial", in: *Anatomia do Crime. Revista de Ciências Jurídico-Criminais*, n.º 9, Lisboa: IDPCC-FDUL, pp. 59-75.

POIARES, Nuno (2019b), "A cibersegurança à luz da criminologia moderna", in: *Cyberlaw by CIJIC*, Centro de Investigação Jurídica do Ciberespaço, edição VII, maio, Lisboa: CIJIC-FDUL.

POIARES, Nuno (2019c), "Cibersegurança, literacia e resiliência digital dos idosos", in: *Anuário Janus 2018-2019: A dimensão externa da segurança interna*, 19, Lisboa: Observare-UAL, pp. 118-119.

POIARES, Nuno e DIAS, Eurico (2019d), "Igreja Católica e Direito Criminal: uma abordagem sociológica ao Código Penal Português (1886)", in: *REVER - Revista de Estudos da Religião*, 19, n.º 3, set.-dez., São Paulo: UCP e PUC, pp. 311-329.

POIARES, Nuno (2014), *Políticas de segurança e as dimensões simbólicas da lei: o caso da violência doméstica em Portugal*, tese de doutoramento, Lisboa: ISCTE-IUL.

PRINO, Carla Sofia Abreu (2012), *O enquadramento legal do Facebook*, dissertação de mestrado em Comunicação, *Media* e Justiça, Lisboa: FDUNL e FCSH-UNL.

PROCURADORIA-GERAL DA REPÚBLICA (2019), *Diretiva n.º 5/2019, de 4 de dezembro*, Lisboa: PGR.

PROCURADORIA-GERAL DA REPÚBLICA (2017), *Jurisprudência sobre Prova Digital. Nota Prática nº 12/2017*, Lisboa: PGR.

RAMALHO, David Silva (2014), "A recolha de prova penal em sistemas de computação em nuvem", in: *Revista de Direito Intelectual*, n.º 2, Lisboa: APDI, pp. 123-162.

RAMALHO, David Silva (2017), *Métodos Ocultos de Investigação criminal em Ambiente Digital*, Coimbra: Almedina.

RAMOS, Armando Dias (2017), *A prova digital em processo penal – O correio eletrónico*, 2.ª edição, Lisboa: Chiado Editora.

RODRIGUES, Benjamim S. (2009), *Direito Penal, Parte Especial, I, Direito Penal Informático-Digital*, Coimbra: Coimbra Editora.

SAMPSON, Rana (2013) (2007), *Domestic Violence, Problem-Oriented Guides for Police Problem-Specific Guides*, Series Guide n. 45, Washington: COPS – Office of Community Oriented Policing Services.

SANI, Ana e MORAIS, Cristina (2015), "A polícia no apoio às vítimas de violência de doméstica: estudo exploratório com polícias e vítimas", in: *Direito e Democracia*, v.16, n.1, jan./jun., pp. 5-18.

SANTOS, Ana F. C. (2015), *O cibercrime: desafios e respostas do Direito*, dissertação de mestrado em Direito, Lisboa: Universidade Autónoma de Lisboa.

SAWARI, Adriana (2017), *A tutela do direito à reserva sobre a intimidade da vida privada em Portugal*, dissertação de mestrado em Direito Civil, Coimbra: FDUC.

SG-MAI (2019), *Relatório Anual de Monitorização da Violência Doméstica 2018*, Lisboa: Secretaria-Geral do Ministério da Administração Interna.

SILVA, Tiago A. M. (2018), *Recolha da prova digital nos processos-crime de violência* doméstica, dissertação de mestrado em Ciências Militares, Lisboa: Academia Militar.

SIMAS, Diana V. (2014), *O Cibercrime*, dissertação de mestrado, Lisboa: FDULHT.

SOUSA, Rabindranath C. (1995), *O direito geral de personalidade*, Coimbra: Coimbra Editora.

TEIXEIRA, Paulo Alexandre G. (2013), *O fenómeno do phishing: enquadramento jurídico-penal*, dissertação de mestrado em Direito. Lisboa: UAL.

TOMAR, Richa and DWIVEDI, Suneet Kumar (2014), "Protection of Human Rights of Women from Ancient to Modern Era: Insufficiency in Indian Legislation" (março 12). Disponível em SSRN: https://ssrn.com/abstract=2408052 (11.05.2020)

VAN DER WILK, Adriane (2018), *Cyber violence and hate speech online against women*, Women´s Rights & Gender Equality, Policy Department for Citizens´s Rights and Constituional Affairs, PE 604.979, September. Brussels: EU.

VENÂNCIO, Pedro Dias (2011), *Lei do Cibercrime – Anotada e Comentada*, Coimbra Editora.

VENÂNCIO, Pedro Dias (2006), "Investigação e meios de prova na criminalidade informática", in: *Verbo Jurídico*, dez., pp. 5-34.

VERDELHO, Pedro (2009a), "A nova Lei do Cibercrime", in: *Scientia Iuridica – Revista de Direito Comparado Português e Brasileiro*, n.º 320, out-dez, tomo LVIII, n.º 320, pp. 717 e ss.

VERDELHO, Pedro (2009b), "Phishing e outras formas de defraudação nas redes de comunicação", in: *Direito da Sociedade da Informação*, v. 8, Coimbra Editora, pp. 407-419.

VERÍSSIMO, Paulo Esteves (2007), *Identidade Digital*, Lisboa: APDSI.

WARREN, Samuel e BRANDEIS, Louis (1890), "The right to privacy", in: *Harvard Law Review*, v. IV, n.º 5, dez. 15, pp. 193-220.

XXII Governo Constitucional (2020a), *Manual de Atuação a adotar pelos OPC nas 72 horas subsequentes à apresentação de denúncia por maus-tratoscometidos em contexto de violência doméstica*, maio de 2020. Resolução do Conselho de Ministros n.º 139/2019, de 19 de agosto. Mem-Martins: Secretária de Estado para a Cidadania e Igualdade.

XXII Governo Constitucional (2020b), *Guia de Intervenção Integrada junto de crianças ou jovens vítimas de violência doméstica*, maio de 2020. Mem-Martins: Secretária de Estado para a Cidadania e Igualdade.

XXII Governo Constitucional (2020c), *Plano Anual de Formação Conjunta: Violência contra as Mulheres e Violência Doméstica*, maio de 2020. Mem-Martins: Secretária de Estado para a Cidadania e Igualdade.

XXII Governo Constitucional (2020d), *Guia de requisitos mínimos para programas e projetos de prevenção primária da violência contra as mulheres e violência doméstica*, maio de 2020. Mem-Martins: Secretária de Estado para a Cidadania e Igualdade.

JURISPRUDÊNCIA

Acórdão de 11 de abril de 2019 do TRP, proc.º n.º 24733/17.3T8PRT.P1

Acórdão de 6 de fevereiro de 2019 do TRP, proc.º n.º 3827/16.8JAPRT.P1

Acórdão de 6 novembro de 2018 do TRL, proc.º n.º 329/17.9PALSB.L1-5

Acórdão de 4 de junho de 2018 do TRG, proc.º n.º 121/15.5GAVFL.G1

Acórdão de 10 de abril de 2018 do TRE, proc.º n.º 353/16.9GASSB.E1

Acórdão de 10 de janeiro 2018 do TRC, proc.º n.º 1641/16.0T9VIS.C1

Acórdão de 13 de dezembro de 2017 do TRC, proc.º n.º 269/16.9PCCBR.C1
Acórdão de 27 de setembro 2017 do TRP, proc.º n.º 1342/16.9JAPRT
Acórdão de 26 de setembro 2017 do TRE, proc.º n.º 518/14.8PCSTB.E1
Acórdão de 20 de setembro de 2017 do TRC, proc.º n.º 2/16.5PAMGR.C1
Acórdão de 12 de julho de 2017 do TRP, proc. n.º 47/15.2T9AGD.P1
Acórdão de 14 de junho de 2017 do TRP, proc.º n.º 16/16.5GAAGD.P1
Acórdão de 1 de junho 2017 do TRL, proc.º n.º 3/16.0PAPST.L1-9
Acórdão de 8 de maio de 2017 do TRG, proc.º n.º 669//16.4JABRG.G1
Acórdão de 6 de fevereiro de 2017 do TRG, proc.º n.º 201/16.06GBBCL.G1
Acórdão de 21 de novembro de 2016 do TRG, proc.º n.º 16/15.2GEVCT.G1
Acórdão de 12 de outubro de 2016 do TRP, proc.º n.º 2255/15.7T9PRT.P1
Acordão de 7 de julho de 2016 do TRP, proc. n.º 18/15.9GAPRD.P1
Acórdão de 29 de março de 2016 do TRE, proc.º n.º 558/13.4GBLLE.E1
Acórdão de 5 de junho de 2015 do TRP, proc.º n.º 101/13.5TAMCN.P1
Acórdão de 25 de junho de 2015 do TRE, proc. n.º 789/13.7TMSTB-B.E1
Acórdão de 20 de janeiro de 2015 do TRE, proc.º n.º 228/13.3TASTR.E1
Acórdão de 8 de outubro de 2014 do TRP, proc.º n.º 956/10.5PJPRT.P1
Acórdão de 10 de setembro de 2014 do TRP, proc.º n.º 648/12.0PIVNG.P1
Acórdão de 10 de julho de 2014 do TRG, proc.º n.º 591/11.0PBGMR-G1
Acórdão de 29 de janeiro de 2014 do TRC, proc.º n.º 1290/12.1PBAVR.C1
Acórdão de 1 de outubro de 2013 do TRE, proc.º n.º 258/11.0GAOLH.E1
Acórdão de 18 de março de 2013 do TRG, proc.º n.º 753/09.0JABRG.G1
Acórdão de 27 de fevereiro de 2013 do TRC, proc.º n.º 83/12.0GCGRD.C1
Acórdão de 16 de janeiro de 2013 do TRP, proc.º n.º 201/10.3GAMCD.P1
Acórdão de 8 de janeiro de 2013 do TRE, proc.º n.º 113/10.0TAVVC.E1
Acórdão 15 de outubro de 2012 do TRG, proc.º n.º 639/08.6GBFLG.G1
Acórdão de 10 de setembro de 2012 do TRG, proc.º n.º 1011/11.6GBBCL.G1
Acórdão de 3 de julho de 2012 do TRE, proc.º n.º 53/10.3GDFTR.E1
Acórdão de 29 de maio de 2012 do TRE, proc.º n.º 253/07.3 JASTB
Acórdão de 29 de fevereiro de 2012 do TRP, proc.º n.º 368/09.3PQPRT.P1
Acórdão de 27 de fevereiro de 2008 do TRL, proc. n.º 1702/2008-3
Acórdão de 24 de abril de 2006 do STJ, proc.º n.º 06P975
Sentença Carlos Trabajo Rueda contra o Reino de Espanha, 30 de maio de 2017, TEDH
Sentença Robathin contra Áustria, 3 de outubro de 2012, TEDH

Sentença Ivashchenko contra a Rússia, 13 de fevereiro de 2018, TEDH

DIPLOMAS

Lei n.º 58/2019, de 8 agosto: Lei da Proteção de Dados Pessoais

Resolução do Conselho de Ministros n.º 61/2018, de 21 de maio

Convenção Europeia dos Direitos Humanos, TEDH, 4.11.1950 (versão atualizada)

Constituição da República Portuguesa

Código Civil, aprovado pelo DL n.º 47344, Série I, 25.11.1966 (versão atualizada)

Lei n.º 44/2018, de 9 de agosto: 46.ª alteração ao Código Penal

Lei n.º 19/2013, de 21 de fevereiro: 1.ª alteração à Lei n.º 112/2009, de 16 de setembro

Lei n.º 112/2009, de 16 de setembro, alterada pela Lei n.º 19/2013, de 21 de fevereiro; a Retificação n.º 15/2013, de 19 de março; a Lei n.º 82-B/2014, 31 de dez.; a Lei n.º 129/2015, de 3 de setembro; a Lei n.º 42/2016, de 28 de dezembro; e a Lei n.º 24/2017, de 24 de maio

Lei n.º 109/2009, de 15 de setembro: aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa

Lei n.º 32/2008, de 17 de julho: transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março

Lei n.º 59/2007, 4 de setembro: 23.ª alteração ao Código Penal

Lei n.º 7/2000, 27 de maio: reforça as medidas de proteção a pessoas vítimas de violência

Lei n.º 109/91, de 17 de agosto: Lei da Criminalidade Informática

Código de Processo Penal, aprovado pelo Decreto-Lei n.º 78/87, de 17 de fevereiro

Código Penal, aprovado pelo Decreto-Lei n.º 400/82, de 23 de setembro

CYBERLAW
by CIJIC

DA ADMISSIBILIDADE DA UTILIZAÇÃO DE BENWARE NO DIREITO PORTUGUÊS

ON THE ADMISSIBILITY OF THE USE OF BENWARE UNDER PORTUGUESE LAW

DUARTE RODRIGUES NUNES *

* Juiz de Direito, Professor Convidado da Universidade Europeia (Direito penal), Doutor em Direito pela Faculdade de Direito de Lisboa, Investigador do Centro de Investigação de Direito Penal e Ciências Criminais e do Centro de Investigação Jurídica do Ciberespaço.

RESUMO

A utilização das medidas antiforenses e de meios de comunicação como as comunicações por VoIP pelos criminosos dificulta de sobremaneira a investigação criminal. Por isso, as autoridades têm de utilizar meios que neutralizem essas dificuldades. Um desses meios é a instalação sub-reptícia de programas informáticos que permitam infiltrar sistemas informáticos para obter informações relevantes para a investigação (*benware*). A lei portuguesa não prevê expressamente a utilização de *benware*, apenas existindo uma referência implícita ao uso de *benware* no art. 19.º, n.º 2, da Lei n.º 109/2009. Apesar disso, a utilização de *benware* é admissível à luz do Direito português, embora seja preferível que o legislador preveja expressamente essa possibilidade na lei.

Palavras-chave: Buscas *online* – Cibercrime – investigação criminal – prova digital – Direito à confidencialidade e à integridade dos sistemas técnico-informacionais.

ABSTRACT

The use of anti-forensic measures and means of communication, such as VoIP communications, by criminals, makes criminal investigation extremely difficult. Therefore, the authorities must use means that can counteract these difficulties. One of these means is the surreptitious installation of computer programs that permit to infiltrate computer systems in order to obtain information that is relevant to the investigation (benware). Portuguese law does not expressly provide for the use of benware. There is only an implicit reference to the use of benware in art. 19, no. 2, of Law no. 109/2009. Nevertheless, the use of benware is admissible under Portuguese Law, although it is preferable that the legislator expressly provides for this possibility in the Law.

Keywords: Remote computer searches – Cybercrime – Criminal investigation – Digital evidence – Right in Confidentiality and Integrity of Information Technology Systems.

Sumário: 1. Introdução e colocação do problema; 2. A utilização de *benware* no Direito comparado; 3. A utilização de *benware* no Direito português; 4. Conclusões. Bibliografia. Jurisprudência.

1. INTRODUÇÃO E COLOCAÇÃO DO PROBLEMA

Devido à crescente utilização das chamadas medidas antiforenses (encriptação das mensagens, esteganografia, utilização de *firewalls*, *botnets*, VPN ou *proxies*, da *Dark Web*, de programas como o TOR, *Freenet* e I2P e de criptomoedas, etc.] e de meios de comunicação como as comunicações por VoIP[1] por parte dos agentes de crimes informáticos (precisamente com a finalidade de se protegerem das medidas de prevenção criminal e de investigação criminal levadas a cabo pelas autoridades), torna-se cada vez mais necessária a utilização, pelas autoridades, de mecanismos e dispositivos que permitam neutralizar a utilização de medidas antiforenses e a proteção proporcionada pela utilização de meios de comunicação como as comunicações por VoIP.

Um desses mecanismos e dispositivos é precisamente a instalação sub-reptícia de programas informáticos (vírus, *worms*, "cavalos de Troia", *keyloggers*, *backdoors*, *spyware*, etc.) que permitam que as autoridades se infiltrem num sistema informático[2] alheio, com o

1 O VoIP (*Voice over Internet Protocol*) é uma forma de comunicar "telefonicamente" através da Internet mediante a utilização de um *software* específico (*Skype Google Talk, Facebook, Whatsapp, Telegram, Viber, Gizmo, Fring, Adphone, Camfrog, MinoCall, VoipBuster, Voipdiscount UOL VoIP*, etc.), permitindo também a comunicação sonora e imagética. Apesar de a comunicação por VoIP se assemelhar a uma chamada telefónica, o seu funcionamento é radicalmente diverso, pois a comunicação via VoIP processa-se nos seguintes termos: um dos interlocutores liga-se a um determinado provedor de acesso à Internet (através de um qualquer sistema informático), autentica-se no programa de VoIP através de um endereço e um código de acesso e "telefona" ao outro interlocutor. As palavras e imagens trocadas entre ambos são convertidas em sinal digital e esses dados são encriptados pelo sistema de VoIP e passam a ser *peer to peer*, circulando os pacotes de dados encriptados na Internet até chegarem ao destinatário, sendo então desencriptados; a comunicação é instantânea, não consiste em nenhuma "caixa de cartas" (como sucede com o correio eletrónico) nem passa por nenhum computador central, o que significa que tudo passa por uma rede de *peer to peer* em contínua modificação e sem nunca estar sob o controlo de terceiros (incluindo a empresa que fornece o serviço de VoIP).

2 Na aceção do art. 2.º, al. a), da Lei n.º 109/2009, de 15 de setembro: «*qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção*».

intuito de obter informações relevantes para a investigação (incluindo a prevenção criminal), que, de outro modo, não poderiam ou dificilmente poderiam obter[3].

No fundo, trata-se de programas que são, usualmente, subsumidos ao conceito de *malware*[4]. Todavia, optamos por denominar este tipo de programas informáticos, quando usados para fins de prevenção ou repressão criminais pelas autoridades (fins legítimos e absolutamente essenciais em qualquer Estado de Direito), *benware*[5].

Tendo em conta a necessária "clandestinidade" da instalação do *benware* nos sistemas informáticos visados – que faz antever o cariz "oculto" das medidas investigatórias cuja execução essa instalação visa permitir –, a utilização do *benware* está intimamente ligada à questão dos métodos "ocultos" de investigação criminal[6]. A instalação do *benware* terá de ser precedida pela "colocação" (e ulterior instalação) do programa no sistema informático na sequência de o utilizador visitar uma determinada página da Internet (em regra, alojada na *Dark Web*) controlada pelas autoridades (permitindo-lhes instalar o programa de forma sub-reptícia) (*watering hole tactic*)[7], por meio do envio do programa de instalação para o sistema informático visado através de um *e-mail* contendo um anexo infetado ou um *link* para um sítio da Internet aparentemente legítimo (sendo o sistema informático infetado

3 Cfr. JONATHAN MAYER, Constitutional Malware, pp. 6-7.

4 Designação que resulta da aglutinação de sílabas das palavras inglesas *malicious* e *software* e que significa programa informático malicioso, precisamente porque se trata de programas informáticos que visam permitir a quem os utiliza infiltrar-se num sistema informático alheio, com o intuito de causar prejuízos ou de obter informações (confidenciais ou não), que, de outro modo, não poderia obter, em regra para fins criminosos (preparação ou execução de crimes ou apagamento de provas de crimes cometidos, incluindo o ataque informático a sistemas informáticos pertencentes às autoridades).

5 *Benign software*: *software* benigno.

6 Os métodos "ocultos" de investigação criminal são os métodos de investigação criminal «*que configuram «uma intromissão nos processos de ação, interação e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto ou dele se apercebam*» e que, por isso, «*continuam a agir, interagir, expressar-se e comunicar de forma "inocente", fazendo ou dizendo coisas de sentido claramente autoincriminatório ou incriminatório daqueles que com elas interagem ou comunicam*», podendo ser "ocultos "por natureza" ou apenas eventualmente "ocultos", consistindo os primeiros naqueles métodos que, pela sua própria natureza, só podem ser utilizados "às ocultas" (ações encobertas, escutas telefónicas, etc.) e os segundos naqueles que tanto podem ser utilizados de forma "aberta" como "às ocultas" (*v.g.* a fixação e comparação de perfis de ADN) (cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 202-203).

7 Esta técnica de introdução do *benware* no sistema informático suscita a questão da "autorização para todos os sistemas informáticos" ("*All computers" warrant*), dado que todas as pessoas que acedam ao *website* (incluindo pesssoas inocentes) verão os seus sistemas informáticos infetados com o *benware* e sujeitos a buscas *online*, o que suscita questões relacionadas com a proporcionalidade da medida, mais concretamente questões relacionadas com a *probable cause* no Direito norte-americano (cfr. DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 762 e ss., e JONATHAN MAYER, Constitutional Malware, p. 60) e com a exigência da existência de uma suspeita *objetiva* e fundada nos termos do Direito português enquanto pressuposto geral, embora implícito, de todos os meios de obtenção de prova que restrinjam direitos fundamentais de forma intensa (cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 472 e ss.).

quando o utilizador clica no *link*) (*social engeneering tactic*) ou mediante a procura e o consequente aproveitamento de alguma fragilidade na segurança do sistema informático (*máxime* falhas de segurança que algum programa ou aplicação instalados contenha)[8] ou mesmo através de atualizações de *software* que o visado permita que sejam efetuadas no sistema informático (reconduzível à *social engeneering tactic*)[9]. No entanto, parece-nos que os criminosos cautelosos dificilmente abrirão o *link* do *e-mail* que contém o *benware*, pelo que o programa terá de ser instalado por alguma das outras formas que referimos.

Tanto a instalação do *benware* como a execução da operação proporcionada pela instalação do *benware* terão de evitar a "atuação" de dispositivos de segurança instalados no sistema informático (antivírus, antispyware, *firewalls*, etc.), a fim de que não apaguem o *benware* nem o detetem ("avisando" o utilizador)[10].

A utilização de *benware* é essencial no caso da busca *online* (*online-Durchsuchung*), que consiste na infiltração sub-reptícia e à distância num sistema informático para observação/monitorização da sua utilização e leitura e eventual cópia dos dados nele armazenados ou acessíveis a partir dele, podendo consistir num único acesso (*Daten-Spiegelung*) ou ocorrer de forma contínua e prolongada no tempo (*Daten-Monitoring*)[11]. A busca *online* caracteriza-se (e diferencia-se das buscas "clássicas" previstas nos arts. 174.º, 176.º e 177.º do CPP e da pesquisa de dados informáticos prevista no art. 15.º da Lei n.º 109/2009, de 15 de setembro) por ser realizada *online*, à distância, "às ocultas", com recurso a meios técnicos e implicar a prévia instalação sub-reptícia, no sistema informático visado, de um programa informático do tipo "cavalo de Troia" (que constitui um mero ato

8 Cfr. MARCUS KÖHLER, "100a", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 410, DAVID SILVA RAMALHO, "O uso de *malware* como meio de obtenção de prova em processo penal", *in* Revista de Concorrência e Regulação, n.º 16, pp. 205 e ss., JONATHAN MAYER, Constitutional Malware, pp. 13 e ss., e DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 736-737, 739 e 741-742.

9 Cfr. JONATHAN MAYER, Constitutional Malware, p. 15, refere que a colocação do *benware* (para posterior instalação e pesquisa) poderá ocorrer de qualquer forma, dando como exemplos "adicionais" a entrada sub-reptícia no local onde está o sistema informático e instalação "presencial" do *software* e a apreensão do sistema informático de um criminoso participante na atividade criminosa sob investigação e executar a diligência a partir desse sistema.

10 Cfr. JONATHAN MAYER, Constitutional Malware, pp. 15-16.

11 Cfr. COSTA ANDRADE, "Bruscamente no Verão Passado" p. 166, e também em "Art. 194.º", *in* Comentário Conimbricense, I, 2.ª Edição, p. 1103, PAULO PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 502 e 541, BÄR, TK-Überwachung, p. 75, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 803 (com mais indicações bibliográficas), e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 226-227, e SUSAN BRENNER, "Law, Dissonance and Remote Computer Searches", *in* North Carolina Journal of Law & Technology, Volume 14, 1, p. 61.

preparatório da execução da busca *online*)[12]. No entanto, ainda que constitua um ato preparatório da execução da busca *online* e/ou de outros meios de obtenção de prova (como a intervenção nas comunicações eletrónicas mediante a vigilância nas fontes e a vigilância acústica e/ou ótica), a instalação de *benware* restringe o direito à confidencialidade e à integridade dos sistemas técnico-informacionais[13], sendo essa a raiz do problema da admissibilidade da utilização de *benware* na ausência de norma legal que a preveja expressamente.

Do mesmo modo, a utilização de *benware* é igualmente essencial no caso da vigilância nas fontes (*Quellen-Telekommunikationsüberwachung* ou *Quellen-TKü*), que consiste na interceção de comunicações (que terão de estar em curso[14]) que sejam encriptadas antes da sua saída do sistema informático "emissor" e desencriptadas depois da sua receção no sistema informático "recetor" (como sucede, por exemplo, nas comunicações por VoIP), sendo assim designada precisamente pelo facto de a interceção só pode ocorrer antes da encriptação ou depois da desencriptação dos dados (pois, após a sua encriptação e antes da sua desencriptação, será impossível de realizar), o que requer a instalação de *software* adequado no sistema informático visado (*v.g.* programas do tipo "cavalo de Troia"). Também na vigilância nas fontes é necessária a prévia instalação de *benware*, o que constitui um mero ato preparatório da execução da interceção das comunicações[15].

Uma outra situação – esta eventual (pois depende do modo como a vigilância acústica e/ou ótica, sob a forma de registo de voz e imagem[16] ou de interceção de comunicações entre

12 Cfr. PAULO PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 502 e 541, COSTA ANDRADE, "Bruscamente no Verão Passado", p 166, e BÄR, TK-Überwachung, p. 75. Relativamente ao modo de instalar esse *sotftware*, *vide* BÄR, *Op. Cit.*, pp. 75-76.

13 Cfr. ROXIN/SCHÜNEMANN, Strafverfahrensrecht, 27.ª Edição, p. 292, e MARCUS KÖHLER, "100a", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, pp. 409-410.

Acerca do direito à confidencialidade e à integridade dos sistemas técnico-informacionais e da sua aplicabilidade no Direito português, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 240 e ss.

14 Cfr. MARCUS KÖHLER, "100a", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 409, e também em "100b", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 420.

15 Como refere BÄR, TK-Überwachung, p. 55, a instalação do *software* necessário para intercetar as comunicações "na fonte" é um ato preparatório da realização das "escutas", sendo em tudo similar à colocação de um localizador de GPS no veículo do visado ou dos microfones no interior da residência onde irá ser realizada a intervenção nas conversações entre presentes; daí que tenhamos de considerar que a instalação sub-reptícia do *software* é um ato que está incluído, por natureza, na autorização da realização das escutas [contra, HOFFMANN-RIEM, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigener informationstechnischer Systeme e BUERMEYER/BÄCKER, Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO, p. 434).

16 Nos termos do art. 6.º da Lei n.º 5/2002, de 11 de janeiro.

presentes[17], é levada a cabo) –, em que poderá ser necessária a utilização de *benware* é precisamente a vigilância acústica e/ou ótica quando deva/tenha de ser levada a cabo mediante a ativação (sub-reptícia) da câmara e/ou do microfone do sistema informático (computador, *smartphone*, *tablet*, etc.) (*captatore informatico*).

Apesar do disposto no art. 19.º, n.º 2, da Lei n.º 109/2009, não nos parece que a utilização de *benware* seja necessária nas ações encobertas *ex se*, sem prejuízo de poder ocorrer – e ocorrer – relativamente a (outros) meios de obtenção de prova utilizados no âmbito de ações encobertas.

Ao contrário do que sucedeu noutras ordens jurídicas, o legislador português não regula expressamente a utilização de *benware*, o mesmo sucedendo com as buscas *online*, a vigilância nas fontes e a ativação sub-reptícia da câmara e/ou do microfone do sistema no âmbito do registo de voz e imagem ou da interceção de comunicações entre presentes.

Deste modo, o problema central deste estudo prende-se com a admissibilidade da utilização do *benware* na investigação criminal à luz do Direito português.

17 Nos termos do art. 189.º, n.º 1, do CPP.

2. A UTILIZAÇÃO DE BENWARE NO DIREITO COMPARADO

Começando pelo Direito alemão[18], o §100a I e III[19] da *Strafprozessordnung* (StPO) prevê expressamente a vigilância nas fontes, que segue o mesmo regime jurídico das escutas telefónicas, devendo ser autorizada pelo Juiz ou, em situações de urgência, pelo Ministério Público (com ulterior ratificação do Juiz no prazo de 3 dias úteis)[20] sempre que existam suspeitas fundadas da prática de um crime previsto no §100a II e a diligência seja indispensável para a descoberta da verdade ou do paradeiro do arguido ou suspeito ou a prova seja, de outra forma, impossível ou muito difícil de obter[21]. Pode ser dirigida contra o arguido ou suspeito ou contra pessoas em relação às quais existam suspeitas fundadas de que recebem ou transmitem mensagens destinadas ou provenientes do arguido ou suspeito[22] durante um período até 3 meses, renovável por períodos até 3 meses[23], mediante despacho fundamentado nos termos do §100e IV StPO, jamais podendo ser obtidas informações subsumíveis à esfera íntima tal como delimitada pela teoria das três esferas[24]. A lei não prevê o modo de instalação do *benware*[25]. Anteriormente à Reforma da StPO de 2017, o §100a StPO não continha qualquer referência à vigilância nas fontes[26].

---

18 O Direito alemão não prevê expressamente a ativação sub-reptícia da câmara e/ou do microfone do sistema informático no âmbito da vigilância acústica (*Lauschangriff*) nem no âmbito da vigilância ótica (*Spähangriff*), o que leva MARCUS KÖHLER, "100b", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 421, a considerar que o uso do *captatore informatico* – que restringe o direito à confidencialidade e à integridade dos sistemas técnico-informacionais – não é admissível à luz do Direito germânico.

19 Na redação que lhe foi dada pela Reforma da StPO de 2017.

De acordo com o §51 II da *Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten* (*Bundeskriminalamtgesetz* – BKAG), *in* http://www.gesetze-im-internet.de/bkag_2018/ (consultada em 09/07/2020), o *Bundeskriminalamt* (Polícia Judiciária Federal) pode realizar vigilâncias nas fontes mediante autorização judicial na prevenção do terrorismo.

20 §100e I StPO.

21 §100a I 1 StPO.

22 §100a III StPO.

23 §100e I StPO.

24 §100d StPO.

25 Como nota MARCUS KÖHLER, "100a", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 410.

26 Por isso e porque a instalação de *benware* restringe o direito à confidencialidade e à integridade dos sistemas técnico-informacionais [cfr. ROXIN/SCHÜNEMANN, Strafverfahrensrecht, 27.ª Edição, p. 292, MARCUS KÖHLER, "100a", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, pp. 409-410, e Sentença do *Bundesverfassungsgericht* de 27/02/2008 (1 BvR 370/07 e 1 BvR 595/07)] –, a admissibilidade da vigilância nas fontes era controvertida na Doutrina alemã. Com efeito, alguns autores pronunciavam-se pela inadmissibilidade, argumentando que, sendo a vigilância nas fontes similar à busca *online* ao nível da execução (o que excluiria a aplicação do §100a StPO), como a StPO não previa este meio de obtenção de prova, também não seria admissível recorrer à vigilância nas fontes em sede de investigação criminal (cfr. KLESCZEWSKI, "Straftataufklärung im Internet – Technische Möglichkeiten und rechtliche Grenzen von Strafprozessualen Ermittlungseingriffen im Internet", *in* Zeitschrift für die gesamte Strafrechtswissenschaft, 2012, p. 742, SINGELNSTEIN, "Möglichkeiten und Grenzen neuerer

Por sua vez, o §100b da StPO[27] prevê a busca *online* em matéria de repressão penal, a qual deve ser autorizada por 3 juízes da Secção (*Kammer*) criminal do *Landgericht*

strafprozessualer Ermittlungsmassnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung&Co", *in* Neue Zeitschrift für Strafrecht, 2012, p. 599, HOFFMANN-RIEM, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigener informationstechnischer Systeme, e BUERMEYER/BÄCKER, Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO, pp. 439-440).

Diversamente, um outro setor da Doutrina pronunciava-se no sentido da admissibilidade, argumentando que havia que diferenciar ambas as realidades, pois a vigilância nas fontes configura uma intervenção nas comunicações eletrónicas que, por razões *meramente técnicas*, poderá ter de ocorrer antes da encriptação ou após a desencriptação dos dados (mas nunca durante o processo comunicacional) e, ao passo que a busca *online* inclui o rastreio do sistema informático na sua globalidade, a vigilância nas fontes limita-se à interceção de comunicações realizadas através de VoIP, sendo que a prévia instalação dos programas necessários para a interceção das comunicações no sistema informático funcionava como uma *Annexkompetenz* relativamente ao §100a, nos termos da qual a autorização para a realização das intervenções nas comunicações legitimava a prévia instalação dos programas informáticos (cfr. BÄR, TK-Überwachung, p. 75, e NACK, "§100a", *in* Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK, 6.ª Edição, p. 476).

27 Anteriormente à entrada em vigor da atual versão do §100b da StPO (no âmbito da Reforma da StPO de 2017), a busca online apenas estava prevista em sede de prevenção criminal do terrorismo (cfr. §§20k VII – atual §49 – da BKAG).

Todavia, ao nível da repressão criminal, apesar de a lei não prever/regular a busca *online*, não existia unanimidade na Jurisprudência alemã, encontrando-se arestos que se pronunciavam pela admissibilidade, aplicando o regime das buscas com base numa interpretação atualista e considerando que a busca *online* não constituía uma restrição intensa de direitos fundamentais [*v.g.* Sentença do *Bundesgerichtshof* de 21/02/2006 (3 BGs 31/06, 3 BJs 32/05 - 4 - (12) - 3 BGs 31/06)] e arestos que consideraram que este meio de obtenção de prova não era admissível, por ausência de previsão legal [*v.g.* Sentença do *Bundesgerichtshof* de 31/01/2007 (StB 18/06).

Por seu turno, o *Bundesverfassungsgericht*, na sua marcante Sentença de 27/02/2008 (1 BvR 370/07 e 1 BvR 595/07), analisou a constitucionalidade do §5 II 11, da Lei de Proteção da Constituição do Estado da Renânia do Norte-Vestefália (*Gesetz über den Verfassungsschutz in Nordrhein-Westfalen*) na versão introduzida pela Lei de 20/12/2006 à luz do art. 2 I, conjugado com os arts. 1 I, 10 I e 19.º I 2, da Lei Fundamental Alemã (Grundgesetz – GG).

O §5 II 11, da Lei de Proteção da Constituição do Estado da Renânia do Norte-Vestefália permitia ao *Bundesamt für Verfassunfsschutz* (Gabinete Federal para a Proteção da Constituição) aceder, de forma sub-reptícia e remota, a sistemas informáticos de indivíduos suspeitos de cometerem ilícitos criminais, a fim de pesquisar os dados aí armazenados ou acessíveis através desse sistema, monitorizar a sua utilização de forma prolongada no tempo e até controlar o próprio sistema informático mediante a prévia instalação sub-reptícia de programas que permitissem esse acesso (*benware*). Nos termos do §3 da Lei de Proteção da Constituição (*Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz* – BVerfSchG), *in* http://www.gesetze-im-internet.de/bverfschg/index.html (consultada em 09/07/2020), compete ao *Bundesamt für Verfassunfsschutz* recolher e analisar informações relativas a atividades ilícitas que atentem contra o Estado de Direito (a "*livre ordem democrática fundamental*"), a existência ou a segurança do Estado federal ou Federação (*Bund*) ou de um Estado federado (*Land*) ou que visem prejudicar ilegalmente a administração dos órgãos constitucionais do Estado federal ou de um Estado federado ou respetivos membros, bem como a atividades que atentem contra a segurança interna ou os interesses externos da República Federal da Alemanha ou de serviços secretos estrangeiros.

O *Bundesverfassungsgericht* considerou que, no caso das buscas *online*, os direitos fundamentais ao sigilo das telecomunicações, à inviolabilidade do domicílio e à autodeterminação informacional não proporcionavam uma tutela eficaz, pelo que, à semelhança do que sucedera com o direito à autodeterminação informacional [Sentença de 15/12/1983 (1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83,1 BvR 440/83 e BvR 484/83)], criou um novo direito fundamental (que, no entendimento do Tribunal, é restringido, e de forma intensa, pela busca *online*): o direito fundamental à confidencialidade e à integridade dos sistemas técnico-informacionais (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*).

E o *Bundesverfassungsgericht* considerou também que a referida norma não cumpria as exigências constitucionais de clareza e certeza jurídica e de proporcionalidade. E estabeleceu as coordenadas que, pela

(Tribunal estadual de 2.ª instância) da área da sede do departamento do Ministério Público competente para a investigação ou, em situações de urgência, pelo Presidente dessa Secção Criminal (com ulterior ratificação de 3 juízes da Secção Criminal no prazo de 3 dias úteis)[28] sempre que existam suspeitas fundadas da prática de um crime previsto no §100b II (cujo catálogo é muito mais restritivo do que o catálogo do §100a) e a diligência seja indispensável para a descoberta da verdade ou do paradeiro do arguido ou suspeito ou a prova seja, de outra forma, impossível ou muito difícil de obter[29]. Pode ser dirigida contra o arguido ou suspeito ou contra pessoas em relação às quais existam suspeitas fundadas de que o arguido ou suspeito utiliza os seus sistemas informáticos e desde que a intervenção apenas nos sistemas informáticos do arguido se mostre insuficiente para a descoberta da verdade ou do paradeiro do arguido ou suspeito ou para a obtenção da prova[30], durante um período até 1 mês, renovável por períodos até 1 mês (e, caso a duração total se prolongue por mais de 6 meses, as ulteriores renovações terão de ser autorizadas pelo *Oberlandesgericht*, o Tribunal supremo de cada um dos *Länder*[31] alemães)[32], mediante despacho fundamentado nos termos do §100e IV StPO, jamais podendo ser obtidas informações subsumíveis à esfera íntima tal como delimitada pela teoria das três esferas[33].

intensidade da restrição do direito à confidencialidade e à integridade dos sistemas técnico-informacionais que o recurso às buscas *online* acarreta, uma futura regulamentação das buscas *online* deveria observar.

Deste modo, de acordo com o Tribunal, só será legítimo o recurso às buscas *online* mediante autorização judicial e desde que exista uma suspeita fundada da existência de um perigo concreto para um bem jurídico particularmente relevante (o Tribunal refere a vida, a integridade física e a liberdade, bem como os bens jurídicos da comunidade cuja lesão ou ameaça de lesão possa pôr em causa os fundamentos ou a existência do Estado ou da Humanidade), devendo a lei conter salvaguardas para proteção da área nuclear da privacidade (a esfera íntima). E, na sua Sentença de 20/04/2016 (1 BvR 966, 1140/09), o *Bundesverfassungsgericht* reafirmou este entendimento, ao afirmar que as restrições intensas de direitos fundamentais por via da utilização de métodos "ocultos" de investigação criminal (como é o caso das buscas *online*) na prevenção criminal só são admissíveis se observarem as exigências do princípio da proporcionalidade, devendo ser limitadas à proteção de bens jurídicos importantes e apenas quanto existir uma suspeita fundada da verificação de um perigo concreto para um desses bens jurídicos, efetivo controlo das operações e suficientes salvaguardas para a proteção da intimidade e do sigilo profissional (com o dever de eliminação dos dados obtidos), só podendo ser restringida a esfera jurídica de terceiros em situações muito limitadas.

Ainda previamente à previsão do recurso à busca *online* na StPO, o *Bundesverfassungsgericht* afirmou a constitucionalidade da interpretação ampla do conceito de telecomunicações do §100a StPO no sentido de incluir a monitorização da navegação na Internet [cfr. Sentença de 06/07/2016 (2 BvR 1454/13)].

28 §100e II StPO.

29 §100b I 1 StPO.

30 §100b III StPO. Todavia, se forem atingidos outros sistemas informáticos, mas essa circunstância for tecnicamente inevitável, as provas obtidas são válidas (cfr. ROXIN/SCHÜNEMANN, Strafverfahtensrecht, 27.ª Edição, p. 292, e MARCUS KÖHLER, "100b", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 422).

31 Estados federados.

32 §100e II StPO.

33 §100d StPO.

Quanto ao Direito italiano[34], prevê-se, no art. 266, 2 e 2-bis, do *Codice di procedura penale*, o uso do *captatore informatico*[35], que consiste num *software* do tipo "cavalo de Troia" que é sub-repticiamente instalado num sistema informático para permitir a ativação do microfone para audição/gravação de conversações, a geolocalização do sistema informático e a ativação da câmara para vigilância ótica (incluindo tirar fotografias). O *captatore informatico* constitui um meio de execução da interceção de comunicações entre presentes e não um meio de obtenção de prova "autónomo", sendo utilizado nos casos em que é admissível a interceção de comunicações entre presentes, que tanto pode ocorrer em locais que gozam da tutela constitucional do domicílio (locais indicados no art. 614 do *Codice penale*) como em locais privados que não gozam dessa tutela.

Nos termos do art. 266, 2 e 2-bis, do *Codice di procedura penale*, a interceção de comunicações entre presentes (e o *captatore informatico*) terá de ser autorizada pelo Juiz ou, em caso de urgência, pelo Ministério Público (com ulterior ratificação do Juiz no prazo de 48 horas contadas da comunicação, que deve ocorrer no prazo máximo de 24 horas) por despacho fundamentado[36] sempre que existam suspeitas fundadas da prática de um crime previsto no art. 266, 1 e 2-bis, e a diligência seja indispensável para a descoberta da verdade ou do paradeiro do arguido ou suspeito ou a prova seja, de outra forma, impossível ou muito difícil de obter[37]. No caso da interceção de comunicações entre presentes "domiciliária", terão de existir fundados indícios de que a atividade criminosa (também) está a ocorrer nesse local[38]; todavia, nos termos do art. 13 do *Decreto legge* n.º 151 de 1991, convertido pela *Legge* n.º 203 de 1991, quando se trate de processos relativos à criminalidade organizada, é

34 No Direito italiano não existe qualquer previsão expressa da busca *online* nem da vigilância nas fontes.

35 Anteriormente à previsão legal do *captatore informatico*, as *Sezioni Unite* da *Suprema Corte de Cassazione* haviam fixado jurisprudência no sentido da admissibilidade da utilização deste meio tecnológico nas investigações relativas à criminalidade organizada, entendendo que se trata apenas de um meio de execução das interceções de comunicações entre presentes, dispensando o art. 13 do *Decreto legge* n.º 151 de 1991, convertido pela *Legge* n.º 203 de 1991, a exigência de que a atividade criminosa não esteja a ocorrer no local protegido pela tutela do domicílio onde deverá ser realizada a interceção (derrogando, assim, o art. 266, 2, do *Codice di procedura penale*), pelo que nada impede a sua utilização (tendo em conta a natureza "itinerante" dos sistemas informáticos da atualidade como o *smartphone*, o *tablet* ou o computador); diversamente, nos demais casos, em que há que observar o disposto no art. 266,2, a *Corte de Cassazione* considerou que já não será admissível, uma vez que, no momento da concessão da autorização, não é possível prever em que locais "domiciliários" o *captatore informatico* poderia vir a ser instalado no sistema (cfr. Sentença das *Sezioni Unite* da *Suprema Corte de Cassazione* de 28/04/2016-01/07/2016, n.º 26889).

No mesmo sentido, cumpre ainda referir as Sentenças da *Suprema Corte di Cassazione* de 30/05/2017-20/10/2017, n.º 48370 (Sez. V), 08/03/2018-09/10/2018, n.º 45486 (Sez. VI), e 25/06/2019-17/12/2019, n.º 50972 (Sez. I).

36 Art. 267, 1, 2 e 2-bis, do *Codice di procedura penale*.

37 Art. 267, 1, do *Codice di procedura penale*.

38 Art. 267, 2, do *Codice di procedura penale*.

possível a realização de interceções de comunicações entre presentes "domiciliárias" mesmo que a atividade criminosa não esteja a ocorrer nesse local.

Nos casos de *periculum in mora* em que a autorização seja dada pelo Ministério Público e seja utilizado o *captatore informatico*, terá de estar em causa a investigação de crimes previstos no art. 51, 3-bis e 3-quater (*grosso modo*, crimes no âmbito da criminalidade organizada e do terrorismo), e crimes contra a Administração Pública praticados por funcionários públicos ou por pessoas encarregadas do serviço público puníveis com pena de prisão cujo limite máximo seja igual ou superior a 5 anos[39] (o que significa que o legislador considera que a utilização do *captatore informatico* aumenta a danosidade da interceção de comunicações entre presentes, ao ponto de restringir o âmbito dos casos em que o Ministério Público pode lançar mão de um procedimento *ex abrupto* face às situações de interceção de comunicações entre presentes em que não é utilizado o *captatore informatico*).

No que tange à duração da medida, nos termos do art. 267, 3, do *Codice di procedura penale*, após o Juiz autorizar (ou ratificar a autorização do Ministério Público) a interceção de comunicações entre presentes (com ou sem utilização do *captatore informatico*), o Ministério Público terá de proferir um despacho em que determina a modalidade da interceção e a sua duração[40]. A interceção de comunicações entre presentes não pode ter lugar uma duração superior a 15 dias, embora podendo ser renovada[41].

Relativamente ao Direito espanhol, as buscas *online* (*registros remotos sobre equipos informáticos*) estão previstas nos arts. 588 *septies* a, b e c da *Ley de Enjuiciamiento Criminal* (LECr). Nos termos do art. 588 *septies* a, n.º 1, da LECr, a utilização de dados e códigos de identificação e a instalação de *software* que permita o acesso remoto mediante o uso de meios técnicos a um sistema informático ou suporte externo de armazenamento em massa de dados informáticos sem conhecimento do seu proprietário ou utilizador[42] terão de ser autorizadas pelo Juiz[43] e desde que se trate da investigação de crimes cometidos no âmbito

39 Art. 267, 2-bis, do *Codice di procedura penale*.
40 Cfr. TONINI, Manuale di Procedura Penale, 12.ª Edição, p. 385.
41 Art. 267, 3, do *Codice di procedura penale*.
42 De acordo com LORENA BACHMAIER WINTER, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *in* Boletín del Ministerio de Justicia, Núm. 2195, p. 14, a busca *online* prevista nos arts. 588 *septies* a, b e c da LECr não permite a interceção de comunicações informáticas.
43 Devendo o despacho de autorização observar as exigências do n.º 2 desse art. 588 *septies* a e dos arts. 588 *bis* c, n.º 3, e 588 *sexies* c, n.º 1, igualmente da LECr. LORENA BACHMAIER WINTER, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *in* Boletín del Ministerio de Justicia, Núm. 2195, pp. 19-20, refere que o legislador espanhol, ao contrário do que sucede no art. 588 *ter* d (relativo à intervenção nas comunicações telefónicas e telemáticas), não previu a possibilidade de lançar mão

de organizações criminosas, de terrorismo, de crime cometidos contra menores ou incapazes, contra a Constituição, de traição e relativos à defesa nacional ou de crimes cometidos com utilização de meios informáticos ou de qualquer outra tecnologia da informação ou das comunicações ou serviço de comunicações[44]. O âmbito da busca *online* poderá ser ampliado mediante autorização judicial sempre que existam razões fundadas para crer que os dados que as autoridades pretendem obter estão armazenados noutro sistema informático o noutra parte do sistema informático alvo da busca *online*[45]. A busca *online* só pode ser autorizada por um prazo máximo de 1 mês, prorrogável até ao limite máximo de 3 meses[46].

No Direito norte-americano não existe legislação específica relativamente à utilização de *benware* na investigação criminal, à exceção da *Rule 41* das *Federal Rules of Criminal Procedure*, cuja epígrafe é *Search and Seizure* (buscas e apreensões), e na qual foi introduzida, em 2016, uma regulamentação específica para as pesquisas em dispositivos informáticos e apreensões de dados informáticos armazenados em tais dispositivos realizadas de forma remota.

Contudo, já antes dessa alteração legislativa se admitia a utilização das buscas *online*, contanto que tal não violasse a Quarta Emenda à Constituição.

Inicialmente, a Jurisprudência do *Supreme Court of the United States* entendia que só existiria violação da Quarta Emenda nos casos em que a busca e/ou a apreensão implicassem a entrada física em propriedade alheia (*Physical Trespass Doctrine*)[47]. Todavia, o mesmo Tribunal, na marcante Sentença Katz *v.* United States[48], abandonou a *Physical Trespass Doctrine* e ampliou o âmbito de proteção da Quarta Emenda, entendendo que essa tutela,

---

de procedimentos *ex abrupto* em situações de *periculum in mora* nem se mostra possível aplicar o mencionado preceito às buscas *online*.

44 De acordo com LORENA BACHMAIER WINTER, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *in* Boletín del Ministerio de Justicia, Núm. 2195, pp. 9, 10 e 11, terá de existir uma suspeita fundada (e não apenas uma suspeita inicial e muito menos conjeturas ou suposições) da prática de um desses crimes (que, para existir, poderá implicar a realização prévia de outras diligências), sendo que a lei não fixa qualquer exigência quanto à moldura penal aplicável ao crime em causa (cfr. pp. 14-15).

45 Art. 588 *septies* a, n.º 3, da LECr.

46 Art. 588 *septies* c da LECr. LORENA BACHMAIER WINTER, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *in* Boletín del Ministerio de Justicia, Núm. 2195, p. 18, critica a redação da lei, entendendo que deveria ter clarificado a questão do início da contagem do prazo da duração da busca *online*, que, pela sua natureza, implica a prévia instalação do *benware*, podendo decorrer um determinado lapso de tempo até que as autoridades logrem essa instalação tornando o prazo máximo de 3 meses insuficiente; por isso, a autora entende que a contagem do prazo deveria iniciar-se a partir da instalação do *benware*.

47 Cfr. Sentenças Olmstead *v.* United States (1928) e Goldman *v.* United States (1942) do *Supreme Court of the United States*.

48 Sentença Katz *v.* United States do *Supreme Court of the United States* (1967).

para além de não se limitar à apreensão de bens corpóreos e incluir também a interceção e gravação de conversações e comunicações[49], não abrangia apenas espaços, mas também as pessoas, contanto que exista, no caso concreto, uma expectativa razoável de privacidade da pessoa visada (pelo que a violação da Quarta Emenda não depende da entrada física das autoridades na propriedade privada, mas da existência de uma expectativa razoável de privacidade); e, na situação *sub juditio* nessa Sentença, o *Supreme Court of the United States* considerou que a realização de escutas através de um dispositivo eletrónico de escuta e gravação colocado na parte externa da cabine telefónica a partir da qual o arguido realizara chamadas telefónicas relativas a apostas ilegais estava abrangida pelo âmbito de tutela da Quarta Emenda.

Ainda de acordo com a referida Sentença Katz *v.* United States, a existência de uma expectativa razoável de privacidade depende da verificação de dois pressupostos cumulativos: (1) a pessoa que invoca a Quarta Emenda ter uma expectativa subjetiva de privacidade e (2) a Sociedade reconhecer que essa expectativa é razoável[50].

Para além da demonstração da existência de uma expectativa razoável de privacidade, quem invocar a Quarta Emenda terá de demonstrar que a sua privacidade e/ou a sua propriedade (e não a de terceiros) foram lesadas pela busca e/ou pela apreensão, o que implica saber se essa pessoa alegou que um seu interesse legalmente protegido foi efetivamente lesado (*injury of fact*) e se essa alegação assenta nos seus direitos ou interesses ou num direito ou interesse de um terceiro[51].

Assim, considera-se que as buscas e apreensões (incluindo as pesquisas em sistemas informáticos e as apreensões de dados informáticos[52]) restringem a Quarta Emenda[53], que

49 Como o *Supreme Court of the United States* também já havia afirmado na sua Sentença Silverman *v.* United States (1961).
50 Cfr. Sentença Katz *v.* United States do *Supreme Court of the United States* (1967).
51 Cfr. TERI DOBBINS BAXTER, "Great (and Reasonable) Expectations: Fourth Amendment Protection for Attorney-Client Communications", *in* Seattle University Law Review 35, pp. 39-40, e Sentença Rakas *v.* Illinois do *Supreme Court of the United States* (1978).
52 Cfr. THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, p. 208, SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, pp. 12-13, e Sentenças United States *v.* Lin Lyn Trading, Ltd. do *United States Court of Appeals, 10th Circuit* (1998) e United States *v.* Hunter do *United States Court for the District of Vermont* (1998).
53 Cfr. TERI DOBBINS BAXTER, "Great (and Reasonable) Expectations: Fourth Amendment Protection for Attorney-Client Communications", *in* Seattle University Law Review 35, pp. 40 e ss., THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, pp. 197-198, ERIC D. MCARTHUR, "The Search and Seizure of Privileged Attorney-Client Communications", *in* University of Chicago Law Review, Vol. 72, p. 732, e Sentenças Andresen *v.* Maryland do *Supreme Court of the United States* (1976), Rakas *v.* Illinois do *Supreme Court of the United States* (1978), Klitzman, Klitzman and Gallagher v. Krut do *United States Court of Appeals, 3rd Circuit* (1984), United States *v.* Lin Lyn Trading, Ltd. do *United States Court of Appeals, 10th Circuit* (1998), Ferguson *v.* City of Charleston do *United States Court of Appeals, 4th Circuit* (2001), United States *v.* Hunter do *United*

proíbe a realização de buscas e apreensões desrazoáveis (devendo a razoabilidade da diligência ser aferida à luz da decisão que concede a autorização e do modo como a diligência é executada)[54], embora apenas sendo aplicável às buscas e apreensões realizadas no território dos Estados Unidos ou que incidam sobre sistemas informáticos ou dados informáticos localizados no território do Estados Unidos[55].

Entende-se que se estará perante buscas e apreensões desrazoáveis, por exemplo, nos casos em que o seu objeto seja excessivamente amplo[56] (*máxime* no caso de mandados de busca "gerais") ou quando sejam realizadas sem autorização judicial (*warrant*) ou fora do âmbito das exceções à exigência de autorização judicial (*v.g.* consentimento do visado, situação de *periculum in mora* para a obtenção da prova ou para a segurança dos agentes ou de terceiros ou o local a buscar não se situar no território dos Estados Unidos)[57].

Contudo, a Quarta Emenda apenas protege contra buscas e apreensões que sejam realizadas pelas autoridades ou por particulares atuando sob a direção das autoridades[58], não incluindo os casos em que as buscas e as apreensões são realizadas por particulares sem qualquer direção das autoridades nem as buscas e apreensões realizadas pelas autoridades quando se limitem a "replicar" buscas e/ou apreensões anteriormente realizadas por

---

States Court for the District of Vermont (1998) e United States v. Skeddle do *United States District Court for the North District of Ohio, Western Division* (1997).

54 Cfr. LAFAVE/ISRAEL/KING/KERR, Criminal Procedure, 5.ª Edição, p. 151, SHELLY MOTT DIAZ, "A Guilty Attorney with Innocent Clients: Invocation of the Fourth Amendment to Challenge the Search of Privileged Information", *in* Mississippi Law Journal, Volume 79, p. 60, e Sentenças Andresen *v.* Maryland do *Supreme Court of the United States* (1976), Zurcher *v.* Stanford Daily do *Supreme Court of the United States* (1978) e United States *v.* Hunter do *United States Court for the District of Vermont* (1998)

55 A Jurisprudência norte-americana tem entendido que a Quarta Emenda não abrange as buscas e apreensões e, deste modo, as buscas *online* e outros acessos remotos a sistemas informáticos e/ou dados informáticos localizados no Estrangeiro e pertencentes a estrangeiros não residentes nos Estados Unidos, como aconteceu nos Casos Gorshkov e Ivanov, em que se considerou não abrangida pela tutela da Quarta Emenda, uma busca *online* realizada pelo FBI nos sistemas informáticos (localizados na Rússia) de dois cidadãos russos (Gorshkov e Ivanov) não residentes nos Estados Unidos sem autorização judicial (e sem que existisse qualquer situação que a dispensasse) (acerca deste caso, *vide* SUSAN BRENNER, "Law, Dissonance and Remote Computer Searches", *in* North Carolina Journal of Law & Technology, Volume 14, pp. 49-50).

56 Cfr. SHELLY MOTT DIAZ, "A Guilty Attorney with Innocent Clients: Invocation of the Fourth Amendment to Challenge the Search of Privileged Information", *in* Mississippi Law Journal, Volume 79, pp. 68-69, e Sentenças Andresen *v.* Maryland do *Supreme Court of the United States* (1976), Klitzman, Klitzman and Gallagher v. Krut do *United States Court of Appeals, 3rd Circuit* (1984), United States *v.* Hall do *United States Court of Appeals, 7th Circuit* (1998), United States *v.* Hunter do *United States Court for the District of Vermont* (1998) e O' Connor *v.* Johnson do *Supreme Court of Minnesota* (1979).

57 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, pp. 7 e 16-17.

58 Cfr. TERI DOBBINS BAXTER, "Great (and Reasonable) Expectations: Fourth Amendment Protection for Attorney-Client Communications", *in* Seattle University Law Review 35, pp. 46-47, THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, pp. 232 e ss., e Sentenças Smith *v.* Maryland do *Supreme Court of the United States* (1979), United States *v.* Jacobsen do *Supreme Court of the United States* (1984) e United States *v.* Hall do *United States Court of Appeals, 7th Circuit* (1998).

particulares que não atuem sob a direção das autoridades[59]. Todavia, a tutela da Quarta Emenda já abrange a parte da busca ou apreensão em que as autoridades vão além da mera "replicação" da busca ou apreensão realizada pelo particular *motu proprio*[60].

A Quarta Emenda não impede, em absoluto, a realização de buscas e apreensões visando pessoas que não sejam arguidas nem suspeitas, desde que exista autorização judicial[61] (*warrant*) ou uma exceção à exigência de autorização judicial (*v.g.* consentimento do visado, situação de *periculum in mora* para a obtenção da prova ou para a segurança dos agentes ou de terceiros ou o local a buscar não se situar no território dos Estados Unidos[62]), *probable cause* (*i.e.*, uma probabilidade fundada de que a diligência permitirá obter provas do crime sob investigação[63], visando-se evitar *phishing expeditions*[64]) e o local a ser alvo da busca e os elementos a apreender estejam suficientemente especificados na autorização judicial, para que as autoridades que executarem a diligência saibam, com razoável certeza, quais os locais a buscar e quais os elementos a apreender[65].

---

59 *V.g.* quando um técnico informático a quem o visado entregou o computador para reparação visiona os ficheiros armazenados nesse computador e informa as autoridades acerca daquilo que encontrou e as autoridades apreendem o computador e pesquisam os dados aí armazenados.

60 Cfr. THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, pp. 241 e ss., e Sentenças Walter *v.* United States do *Supreme Court of the United States* (1980), United States *v.* Jacobsen do *Supreme Court of the United States* (1984) e United States *v.* Hall do *United States Court of Appeals, 7th Circuit* (1998).

61 De acordo com as Sentenças Chimel v. California (1969) e Coolidge v. New Hampshire (1971) do *Supreme Court of the United States*, a autorização do Juiz, enquanto entidade neutra, visa precisamente obstar ao arbítrio nas restrições da Quarta Emenda.

62 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, pp. 16-17, e Sentença Coolidge v. New Hampshire do *Supreme Court of the United States* (1971).

63 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, p. 13, e DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), p. 761.

64 Cfr. DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), p. 761, e Sentenças Katz *v.* United States (1967), Chimel v. California (1969) e Coolidge v. New Hampshire (1971) do *Supreme Court of the United States*.

65 Cfr. TERI DOBBINS BAXTER, "Great (and Reasonable) Expectations: Fourth Amendment Protection for Attorney-Client Communications", *in* Seattle University Law Review 35, pp. 43 e 64, ERIC D. MCARTHUR, "The Search and Seizure of Privileged Attorney-Client Communications", *in* University of Chicago Law Review, Vol. 72, p. 732, THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, p. 270, SHELLY MOTT DIAZ, "A Guilty Attorney with Innocent Clients: Invocation of the Fourth Amendment to Challenge the Search of Privileged Information", *in* Mississippi Law Journal, Volume 79, p. 61, e Sentenças Zurcher *v.* Stanford Daily do *Supreme Court of the United States* (1978), United States *v.* Hunter do *United States Court for the District of Vermont* (1998), National City Trading Corp. *v.* United States do *United States Court of Appeals, 2nd Circuit* (1980) e O' Connor *v.* Johnson do *Supreme Court of Minnesota* (1979).

No entanto, relativamente à delimitação do âmbito das buscas e dos documentos a serem apreendidos, o *Supreme Court of the United States*, na Sentença Andresen *v.* Maryland (1976), entendeu que existem perigos graves inerentes à execução de uma busca e apreensão dos documentos que não estão necessariamente presentes numa busca que vise a apreensão de objetos físicos (cuja relevância é mais facilmente verificável), visto que, no caso das buscas e apreensões de documentos, irão ser analisados documentos irrelevantes para a investigação (para identificar e apreender aqueles cuja apreensão foi autorizada), o que impõe a adoção de procedimentos que permitam minimizar as restrições da privacidade. Mas, o Tribunal também referiu que, no caso de

No caso de apreensões de elementos probatórios que estejam na posse de um terceiro, o proprietário que tiver confiado esses elementos a esse terceiro não tem legitimidade para impugnar a medida por violação da Quarta Emenda, salvo se demonstrar a existência de uma expectativa razoável de privacidade[66]. Assim, por exemplo, a pessoa contra quem forem utilizadas as provas obtidas através de uma busca e apreensão visando um espaço pertencente a um terceiro inocente não tem legitimidade para invocar a violação da Quarta Emenda[67], o mesmo sucedendo com quem ocupe ilegitimamente o local que é objeto da busca[68].

No que tange especificamente às buscas *online* (*remote computer searches*), vem-se entendendo que as buscas *online* constituem uma busca (*search*) para efeitos de proteção no âmbito da Quarta Emenda, pelo que os cidadãos e estrangeiros residentes no território dos Estados Unidos têm uma expectativa razoável de privacidade (*reasonable expectation of privacy*) relativamente aos seus sistemas informáticos e dados informáticos[69], salvo se

---

investigações complexas, é possível que o esquema criminoso só possa ser provado reunindo muitos elementos de prova, incluindo elementos que, considerados isoladamente, pouco ou nada demonstrariam, sendo que a complexidade de um esquema criminoso não pode ser usada como um escudo para evitar a deteção quando exista causa provável para crer que um crime foi cometido e que as provas do seu cometimento estão na posse do visado. Daí que, em tais casos, uma busca e apreensão com base num mandado que delimite o âmbito da diligência de uma forma mais "geral" não viole a Quarta Emenda. De acordo com SHELLY MOTT DIAZ, *Op. Cit.*, p. 60, e THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, p. 197, este entendimento tem sido seguido pelos demais Tribunais para sustentarem a admissibilidade de buscas e apreensões de documentos com um objeto mais amplo.

66 Cfr. Sentenças Couch *v.* United States (1973), United States *v.* Miller (1976) e Rakas *v.* Illinois (1978), todas do *Supreme Court of the United States.*

67 Cfr. Sentença Rakas *v.* Illinois do *Supreme Court of the United States* (1978).

68 Assim, Sentença Rakas *v.* Illinois do *Supreme Court of the United States* (1978).

69 Cfr. SUSAN BRENNER, "Law, Dissonance and Remote Computer Searches", *in* North Carolina Journal of Law & Technology, Volume 14, 1, pp. 51-52 e 61, e também em Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, pp. 8, 10 e 12, DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 755 e ss., JONATHAN MAYER, Constitutional Malware, pp. 19 e ss., 26 e 39, e Sentenças Riley *v.* California do *Supreme Court of the United States* (2014), Guest *v.* Leis do *United States Court of Appeals, 6th Circuit* (2001), United States *v.* Lifshitz do *United States Court of Appeals, 2nd Circuit* (2004), United States v. Forrester do *United States Court of Appeals, 9th Circuit* (2007), United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008) e Commonwealth *v.* Cormier do *Massachussets Superior Court* (2011).

De notar que DEVIN M. ADAMS, *Idem*, pp. 756 e ss., considera, inclusivamente, que também o ato de envio do *benware* para o sistema informático visado restringe a Quarta Emenda; diversamente, JONATHAN MAYER, *Idem*, p. 52, entende que tal deverá ser aferido caso a caso, excluindo a restrição da Quarta Emenda nos casos de envio remoto do *benware* no sistema informático visado.

Mas já será diferente quanto à instalação do *benware* e à neutralização dos dispositivos de proteção do sistema informático (para não apagarem nem "avisarem" o visado acerca da presença do *benware*), em que se entende que essa neutralização, ao constituir uma quebra da integridade do sistema informático, restringe a Quarta Emenda (cfr. JONATHAN MAYER, *Idem*, p. 53); contudo, se esta é a regra, existem exceções, que dispensam a obtenção de uma autorização judicial para instalar o *benware*, como sucede, por exemplo, com as redes de partilha de ficheiros *peer-to-peer* quando se "anunciem" no âmbito de redes públicas, mas não quando tal ocorra no âmbito de redes privadas, ainda que sem qualquer proteção [cfr. JONATHAN MAYER, *Idem*, pp. 53, 54, e Sentenças United States v. Ganoe do *United States Court of Appeals, 9th Circuit* (2008) e United States

tiverem exposto tais dados ao conhecimento de terceiros através da instalação e utilização de *software* de partilha de dados que exponha pelo menos parte desses dados a outros utilizadores[70] ou do envio de mensagens após a chegada destas ao destinatário[71]. E entende-se também que a mera circunstância de aceder à Internet não retira ao respetivo titular a expectativa razoável de privacidade[72], o mesmo valendo nos casos em que outras pessoas tenham, ocasionalmente, acesso ao sistema informático[73].

Todavia, tem-se entendido que as informações disponibilizadas pelo cliente ao fornecedor de serviços (provedor) não estão protegidas pela Quarta Emenda em virtude de não existir qualquer expectativa razoável de privacidade a partir do momento em que as partilhou com um terceiro (o fornecedor de serviço)[74], o que inclui os dados relativos à subscrição do serviço[75], os dados de tráfego e os endereços de IP dos *websites* que o utilizador da Internet visita[76] e o tamanho dos ficheiros e outros dados que não sejam relativos ao conteúdo a que o fornecedor de serviço tenha forçosamente acesso no âmbito da prestação de serviços[77].

Também as buscas *online* têm de ser alvo de uma autorização judicial ("*Trojan warrant*") – que terá de identificar (caso seja conhecido[78]) o(s) sistema(s) informático(s)

---

v. Perrine do *United States Court of Appeals, 10th Circuit* (2008)]; JONATHAN MAYER, *Idem*, pp. 54 e ss., refere outras possíveis exceções (*in abstracto*), mas que rejeita na sua totalidade.

Por fim, JONATHAN MAYER, *Idem*, pp. 21 e ss., leva a cabo uma análise da proteção, no âmbito da Quarta Emenda, das buscas *online* na vertente da "Quarta Emenda centrada no dispositivo" ("*Device-Centric Fourth Amendment*") – tendo em conta o entendimento tradicional relativo ao âmbito de proteção da Quarta Emenda – e na vertente da "Quarta Emenda centrada nos dados" ("*Data-Centric Fourth Amendment*") – tendo em conta a nova conceção resultante da Sentença Katz *v.* United States –, acabando por concluir que a Quarta Emenda tutela, quer o sistema informático *ex se* quer os dados informáticos.

70 Cfr. SUSAN BRENNER, "Law, Dissonance and Remote Computer Searches", *in* North Carolina Journal of Law & Technology, Volume 14, 1, p. 61, e Sentença United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008).

71 Cfr. Sentenças United States *v.* Lifshitz do *United States Court of Appeals, 2nd Circuit* (2004) e United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008).

72 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, pp. 10-11, e Sentença United States *v.* Heckenkamp do *United States Court of Appeals, 9th Circuit* (2007).

73 Cfr. Sentenças Leventhal v. Knapek do *United States Court of Appeals, 2nd Circuit* (2001) e United States *v.* Heckenkamp do *United States Court of Appeals, 9th Circuit* (2007).

74 Cfr. Sentenças Guest *v.* Leis do *United States Court of Appeals, 6th Circuit* (2001) e United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008).

75 Assim, Sentenças Guest *v.* Leis do *United States Court of Appeals, 6th Circuit* (2001) e United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008).

76 Cfr. DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 754-755, e Sentenças United States v. Forrester do *United States Court of Appeals, 9th Circuit* (2007) e United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008).

77 Cfr. Sentenças United States v. Forrester do *United States Court of Appeals, 9th Circuit* (2007) e United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008).

78 Em tais situações, JONATHAN MAYER, Constitutional Malware, p. 59, considera que será sempre possível definir um conjunto de critérios objetivos baseados nas circunstâncias do caso sob investigação, a fim de que o

que irá(ão) ser alvo da pesquisa e os ficheiros que deverão ser procurados e apreendidos (especificando o tipo de dados que os agentes policiais estão autorizados a buscar e apreender, como, por exemplo, indicando que irão ser buscados dados relativos a pornografia infantil, a terrorismo ou a tráfico de estupefacientes) – e terá de existir *probable cause* (ou seja, terão de existir circunstâncias objetivas que sejam suficientes para criar num *bonus pater familias* a convicção de que irão ser encontradas informações relevantes para a investigação no sistema informático que irá ser pesquisado[79])[80]. Contudo, no caso da autorização judicial, a mesma poderá ser dispensada sempre que ocorra alguma das exceções à exigência da autorização, designadamente o consentimento do visado, a verificação de uma situação de *periculum in mora* (*exigent circumstances)* quanto à segurança dos agentes policiais ou de terceiros ou quanto à perda de provas essenciais para a investigação ou o sistema informático que irá ser alvo da busca *online* não se encontrar no território dos Estados Unidos[81].

Discutida é a aplicação da *Plain View Doctrine*[82], existindo autores e Jurisprudência que negam a sua aplicabilidade às pesquisas em sistemas informáticos (incluindo as buscas *online*), apenas sendo admissível apreender os dados informáticos especificados na

benware, quando for instalado, o seja num sistema informático que satisfaça as exigências da Quarta Emenda em matéria de *probable cause*, a fim de obstar a *fishing expeditions*.

79 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, p. 13, e DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 66-67.

80 Assim, SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, p. 14, DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 760 e ss., e Sentenças Katz *v.* United States (1967), Chimel v. California (1969), Coolidge v. New Hampshire (1971) e Riley *v.* California (2014) do *Supreme Court of the United States* e United States v. Wey do *United States District Court for the Southern District of New York* (2017).

81 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, pp. 16-17, e Sentenças Riley *v.* California do *Supreme Court of the United States* (2014), United States *v.* Gorshkov do *United States District Court for the Western District of Washington* (2001) e United States v. Ivanov do *United States District Court for the District of Connecticut* (2001).

82 De acordo com a *Plain View Doctrine*, poderão ser apreendidos elementos que sejam encontrados no decurso de uma busca que não tenham qualquer relação com o crime cuja investigação motivou a diligência, desde que se verifiquem três pressupostos: (1) uma prévia intrusão lícita (*v.g.* uma busca ou pesquisa informática regularmente autorizadas), (2) o objeto em causa ter sido observado no estrito âmbito da diligência definido pela autorização judicial (*v.g.* se for procurada uma arma com determinadas dimensões, não será lícito aos investigadores realizarem buscas em locais em que tal arma, pelas suas dimensões, manifestamente não possa estar, pelo que o objeto fortuitamente encontrado terá de estar num local em que a arma procurada pudesse ser encontrada) e (3) o caráter criminoso do objeto fortuitamente encontrado ser manifesto (acerca da *Plain View Doctrine*, *vide* THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, pp. 275-276).

autorização da apreensão (*Special Doctrine*)[83], mas também não faltando Doutrina e Jurisprudência que afirmam a sua aplicabilidade em tais situações[84].

Quanto à duração da busca *online*, nos termos da *Rule 41* das *Federal Rules of Criminal Procedure*, a sua duração máxima é de 14 dias, findos os quais, ou é obtida nova autorização judicial ou haverá que desinstalar o *benware*.

A Jurisprudência norte-americana também já admitiu a vigilância ótica mediante a ativação *online* da câmara do sistema informático na Sentença In re Warrant to Search Target Computer at Premises Unknown do *United States District Court for the Southern District of Texas*[85]. O Tribunal, aplicando os critérios definidos pelo *Supreme Court of the United States* na Sentença Berger *v.* New York[86] relativamente às escutas telefónicas e à vigilância acústica e constantes do *Wiretap Act* (§2511 do *United States Code*[87]) e aplicados, por analogia, à vigilância ótica pelo *United States Court of Appeals (5th Circuit)* na Sentença United States *v.* Cuevas-Sanchez[88], admitiu a vigilância ótica mediante a ativação *online* da câmara do sistema informático, embora considerando que terá de existir *probable cause* e autorização do Juiz, devendo tal autorização (1) justificar a insuficiência de outros meios de obtenção de prova para obter as provas no caso concreto (seja porque foram utilizados sem êxito seja porque, de acordo com uma apreciação razoável, se afiguram *ab initio* insuficientes ou perigosos), (2) descrever especificamente o tipo de comunicação que se pretende intercetar (*in casu*, o tipo de imagem que se pretende recolher) e o crime concretamente em causa no caso concreto, (3) indicar a duração da autorização, que não deve exceder o necessário para atingir o objetivo da autorização nem, em qualquer caso, mais de 30 dias (embora sejam possíveis extensões) e (4) identificar as medidas que serão

83 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, p. 17 (embora apenas quanto às buscas *online*, pelo facto de serem realizadas com utilização de meios técnicos), e Sentença United States v. Carey do *United States Court of Appeals, 10th Circuit* (1999).
84 Cfr. THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, pp. 275-276, e Sentença State *v.* Schroeder do *Court of Appeals of Wisconsin* (2000).
85 Sentença In re Warrant to Search Target Computer at Premises Unknown do *United States District Court for the Southern District of Texas* (2013) (concordando, *vide* JONATHAN MAYER, Constitutional Malware, pp. 73-74).
86 Sentença Berger *v.* New York do *Supreme Court of the United States* (1967).
87 Relativo ao crime de interceção de comunicações telefónicas, orais e eletrónicas [*in* *https://www.law.cornell.edu/uscode/text/18/2511* (consultado em 20/07/2020)].
88 Sentença United States *v.* Cuevas-Sanchez do *United States Court of Appeals, 5h Circuit* (1987); já anteriormente, o *2nd Circuit* do mesmo *United States Court of Appeals*, na Sentença United States *v.* Biasucci, adotara o mesmo entendimento.

adotadas para garantir que a vigilância será limitada apenas à prossecução dos fins para os quais a autorização foi concedida[89].

89 No fundo, exige-se aquilo que a Doutrina e a Jurisprudência norte-americanas designam por "*super warrant*" da Quarta Emenda (relativos aos meios de obtenção de prova mais intensamente restritivos dos direitos fundamentais protegidos por esta Emenda) face ao *warrant* que a mencionada Emenda impõe, por exemplo, em matéria de buscas (incluindo as revistas) e apreensões "tradicionais". De referir que JONATHAN MAYER, Constitutional Malware, pp. 75 e ss., entende que a autorização para a realização de uma busca *online*, pela sua grande danosidade em termos de restrição de direitos fundamentais, deverá observar os requisitos do "*super warrant*" e não os requisitos (menos exigentes) do *warrant* "normal".

3. A UTILIZAÇÃO DO *BENWARE* NO DIREITO PORTUGUÊS

O Direito português não contém qualquer referência expressa à utilização de *benware* na investigação criminal, tal como também não prevê a busca *online*, a vigilância nas fontes e a vigilância acústica e/ou ótica mediante a ativação da câmara e/ou do microfone do sistema informático. Apenas encontramos uma referência implícita ao uso de *benware* no art. 19.º, n.º 2, da Lei n.º 109/2009, relativo às ações encobertas em ambiente informático-digital ou *online*, em que se prevê a possibilidade de utilização de meios e dispositivos informáticos (onde podemos incluir os programas subsumíveis ao conceito de *benware*) no âmbito das ações encobertas *online*[90].

Assim, haverá que analisar a admissibilidade da vigilância nas fontes, as busca *online* e da vigilância acústica e ótica (sob a forma de interceção de comunicações entre presentes e/ou de registo de voz e imagem) com utilização de *benware* para ativação da câmara e/ou do microfone do sistema informático visado.

Começando pela vigilância nas fontes, sendo a nossa lei omissa quanto a essa possibilidade, não existe acordo na Doutrina quanto à sua admissibilidade[91]. Pela nossa parte, consideramos que é admissível, embora devamos repartir a nossa análise em duas vertentes. Quanto à primeira vertente (que se refere à interceção de comunicações *ex se*),

90 Consideramos que esta norma não pode constituir a norma habilitante para o uso de *benware* e, consequentemente, para a realização de buscas *online*, vigilância nas fontes e/ou vigilância acústica e/ou ótica mediante a ativação da câmara e/ou do microfone do sistema informático.

Em primeiro lugar, pela leitura que fazemos da norma, não foi essa a finalidade com que o legislador terá criado essa norma (contra, DAVID SILVA RAMALHO, "O uso de *malware* como meio de obtenção de prova em processo penal", *in* Revista de Concorrência e Regulação, n.º 16, p. 236), que, sem prejuízo de a considerarmos supérflua, apenas tem a finalidade de clarificar a possibilidade de, no âmbito das ações encobertas *online*, serem utilizados meios e dispositivos informáticos, tanto para execução da ação encoberta *ex se* (*v.g.* a ação encoberta ser executada com a utilização de *Cybercops* em vez de pessoas reais) como para a utilização de outros meios de obtenção de prova autónomos (desde logo, as buscas *online*). Por isso, a previsão legal terá de constar de outra norma.

E, em segundo lugar, como refere DAVID SILVA RAMALHO, *Op. Cit.*, pp. 231 e ss., o art. 19.º, n.º 2, da Lei n.º 109/2009 padece da clareza, previsibilidade e precisão exigíveis em sede de restrições de direitos fundamentais quanto aos pressupostos e requisitos da utilização de *benware*, bem como da realização de buscas *online*, vigilância nas fontes e vigilância acústica e/ou ótica mediante a ativação da câmara e/ou do microfone do sistema informático (que, para mais, são meios de obtenção de prova/métodos "ocultos" de investigação criminal fortemente restritivos de direitos fundamentais).

91 Considerando que o art. 18.º da Lei n.º 109/2009 permite a vigilância nas fontes, *vide* PEDRO DIAS VENÂNCIO, Lei do Cibercrime, p. 119, e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 572, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 156; contra, entendendo que, inexistindo previsão legal expressa, a vigilância nas fontes não é admissível, COSTA ANDRADE, "Bruscamente no Verão Passado" p. 165, e DAVID SILVA RAMALHO, Métodos Ocultos de Investigação Criminal em Ambiente Digital, pp. 339 e ss.

não se levantam particulares dúvidas quanto à admissibilidade, contanto que estejam verificados os pressupostos legais previstos no art. 18.º da Lei n.º 109/2009.

Por seu turno, quanto à segunda vertente (que se refere à instalação do *benware*), que é a que suscita as divergências doutrinais quanto à admissibilidade que referimos, não vemos em que medida a falta de previsão legal da possibilidade de instalação sub-reptícia de *benware* no sistema informático visado para permitir a intervenção nas comunicações (antes da encriptação dos dados no sistema "emissor" ou depois da sua desencriptação no sistema "recetor") constitui fundamento para negar a admissibilidade. Por várias razões.

Em primeiro lugar, a vigilância nas fontes configura uma intervenção nas comunicações eletrónicas que, por razões *meramente técnicas*, requer a prévia instalação de *benware*, sendo que a instalação do *benware* restringe direitos fundamentais de uma forma pouco intensa.

Em segundo lugar, a instalação de *benware* configura um mero ato preparatório da intervenção nas comunicações por VoIP, à semelhança do que sucede com a duplicação da linha do número do telefone visado pela escuta telefónica. Ou seja, a instalação de *benware*, para além de constituir uma restrição de direitos fundamentais muito pouco significativa (sobretudo quando comparada com a restrição que resulta da intervenção nas comunicações), é um ato que está incluído, por natureza, na interceção de comunicações eletrónicas quando realizadas por VoIP.

Em terceiro lugar, o art. 18.º da Lei n.º 109/2009 refere-se a "interceções de comunicações" (em sistemas informáticos) sem operar qualquer distinção, exclusão ou ressalva, pelo que, ao permitir a interceção de quaisquer comunicações realizadas por meio de um sistema informático (onde se incluem as comunicações por meio de VoIP), permite também a interceção de comunicações através de VoIP. E, se o legislador, conhecendo a necessidade de instalar previamente *benware* no sistema informático visado, optou por permitir a interceção de quaisquer comunicações realizadas por meio de um sistema informático (sem operar qualquer distinção, exclusão ou ressalva), não faz qualquer sentido afirmar-se que, como a interceção de comunicações através de VoIP requer a prévia instalação de *benware*, o art. 18.º da Lei n.º 109/2009 não permite a interceção de comunicações nessas circunstâncias.

Em quarto lugar, poderia aduzir-se que a vigilância nas fontes, pelo facto de requerer a prévia instalação de *benware*, é similar às buscas *online* e que, não permitindo a lei a realização de buscas *online*, também a vigilância nas fontes não é permitida. Contudo, como veremos, as buscas *online* são admissíveis à luz da lei portuguesa e, para além disso, a

vigilância nas fontes e as buscas *online* são realidades completamente diversas, pois aquela constitui uma intervenção nas comunicações, ao passo que esta consiste no rastreio do sistema informático na sua globalidade.

Em quinto lugar, poderia aduzir-se que, se o legislador alemão sentiu necessidade de regular expressamente a vigilância nas fontes, então, a sua não previsão legal expressa torna-a inadmissível à luz do Direito português. Todavia, sem prejuízo de ser preferível uma previsão legal expressa, consideramos que a nossa lei vigente contém suficientes salvaguardas em termos de restrição de direitos fundamentais; e também não podemos olvidar que as normas relativas aos meios de obtenção de prova não são normas processuais penais materiais (e não devem, por isso, seguir o mesmo regime das normas penais positivas)[92] nem que as exigências de certeza jurídica e de tutela da confiança[93] não são as mesmas quando se trate de impor limitações à licitude de condutas e quando se estabelecem os requisitos da utilização de um dado meio de obtenção de prova[94].

E, por último, nem se diga que, como aduzem COSTA ANDRADE e o *Bundesverfassungsgericht*[95], implicando a execução da vigilância nas fontes a prévia instalação de *malware* (para nós, *benware*), não está garantido o não acesso a outras informações (*v.g.* dados armazenados, navegação na Internet, etc.) para além das comunicações por VoIP. Com efeito, ainda que, em abstrato, tal pudesse suceder, não há que partir de uma suspeição generalizada quanto à atuação das autoridades e, se se concluísse que assim sucedera, as provas seriam ilícitas e as pessoas que assim atuassem seriam alvo de responsabilidade penal, civil e disciplinar.

Em suma, a vigilância nas fontes é admissível à luz do art. 18.º da Lei n.º 109/2009. No entanto, para afastar quaisquer dúvidas a este respeito, o legislador português deveria, tal como fez o legislador alemão, prever expressamente a possibilidade de lançar mão da vigilância nas fontes. E afirmamos que o legislador deverá prever expressamente essa

92 *Vide* os nossos argumentos em DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 298-299.

93 Como refere LARENZ, Metodologia da Ciência do Direito, 3.ª Edição, pp. 603-604, nem toda a confiança merecerá proteção, apenas a merecendo aquela que for justificada pelas circunstâncias e sendo que o princípio da confiança poderá colidir com outros princípios jurídicos a que poderá caber a prevalência no caso concreto.

94 Cfr. Acórdão Malone c. Reino Unido, do Tribunal Europeu dos Direitos Humanos e Sentença do *Tribunal Constitucional de España* n.º 49/1999.

Quanto às razões por que entendemos que as exigências de certeza jurídica e de tutela da confiança não são as mesmas em ambas as situações, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 290-291.

95 COSTA ANDRADE, "Bruscamente no Verão Passado" p. 165, e Sentença do *Bundesverfassungsgericht* de 27/02/2008 (1 BvR 370/07 e 1 BvR 595/07).

possibilidade, atenta a elevada utilização das comunicações por VoIP nos dias de hoje e a existência de aplicações informáticas que proporcionam uma elevadíssima proteção às comunicações realizadas com recurso a essas aplicações (*máxime* o *Telegram*), que torna as comunicações por VoIP um dos meios preferidos dos criminosos para a preparação e execução dos crimes e apagamento dos seus vestígios e, desse modo, a interceção de tais comunicações é absolutamente essencial para a descoberta da verdade material e para a obtenção de provas do cometimento de crimes[96].

Passando às buscas *online*, sendo a nossa lei omissa também quanto a este meio de obtenção de prova, não existe acordo na Doutrina quanto à sua admissibilidade[97] e, entre os defensores da admissibilidade, não existe acordo quanto à norma habilitante[98]. A este respeito, entendemos que a análise deverá partir da diferenciação entre os casos em que a busca consiste num único acesso (*Daten-Spiegelung*) e os casos em que ocorre de forma contínua e prolongada no tempo (*Daten-Monitoring*).

---

96 Como se viu no recente Caso EncroChat. A respeito deste caso, *vide* EUROPOL, "Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe" (Press release).

97 PAULO PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 502 e 545, JOÃO CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, pp. 42 e ss. (embora apenas no âmbito de uma ação encoberta em ambiente informático-digital), e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 809 e ss., e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 226 e ss., pronunciam-se pela admissibilidade, ao passo que DAVID SILVA RAMALHO, "O uso de *Malware* como meio de obtenção de prova em processo penal", *in* Revista de Concorrência e Regulação, n.º 16, p. 227, e também em Métodos Ocultos de Investigação Criminal em Ambiente Digital, pp. 346 e ss., RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, pp. 196 e ss., 248 e 273, BENJAMIM SILVA RODRIGUES, Da Prova Penal, II, pp. 474-475, ARMANDO DIAS RAMOS, A prova digital em processo penal: O correio eletrónico, p. 91, MARIA BEATRIZ SEABRA DE BRITO, Novas Tecnologias e Legalidade da prova em Processo Penal, p. 97, e MARCOLINO DE JESUS, Os Meios de Obtenção de Prova em Processo Penal, p. 196, se pronunciam no sentido oposto.

DAVID SILVA RAMALHO, "O uso de m*alware* como meio de obtenção de prova em processo penal", *in* Revista de Concorrência e Regulação, n.º 16, p. 227, e também em Métodos Ocultos de Investigação Criminal em Ambiente Digital, pp. 346 e ss., entende que o art. 19.º, n.º 2, da Lei n.º 109/2009 não observa as exigências de segurança jurídica, densificação e qualidade da lei restritiva de direitos fundamentais e é incompatível com os ditames do princípio da proporcionalidade quando permite o recurso à busca *online* (e o mesmo sucede quanto à ação encoberta em ambiente informático-digital) para investigar crimes de pequena gravidade e, por isso, é inconstitucional quando aplicado às buscas *online*.

98 Ao passo que PAULO PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 502 e 545, considera que a norma habilitante é o art. 15.º da Lei n.º 109/2009 (sendo uma eventual inconstitucionalidade decorrente de a obtenção de dados íntimos ou privados ocorrer sem intervenção judicial é afastada pelo art. 16.º, n.º 3, da mesma Lei, ao impor uma intervenção judicial, ainda que *a posteriori*, no caso de serem obtidos dados informáticos dessa natureza no decurso da pesquisa informática ou de outro acesso legítimo a um sistema informático), JOÃO CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, pp. 42 e ss., entende que a norma habilitante é o art. 19.º, n.º 2, do Lei n.º 109/2009, que permite a utilização de meios e dispositivos informáticos no decurso de uma ação encoberta *online*. Pela nossa parte, como veremos, concordamos com PAULO PINTO DE ALBUQUERQUE, embora com as especificidades que referiremos no texto e que sempre temos defendido noutras publicações.

Começando pelos casos de *Daten-Spiegelung*, prevê-se, no art. 15.º da Lei n.º 109/2009, a possibilidade de realizar pesquisas de dados informáticos armazenados em sistemas informáticos, não exigindo a lei que a pesquisa apenas possa ser "presencial", "física" (porquanto se refere apenas à obtenção de dados informáticos armazenados num sistema informático e não ao modo concreto da sua obtenção). Por isso, em obediência ao princípio *ubi lex non distinguit nec nos distinguere debemus*, a busca *online* na modalidade de *Daten-Spiegelung* poderá ser realizada com base neste preceito.

Passando aos casos de *Daten-Monitoring*, que, ao permitir uma monitorização, em tempo real e prolongada no tempo, dos dados existentes num sistema informático e da própria navegação *online*, possui uma danosidade muito similar à da intervenção nas comunicações eletrónicas em termos de restrição de direitos fundamentais. Na medida em que o legislador, ao admitir as buscas *online* no art. 15.º da Lei n.º 109/2009, não opera qualquer distinção, consideramos que tal preceito permite, também na modalidade de *Daten-Monitoring*, a realização de buscas *online*. Porém, atenta a sua maior danosidade face à modalidade de *Daten-Spiegelung* e sendo essa danosidade similar à da intervenção nas comunicações eletrónicas, deverá operar-se uma interpretação conforme à Constituição (por imposição da proibição do excesso), pelo que o art. 15.º deverá ser interpretado de forma hábil, de molde a apenas serem admissíveis buscas *online* na modalidade de *Daten-Monitoring* nos casos em que também fosse admissível lançar mão da intervenção nas comunicações eletrónicas nos termos do art. 18.º da Lei n.º 109/2009, aplicando-se *mutatis mutandis* o respetivo regime jurídico.

Contra a admissibilidade das buscas *online* à luz do Direito português são pensáveis, em abstrato, os seguintes argumentos:

a) o facto de a lei exigir a presença da autoridade judiciária durante a pesquisa de dados informáticos (cf.. art. 15.º, n.º 1, da Lei n.º 109/2009);

b) a circunstância de o art. 15.º, n.º 6, da Lei n.º 109/2009 mandar aplicar as regras de execução das buscas previstas no CPP e no Estatuto do Jornalista (entre as quais se conta a entrega, ao visado, de uma cópia do despacho que determinou a busca e a possibilidade de assistir à diligência e fazer-se acompanhar por um terceiro);

c) as formas de efetivar a apreensão dos dados previstas no art. 16.º, n.º 7, als. a) a d), da Lei n.º 109/2009; e

d) a lei não prever expressamente as buscas *online*.

Contudo, quanto à necessidade de presença da autoridade judiciária durante a pesquisa de dados informáticos, além de se tratar de uma regra de cariz meramente procedimental, o

próprio legislador refere que tal dever só existirá "*sempre que* [for] *possível*", pelo que a não presença em nada obsta à admissibilidade da busca *online*[99]; ademais, a presença do magistrado, porque a lei não o especifica (e, como tal, não impõe qualquer distinção entre ambas as situações), tanto poderá ser para dirigir *in loco* a diligência como para o fazer *online*, não impondo a lei que esteja no local onde está o sistema informático visado, pelo que poderá estar no local onde está o sistema informático através do qual se acede[100].

Quanto à circunstância de, no art. 15.º, n.º 6, da Lei n.º 109/2009, o legislador mandar aplicar as regras das buscas "*com as necessárias adaptações*", esse preceito não exige que a busca informática seja "presencial" (pois o conceito de busca deverá ser lido de forma atualista, daí resultando que não tem de ser necessariamente realizada de forma "aberta" e "presencial" nem tem de se limitar à apreensão de coisas corpóreas, podendo e devendo ser dirigidas à descoberta de quaisquer meios de prova e de vestígios do crime – que é a finalidade de qualquer busca –, sejam corpóreos ou não[101]); além disso, as regras relativas às buscas que aqui estão em causa são de cariz procedimental e não material (ou seja, referem-se ao "como" e não ao "se")[102].

No que concerne às formas de efetivar a apreensão dos dados previstas no art. 16.º, n.º 7, als. a) a d), da Lei n.º 109/2009, a lei não impõe que a apreensão dos dados informáticos ocorra no local onde o sistema informático ou o suporte em que estão armazenados se encontram (não se podendo olvidar que a sua efetiva localização pode nem ser conhecida das autoridades[103] ou situar-se num Estado que recusa qualquer cooperação internacional), podendo ser concretizada à distância mediante cópia em suporte

99 Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 809-810, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 228, e, à luz do Direito alemão, Sentença do *Bundesgerichtshof* de 21 de fevereiro de 2006. Relativamente às buscas não domiciliárias e às buscas domiciliárias, como refere DUARTE RODRIGUES NUNES, Revistas e buscas no Código de Processo Penal, pp. 93 e 163, a não observância do art. 174.º, n.º 3, do CPP constitui uma mera irregularidade que não afeta a validade das provas obtidas (cfr. arts. 118.º, n.ºs 1 e 2, e 123.º do CPP).

100 Cfr. JOÃO CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, p. 42 (nota 29), e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 810, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 228-229.

101 Cfr. KEMPER, "Die Beschlagnahmefähigkeit von Daten und E-Mails", *in* Neue Zeitschrift für Strafrecht, 2005, pp. 538-539, HOFMANN, "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, p. 123, e Sentença do *Bundesgerichtshof* de 21 de fevereiro de 2006.

102 Cfr., à luz do Direito alemão, Sentença do *Bundesgerichtshof* de 21 de fevereiro de 2006.

103 A utilização de *proxies* permite simular que o sistema informático se encontra num país diverso e até muito distante do país onde realmente se encontra e, desse modo, dissimular a verdadeira localização. Do mesmo modo, no caso do *Cloud computing*, a localização dos servidores onde os dados estão armazenados pode não ser conhecida.

autónomo[104], sendo que, pelo menos no caso das formas de apreensão previstas nas als. b) e d), do ponto de vista técnico, a apreensão pode perfeitamente ser efetivada *online* e, nos termos do corpo do n.º 7 do art. 16.º, o legislador determina que a escolha da forma de concretizar a apreensão deverá nortear-se por critérios de adequação e de proporcionalidade[105]; ademais, nos casos previstos no art. 15.º, n.º 5 (que, na Alemanha, é designada por "*busca online light*"), a apreensão dos dados só poderá ser efetuada *online*, dúvidas não restando de que, nesses casos – expressamente previstos na lei –, a circunstância de a apreensão dos dados só poder ser efetuada *online*, não impede a realização de pesquisas em sistemas informáticos[106].

E, quanto ao argumento da falta de previsão legal, em primeiro lugar, a lei não distingue entre pesquisas "presenciais" e pesquisas *online*, não exclui expressamente as pesquisas *online* nem restringe as pesquisas em sistemas informáticos apenas aos casos em que sejam "presenciais"; e, além disso, prevê, inclusivamente, um caso de pesquisa remota no art. 15.º, n.º 5 da Lei n.º 109/2009.

Em segundo lugar, em 2009 já era tecnicamente possível a realização de pesquisas remotas em sistemas informáticos (ao ponto de o legislador ter previsto uma modalidade – que não configura uma busca *online* na aceção que aqui estamos a analisar – de pesquisa em sistema informático como a que consta do art. 15.º, n.º 5 da Lei n.º 109/2009), pelo que não se pode considerar – à míngua de elementos que apontem no sentido oposto – que o legislador apenas terá tido em conta as pesquisas "presenciais".

Em terceiro lugar, a busca *online* nem sequer implica a entrada no local onde está o sistema informático (que até poderá ser um espaço que goza da tutela do direito à inviolabilidade do domicílio) nem a apreensão do sistema informático[107], pelo que, nos casos em que a busca *online* consista num único acesso, é menos lesiva do que uma pesquisa "presencial" em termos de restrição de direitos fundamentais[108].

---

104 Cfr. JOÃO CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, p. 42 (nota 29), e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 810, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 229.

105 Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 810, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 229.

106 Assim, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 810-811, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 229.

107 Cfr. HOFMANN, "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, p. 124.

108 No mesmo sentido, SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, p. 9; contra, DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National

Em quarto lugar, o art. 15.º da Lei n.º 109/2009[109] prevê um caso de pesquisa em sistema informático realizado remotamente, pelo que, tendo em conta o que referimos no primeiro argumento, podemos fundar a admissibilidade da busca *online*, pelo menos numa interpretação extensiva[110] desse preceito. Na verdade, radicando a particularidade da busca *online* em não ser realizada no local onde se encontra o sistema informático visado, a busca *online* nem por isso deixa de ser uma pesquisa de dados informáticos específicos e determinados que estão armazenados num determinado sistema informático, pelo que continuamos no âmbito do sentido possível da expressão "*pesquisa de dados informáticos específicos e determinados que estão armazenados num determinado sistema informático*".

Em quinto lugar, nem se diga que, em termos de pesquisa *online*, o legislador ao prever a extensão *online* da pesquisa no art. 15.º, n.º 5, da Lei n.º 109/2009 apenas quis permitir essa extensão e nada mais, porquanto tal extensão também poderá ocorrer no âmbito de uma busca *online*, designadamente quando, no decurso da mesma, se verifique que os dados estão (ou existem mais dados relevantes) armazenados num outro sistema informático que seja legitimamente acessível através do sistema que estava a ser alvo da busca *online*.

Em sexto lugar, a busca *online* é apenas uma forma de efetivação de uma pesquisa num sistema informático, sendo que nada na Constituição ou na lei impõe que as diligências investigatórias sejam realizadas, em regra, com o conhecimento dos visados, razão pela qual, o mero caráter "oculto" não é argumento para obstar à admissibilidade das buscas *online*[111].

Em sétimo lugar, a especificidade da busca *online* que mais dúvidas suscita quanto à sua admissibilidade é a prévia instalação de programas informáticos que permitam o acesso (necessariamente sub-reptício) ao sistema informático. Ora, a instalação de *benware* é um mero ato preparatório da pesquisa informática (na modalidade de busca *online*), à semelhança do que sucede com essa mesma instalação no caso da vigilância nas fontes, com a colocação de localizadores de GPS no caso da obtenção de dados de localização através

---

search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), p. 755, LORENA BACHMAIER WINTER, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *in* Boletín del Ministerio de Justicia, Núm. 2195, pp. 24-25, e Sentença Riley *v.* California do *Supreme Court of the United States* (2014).

109 Cfr. PAULO PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 502 e 545.

110 E não atualista, dado que, em 2009, já era tecnicamente possível efetuar buscas *online*. Porém, na medida em que, não distinguindo a lei entre pesquisa "presencial" e busca *online*, cremos que nem será necessário lançar mão de uma interpretação extensiva.

111 Cfr. HOFMANN, "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, p. 123.

de sistema GPS ou com a duplicação da linha do número do telefone visado pela escuta telefónica.

Em oitavo lugar, ainda que a mera instalação do *benware* restrinja direitos fundamentais, trata-se de uma restrição muito pouco significativa (sobretudo quando comparada com a restrição que pode resultar do acesso aos dados informáticos, tudo dependendo da natureza dos mesmos) e, para além disso, como referimos, nos casos em que a busca *online* consista num único acesso, é menos lesiva do que a restrição decorrente de uma pesquisa "presencial".

Em nono lugar, nem se diga que, como aduzem COSTA ANDRADE e o *Bundesverfassungsgericht*[112], implicando a execução da busca *online* a prévia instalação de *malware* (para nós, *benware*), não está garantido o não acesso a outras informações (*v.g.* ao teor de comunicações através de vigilância nas fontes não autorizada), pois, como referimos supra, não podemos partir de uma suspeição generalizada quanto à atuação das autoridades e, se se concluísse que assim teria acontecido, as provas seriam ilícitas e as pessoas que assim atuassem seriam alvo de responsabilidade penal, civil e disciplinar.

E, em décimo lugar, poderia aduzir-se que, se os legisladores alemão e espanhol sentiram necessidade de regular expressamente as buscas *online*, então, pelo menos no caso das buscas *online* na modalidade de *Daten-Monitoring*, a não previsão legal expressa torna as buscas *online* inadmissíveis à luz do Direito português. Todavia, sem prejuízo de entendermos que será preferível que o legislador luso preveja e regule expressamente este meio de obtenção de prova, consideramos que a nossa lei vigente contém suficientes salvaguardas em termos de restrição de direitos fundamentais (designadamente se se adotar um regime jurídico como o que propugnamos[113]), não se podendo olvidar que as normas relativas aos meios de obtenção de prova não são normas processuais penais materiais (e não devem, por isso, seguir o mesmo regime das normas penais positivas)[114] nem que as exigências de certeza jurídica e de tutela da confiança[115] não são as mesmas quando se trate

112 COSTA ANDRADE, "Bruscamente no Verão Passado" p. 165, e Sentença do *Bundesverfassungsgericht* de 27/02/2008 (1 BvR 370/07 e 1 BvR 595/07).

113 *Vide*, a este respeito, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 809 e ss., e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 231 e ss.

114 *Vide* os nossos argumentos em DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 298-299.

115 Como refere LARENZ, Metodologia da Ciência do Direito, 3.ª Edição, pp. 603-604, nem toda a confiança merecerá proteção, apenas a merecendo a confiança que for justificada pelas circunstâncias e sendo que o princípio da confiança poderá colidir com outros princípios jurídicos a que poderá caber a prevalência no caso concreto.

de impor limitações à licitude de condutas e quando se estabelecem os requisitos da utilização de um dado meio de obtenção de prova[116].

Deste modo, entendemos que a busca *online* é admissível entre nós, à luz do art. 15.º da Lei n.º 109/2009, embora, nos casos de *Daten-Monitoring*, por imposição da proibição do excesso, o art. 15.º deva ser interpretado de forma hábil, de molde a apenas serem admissíveis buscas *online* nos casos em que também fosse admissível lançar mão da intervenção nas comunicações eletrónicas nos termos do art. 18.º da Lei n.º 109/2009, aplicando-se *mutatis mutandis* o respetivo regime jurídico.

No entanto, reiteramos que, para afastar quaisquer dúvidas a este respeito, o legislador português devesse, tal como fizeram os legisladores espanhol e alemão, prever expressamente a possibilidade de lançar mão das buscas *online*.

E entendemos que a solução legal só poderá ser no sentido da admissibilidade do recurso às buscas *online*, pois, em primeiro lugar, a busca *online* é um meio extremamente eficaz e necessário para a investigação criminal «*tendo em conta a presença praticamente ubíqua do computador no quotidiano dos cidadãos em todos os sectores e domínios da vida e, portanto, também do lado da preparação, planificação e gestão de meios e recursos do crime. E tanto mais quanto mais a fenomenologia criminal ganhar em mobilidade, racionalidade e organização. Resumidamente (...) também as manifestações mais insidiosas e perigosas da criminalidade organizada, e concretamente o terrorismo, apresentam hoje uma indissociável associação à informática. E, nessa medida, expõem uma extensa e fecunda superfície à investigação das instâncias de controlo. E é assim, mesmo tendo em conta os obstáculos técnicos ainda subsistentes e o recurso cada vez mais generalizado a programas de proteção e "blindagem" dos dados*»[117].

116 Cfr. Acórdão Malone c. Reino Unido, do Tribunal Europeu dos Direitos Humanos e Sentença do *Tribunal Constitucional de España* n.º 49/1999.

Quanto às razões por que entendemos que as exigências de certeza jurídica e de tutela da confiança não são as mesmas em ambas as situações, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 290-291.

117 COSTA ANDRADE, "Bruscamente no Verão Passado" pp. 166-167; no mesmo sentido, JOÃO CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, p. 44, HOFMANN, "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, p. 121, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 813, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 231-232, e DAVID SILVA RAMALHO, "The use of malware as a mean of obtaining evidence in Portuguese criminal proceedings", *in* Digital Evidence and Electronic Signature Law Review, 11 (2014), p. 55.

Em segundo lugar, a busca *online* permite monitorizar a navegação na Internet[118], que, não constituindo um processo comunicacional, não pode ser objeto de intervenções nas comunicações. Ademais, em face da existência da *Dark Web*, a determinação do sistema onde os dados estão armazenados ou de onde poderão ser acedidos e a obtenção de credenciais de acesso a *websites* não publicamente acessíveis ou a *darknets* poderá depender do recurso a métodos "ocultos" como as ações encobertas ou as buscas *online*[119].

Em terceiro lugar, a busca *online*, além de permitir – por via do *keylogging* – a obtenção de *passwords* e de outros mecanismos afins[120], permite também analisar o sistema informático em funcionamento e, desse modo, superar as dificuldades causadas pela utilização de medidas antiforenses e aceder mais fácil e rapidamente à informação, o que a pesquisa "presencial" não permite[121], bem como tem, face às pesquisas "presenciais", a vantagem de, pelo seu caráter "oculto", não "revelar" aos visados que estão a ser alvo de uma investigação e de recolha de provas, com evidentes ganhos em termos de eficácia[122].

Em quarto lugar, a busca *online* permite aceder a outros suportes informáticos que não estejam na proximidade do sistema informático no momento em que a pesquisa "presencial" é realizada e cuja existência seja desconhecida pelas autoridades ou lhes tenha sido omitida, bem como, nos casos de *Daten-Monitoring*, permite apreender ficheiros informáticos que apenas estão no sistema informático por um breve lapso de tempo antes de serem apagados[123].

118 Cfr. HOLZNER, Die Online-Durchsuchung: Entwicklung eines neuen Grundrechts, p. 11, e BUERMEYER, Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, p. 161.
119 Cfr. DAVID SILVA RAMALHO, "A investigação criminal na Dark Web", *in* Revista de Concorrência e Regulação n.ºs 14/15, p. 402.
120 Cfr. BUERMEYER, Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, p. 161, e DAVID SILVA RAMALHO, "A investigação criminal na Dark Web", *in* Revista de Concorrência e Regulação n.ºs 14/15, p. 402.
121 Cfr. BUERMEYER, Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, pp. 158 e ss., DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), p. 745, e DAVID SILVA RAMALHO, "A investigação criminal na Dark Web", *in* Revista de Concorrência e Regulação n.ºs 14/15, p. 402.
122 Cfr. ROGGAN, "Präventive Online-Durchsuchungen", *in* Online-Durchsuchungen, p. 99, e BUERMEYER, Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, p. 158.
123 Cfr. BUERMEYER, Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, pp. 159 e 161.

Em quinto lugar, a busca *online* permite investigar os ataques de DDoS[124] lançados através do uso de *botnets*[125].

Por fim, a busca *online* poderá ser um meio de suprir as insuficiências da intervenção nas comunicações eletrónicas ao permitir a obtenção de informação cuja consecução não tenha sido possível durante o processo comunicacional e que tenha sido armazenada num sistema informático – incluindo no caso do *Cloud computing*[126] – cuja localização física não tenha sido possível determinar[127] (o que impede, *ab initio*, a solicitação de cooperação judiciária internacional[128]) ou que estejam localizados no Estrangeiro[129] (especialmente quando se trate de países qualificáveis como paraísos fiscais e/ou jurídico-penais, em que as autoridades locais não cooperam com as suas congéneres de outros países em matéria de investigação criminal ou em que essa cooperação é extremamente demorada e com perdas irreparáveis no plano probatório), superando assim as insuficiências da interceção de

---

124 O ataque do tipo *DoS* (*Denial of Service*), também designado por ataque de negação de serviço, consiste na provocação de uma sobrecarga num sistema informático para que os recursos desse sistema fiquem indisponíveis para os seus utilizadores. Para executar um ataque deste tipo, o atacante envia diversos pedidos de pacotes para o alvo para que ele fique tão sobrecarregado que não consiga responder a qualquer outro pedido de pacote, deixando os seus utilizadores de poder aceder aos dados que se encontram nesse sistema; outra forma de execução consiste em o atacante forçar a vítima a reinicializar ou a consumir todos os recursos da memória e de processamento ou de outro *hardware*, para que o sistema informático não possa fornecer o serviço. Este ataque do tipo *DoS* não constitui qualquer invasão do sistema (que apenas é incapacitado por via da sua sobrecarga), envolvendo apenas um atacante, sendo o mesmo sistema informático que faz os vários pedidos de pacotes ao alvo, apenas sendo atingidos servidores fracos e computadores com pouca capacidade técnica.

Por seu turno, o ataque do tipo *DDoS* (*Distributed Denial of Service*) consiste em um sistema informático "mestre" gerenciar um determinado número (podendo ser na ordem dos milhares) de sistemas informáticos (*zumbis*), 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 constantemente, dependendo do recurso que foi atingido pelo ataque).

125 Cfr. DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), p. 745.

A *botnet* consiste numa rede de sistemas informáticos infetados por *bots* semelhantes. Os agentes do crime irão disseminar m*alware* num grande número de sistemas informáticos, com o objetivo de os transformar em *zumbis* (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 atos de Ciberterrorismo), de cometimento de fraudes, etc. A criação de *botnets* constitui também um ato preparatório de ataques do tipo *DDoS*.

126 No Direito alemão, a pesquisa dos dados armazenados numa nuvem é operada ao abrigo do §100b, relativo à busca *online* (cfr. MARCUS KÖHLER, "100b", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 422.

127 Cfr. ORTIZ PRADILLO, "El registro «*online*» de equipos informáticos como medida de investigación contra el terrorismo (*online durchsuchung*)", *in* Terrorismo y Estado de Derecho, p. 469, HOFMANN, "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, p. 121, e BÖCKENFÖRDE, Die Ermittlung im Netz, p. 469.

128 E, no caso do *Cloud computing*, até poderá saber-se em que nuvem os dados informáticos estão armazenados, mas desconhecer-se o país onde os servidores se encontram (o que impossibilita qualquer pedido de auxílio) ou, conhecendo-se o país, tratar-se de um país que não coopera em matéria de investigação criminal ou a cooperação é demasiado lenta e com perdas irreparáveis em termos de prova. Acerca da dificuldade da investigação em casos de *Cloud computing*, *vide* DAVID SILVA RAMALHO, "A recolha de prova penal em sistemas de computação em nuvem", *in* Revista de Direito Intelectual, 2014, n.º 2, *passim*.

129 Cfr. BÖCKENFÖRDE, Die Ermittlung im Netz, p. 221.

comunicações, uma vez que, em regra, os dados armazenados no sistema não são remetidos por correio eletrónico ou, sendo-o, são-no por via de encriptação do *e-mail*[130].

Por fim, quanto à vigilância acústica e ótica, como referimos, a nossa lei prevê dois meios de obtenção de prova distintos[131]: a interceção de comunicações entre presentes (art. 189.º, n.º 1, do CPP) e o registo de voz e imagem (art. 6.º da Lei n.º 5/2002)[132]. Todavia, tal como não previu expressamente a possibilidade de vigilância acústica e ótica no interior do domicílio (e de espaços que gozam da tutela constitucional do direito à inviolabilidade do domicílio)[133], o legislador também não previu a possibilidade de realizar vigilâncias acústicas e/ou óticas através da ativação da câmara e/ou do microfone de um sistema informático (com a prévia instalação do *software* necessário para esse efeito), como fez o legislador italiano relativamente ao *captatore informatico*.

Pela nossa parte, à semelhança do que referimos quanto à vigilância nas fontes e à busca *online*, entendemos que nada impede a realização de vigilâncias acústicas e/ou óticas através da ativação da câmara e/ou do microfone de um sistema informático precedida da instalação de *benware* (*captatore informatico*), pelo que tal possibilidade é admissível à luz do Direito português.

Em primeiro lugar, o *captatore informatico* consiste apenas num meio de execução das interceções de comunicações entre presentes ou do registo de voz e/ou imagem[134],

Em segundo lugar, a instalação do *benware* é um mero ato preparatório da vigilância acústica e/ou ótica que implica uma restrição de direitos fundamentais muito pouco significativa (sobretudo quando comparada com a restrição que resulta da execução da vigilância acústica e/ou ótica) e porventura menos intensa do que a restrição que resultaria

130 Cfr. BUERMEYER, Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, p. 159, e HOFMANN, "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, p. 121.

131 Relativamente à nossa crítica a esta bipartição de meios de obtenção de prova e à preferibilidade de uma unificação de regimes jurídicos, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 682-683.

132 Acerca da diferença entre ambos os meios de obtenção de prova quanto ao seu âmbito de aplicação, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 680 e ss.

133 O que leva alguma Doutrina, a nosso ver sem razão, a pronunciar-se no sentido da inadmissibilidade da interceção de comunicações entre presentes e do registo de voz e imagem "domiciliários". Acerca das razões porque entendemos que interceção de comunicações entre presentes e do registo de voz e imagem no interior do domicílio e/ou de outros espaços que gozam da tutela constitucional do direito à inviolabilidade do domicílio é admissível à luz do Direito português, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 692 e ss.

134 Cfr., à luz do Direito italiano, Sentenças das *Sezioni Unite* da *Suprema Corte de Cassazione* de 28/04/2016-01/07/2016, n.º 26889, e da *Suprema Corte di Cassazione* de 30/05/2017-20/10/2017, n.º 48370 (Sez. V), 08/03/2018-09/10/2018, n.º 45486 (Sez. VI), e 25/06/2019-17/12/2019, n.º 50972 (Sez. I).

da entrada dos agentes no local onde a vigilância deverá ocorrer (sobretudo se se tratar do domicílio) para colocarem os microfones e/ou as câmaras (que também constitui um mero ato preparatório da vigilância acústica e/ou ótica executadas desse modo).

Em terceiro lugar, os arts. 189.º, n.º 1, do CPP e 6.º da Lei n.º 5/2002 referem-se à "interceção de comunicações entre presentes" e ao "registo de voz e imagem, por qualquer meio, sem consentimento do visado", respetivamente. Ora, no caso do art. 189.º, n.º 1, do CPP, o legislador não consagra qualquer limitação ou restrição quanto ao modo de execução da interceção (pelo que *ubi lex non distinguit nec nos distinguere debemus*) e, no art. 6.º da Lei n.º 5/2002, vai ainda mais longe ao permitir expressamente o registo de voz e imagem *por qualquer meio* (onde se pode incluir o *captatore informatico*).

Em quarto lugar, o recurso ao *captatore informatico* dispensa a entrada "física" das autoridades nos locais reservados e não acessíveis ao público (incluindo o domicílio) em que fosse necessário instalar as câmaras e os microfones (sendo, por isso, como referimos, menos lesivo para os direitos fundamentais e envolvendo menos riscos para os agentes policiais).

Em quinto lugar, poderia aduzir-se que, se o legislador italiano sentiu necessidade de regular expressamente o *captatore informatico*, então, a sua não previsão legal expressa torna-o inadmissível à luz do Direito português[135]. Todavia, sem prejuízo de ser preferível uma previsão legal expressa, consideramos que a nossa lei vigente contém suficientes salvaguardas em termos de restrição de direitos fundamentais; e também não podemos olvidar que as normas relativas aos meios de obtenção de prova não são normas processuais penais materiais (e não devem, por isso, seguir o mesmo regime das normas penais positivas)[136] nem que as exigências de certeza jurídica e de tutela da confiança[137] não são as mesmas quando se trate de impor limitações à licitude de condutas e quando se estabelecem os requisitos da utilização de um dado meio de obtenção de prova[138].

---

135 Como entende MARCUS KÖHLER, "100b", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 421, precisamente por essa razão. à luz do Direito alemão.

136 *Vide* os nossos argumentos em DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 298-299.

137 Como refere LARENZ, Metodologia da Ciência do Direito, 3.ª Edição, pp. 603-604, nem toda a confiança merecerá proteção, apenas a merecendo aquela que seja justificada pelas circunstâncias; ademais, o princípio da confiança pode colidir com outros princípios que devam prevalecer no caso concreto.

138 Cfr. Acórdão Malone c. Reino Unido, do Tribunal Europeu dos Direitos Humanos e Sentença do *Tribunal Constitucional de España* n.º 49/1999.

Quanto às razões por que entendemos que as exigências de certeza jurídica e de tutela da confiança não são as mesmas em ambas as situações, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 290-291.

E, por último, poderia também aduzir-se – como se aduz quanto à vigilância nas fontes e à busca *online* – que, implicando a utilização do *captatore informatico* a prévia instalação de *malware* (para nós, *benware*), não está garantido o não acesso a outras informações (*v.g.* dados armazenados, navegação na Internet, comunicações eletrónicas, etc.). Contudo, como referimos supra, não podemos partir de uma suspeição generalizada quanto à atuação das autoridades e, se se concluísse que assim sucedera, as provas seriam ilícitas e as pessoas que assim atuassem seriam alvo de responsabilidade penal, civil e disciplinar.

Assim, consideramos que a vigilância acústica e/ou ótica através da ativação da câmara e/ou do microfone de um sistema informático precedidas da instalação de *benware* (*captatore informatico*) é admissível à luz do Direito português, mais concretamente nos termos dos arts. 189.º, n.º 1, do CPP e 6.º da Lei n.º 5/2002.

Contudo, o legislador português deveria seguir o exemplo do legislador italiano e prever expressamente a possibilidade de utilização do *captatore informatico*, a fim de dissipar quaisquer dúvidas que possam surgir a esse respeito. E, tal como entendemos nos casos da vigilância nas fontes e da busca *online*, no que tange à utilização do *captatore informatico*, a solução legal só poderá ser no sentido da sua admissibilidade.

Com efeito, sobretudo no caso de criminosos particularmente cautelosos (como sucede no âmbito da criminalidade organizada, terrorismo, criminalidade económico-financeira e Cibercrime), a realização de vigilância acústica e ótica em locais onde os criminosos se sentem especialmente seguros (*máxime* no seu domicílio) e que poderão utilizar para preparar ou executar crimes ou eliminar os vestígios da prática de crimes ou partilhar detalhes a esse respeito com pessoas da sua confiança (*máxime* familiares próximos, que também poderão fazer parte da organização) poderá ser essencial[139].

Ademais, em grupos criminosos "etnicamente fechados" ou assentes exclusivamente em laços familiares, as ações encobertas tendem a ser inúteis ou impossíveis de realizar[140] e, sabendo esses criminosos que as comunicações eletrónicas poderão ser acedidas pelas autoridades[141], tenderão a confiar mais na segurança que lhes é dada pelo domicílio do que

---

139 Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 696.

140 Aludindo à utilidade da vigilância acústica no interior do domicílio como mecanismo para suprir as insuficiências das ações encobertas, *vide* KREY/HAUBRICH, "Zeugenschutz, Rasterfahndung, Lauschangriff, Verdeckte Ermittler", *in* Juristische Rundschau, 1992, p. 313.

141 E, como se afirma na Sentença do *Bundesverfassungsgericht* de 03/03/2004 (1 BvR 2378/98 e 1 BvR 1084/99) , o recurso à intervenção nas comunicações eletrónicas, *maxime* as escutas telefónicas, apresenta uma outra desvantagem face à vigilância acústica: apenas permite intercetar as comunicações que são levadas a cabo mediante meios de comunicação à distância.

na que lhes é oferecida por uma linha telefónica ou pelo Ciberespaço e, por isso, as probabilidades de serem "surpreendidos" no interior do seu domicílio são muito maiores do que enquanto realizam comunicações eletrónicas, proporcionando informações que as autoridades dificilmente obteriam de outra forma[142].

E a vigilância acústica e ótica no interior do domicílio são métodos "ocultos" que permitem atingir eficazmente as cúpulas das organizações criminosas, revelando a sua estrutura organizatória e permitindo identificar os líderes, os apoiantes, os financiadores e os colaboradores externos[143], sendo a sua identificação e prisão essencial para desmantelar a organização e impedir a continuação da sua atividade.

E também não podemos olvidar que a vigilância acústica e ótica apresentam diversas e importantes vantagens face à vigilância "física": (1) permitem a recolha de som e imagem sem necessidade de os investigadores estarem nesse local, (2) não levantam suspeitas de estarem a ser recolhidas provas da atividade criminosa, (3) não põem os investigadores em perigo e (4) proporcionam a obtenção de informações em locais onde não seria possível colocar agentes policiais sem levantar suspeitas[144]. E a vigilância ótica permite captar aspetos que poderão não ser captados pela vigilância acústica, por não conterem qualquer elemento sonoro (*v.g.* a mera entrega de dinheiro ao funcionário corrompido) ou ser usada linguagem codificada indecifrável na comunicação[145].

E especificamente quanto à utilização do *captatore informatico* no âmbito da vigilância acústica e ótica, pela natureza "itinerante" dos sistemas informáticos da atualidade (*smartphone*, *tablet*, computador), os sistemas informáticos podem ser utilizados, pelas autoridades como instrumentos de execução dessas vigilâncias[146], o que dispensa, tanto a entrada dos agentes da autoridade no local onde será realizada a vigilância acústica e/ou ótica para colocarem microfones ou câmaras como a sua permanência nas imediações

142 Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 696-697 (com referências bibliográficas e jurisprudenciais adicionais).

143 Assim, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 697, e Sentença do *Bundesverfassungsgericht* de 03/03/2004 (1 BvR 2378/98 e 1 BvR 1084/99).

144 Cfr. MONTOYA, Informantes y Técnicas de Investigación Encubiertas, Análisis Constitucional y Procesal Penal, 2.ª Edição, p. 343, LEPSIUS, "Die Grenzen der präventivpolizeilichen Telefonüberwachung", *in* Juristische Ausbildung, 2005, p. 433, e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 699.

145 Cfr. GARY MARX, Undercover, p. 58, e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 700.

146 Cfr. Sentenças das *Sezioni Unite* da *Suprema Corte de Cassazione* de 28/04/2016-01/07/2016, n.º 26889, e da *Suprema Corte di Cassazione* de 30/05/2017-20/10/2017, n.º 48370 (Sez. V), 08/03/2018-09/10/2018, n.º 45486 (Sez. VI), e 25/06/2019-17/12/2019, n.º 50972 (Sez. I).

desse local com os dispositivos necessários para a execução da vigilância a partir do exterior, com evidentes ganhos em termos de eficácia da medida e até de segurança dos próprios agentes.

Deste modo, consideramos que a utilização de *benware* no âmbito da investigação criminal é admissível à luz do Direito português vigente, embora – porque, como referimos, restringe o direito fundamental à confidencialidade e à integridade dos sistemas técnico-informacionais – fosse preferível que o legislador o previsse expressamente, a fim de afastar quaisquer dúvidas quanto a essa admissibilidade, que poderão gerar graves prejuízos em termos de eficácia da investigação e, consequentemente, graves deficiências ao nível da proteção dos direitos fundamentais dos cidadãos face a formas de criminalidade particularmente nocivas e que também atentam contra a própria subsistência do Estado de Direito (*máxime* no caso das Máfias, do terrorismo e da corrupção).

4. CONCLUSÕES

A) A crescente utilização das medidas antiforenses e de meios de comunicação como as comunicações por VoIP pelos criminosos dificulta de sobremaneira a deteção da prática de crimes, a descoberta da verdade material e a obtenção de provas.

B) Por isso, as autoridades necessitam cada vez mais de utilizar mecanismos/dispositivos que neutralizem as dificuldades decorrentes da utilização de medidas antiforenses e de meios de comunicação como as comunicações por VoIP pelos criminosos.

C) Um desses mecanismos/dispositivos é a instalação sub-reptícia de programas informáticos (vírus, *worms*, "cavalos de Troia", *keyloggers*, *backdoors*, *spyware*, etc.) que permitam que as autoridades se infiltrem num sistema informático alheio para obterem informações relevantes para a investigação (*benware*).

D) Pela necessária "clandestinidade" da instalação do *benware* nos sistemas informáticos visados – que faz antever o cariz "oculto" das medidas investigatórias cuja execução a sua instalação visa permitir –, a utilização do *benware* está intimamente ligada à questão dos métodos "ocultos" de investigação criminal.

E) A utilização de *benware* é essencial na busca *online* (*online-Durchsuchung*), na vigilância nas fontes (*Quellen-Telekommunikationsüberwachung* ou *Quellen-TKü*) e na vigilância acústica e/ou ótica (sob a forma de registo de voz e imagem ou de interceção de comunicações entre presentes) quando seja realizada mediante a ativação (sub-reptícia) da câmara e/ou do microfone do sistema informático (*captatore informatico*).

F) A utilização de *benware* restringe o direito fundamental à confidencialidade e à integridade dos sistemas técnico-informacionais.

G) Ao contrário de outras ordens jurídicas, o legislador português não regula expressamente a utilização de *benware*, o mesmo sucedendo com as buscas *online*, a vigilância nas fontes e a ativação sub-reptícia da câmara e/ou do microfone do sistema informático no âmbito do registo de voz e imagem ou da interceção de comunicações entre presentes, apenas existindo uma referência implícita ao uso de *benware* no art. 19.º, n.º 2, da Lei n.º 109/2009, em que se prevê a possibilidade de utilizar meios e dispositivos informáticos no âmbito das ações encobertas em ambiente informático-digital ou *online*.

H) Apesar disso, a vigilância nas fontes é admissível à luz do art. 18.º da Lei n.º 109/2009.

I) A busca *online* é admissível à luz do art. 15.º da Lei n.º 109/2009, embora, nos casos em que a infiltração no sistema informático seja levada a cabo de forma contínua e prolongada no tempo (*Daten-Monitoring*), o art. 15.º deva ser interpretado de forma hábil, de molde a apenas serem admissíveis buscas *online* nos casos em que também fosse admissível lançar mão da intervenção nas comunicações eletrónicas nos termos do art. 18.º da Lei n.º 109/2009, aplicando-se *mutatis mutandis* o respetivo regime jurídico.

J) A vigilância acústica [sob a forma de a interceção de comunicações entre presentes (art. 189.º, n.º 1, do CPP) ou de registo de voz (art. 6.º da Lei n.º 5/2002)] e a vigilância ótica (registo de imagem, nos termos do art. 6.º da Lei n.º 5/2002) mediante a ativação sub-reptícia da câmara e/ou do microfone do sistema informático são admissíveis à luz dos mencionados normativos.

K) A utilização de *benware* no âmbito da investigação criminal é admissível à luz do Direito português vigente, embora fosse preferível que o legislador previsse essa possibilidade, a fim de afastar quaisquer dúvidas a este respeito.

BIBLIOGRAFIA

Adams, Devin M. – "The 2016 Amendment to Criminal Rule 41: National seach warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 727 e ss., *in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3335987* (consultado em 14/07/2020).

Albuquerque, Paulo Pinto de – Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Universidade Católica Editora, 4.ª Edição, Lisboa, 2011.

Andrade, Manuel da Costa – "Bruscamente no Verão Passado", a reforma do Código de Processo Penal, Observações críticas sobre uma Lei que podia e devia ter sido diferente, Coimbra Editora, Coimbra, 2009.

Andrade, Manuel da Costa – "Art. 194º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo I, 2.ª Edição, pp. 1080 e ss., Coimbra Editora, Coimbra, 2012.

Bachmaier Winter, Lorena – "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *in* Boletín del Ministerio de Justicia, Núm. 2195, *in https://www.mjusticia.gob.es/cs/Satellite/Portal/1292428206148*

?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheade

rname2=EstudioDoctrinal&blobheadervalue1=attachment%3B+filename%3D1701_Estudio.pdf&blobheadervalue2=1288794492107 (consultado em 13/07/2020).

Bär, Wolfgang – TK-Überwachung, §§100a-101 StPO mit Nebengesetzen Kommentar, Carl Heymanns Verlag, Colónia e Munique, 2010.

Baxter, Teri Dobbins – "Great (and Reasonable) Expectations: Fourth Amendment Protection for Attorney-Client Communications", *in* Seattle University Law Review 35, pp. 35 e ss., *in https://ssrn.com/abstract=1336980* (consultado em 14/07/2020).

Brenner, Susan – Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, *in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1950703* (consultado em 14/07/2020).

Brenner Susan – "Law, Dissonance and Remote Computer Searches", *in* North Carolina Journal of Law & Technology, Volume 14, Issue 1, pp. 43 e ss., *in https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1238&context=ncjolt* (consultado em 14/07/2020).

Brito, **Maria Beatriz Seabra de** – Novas Tecnologias e Legalidade da prova em Processo Penal, Almedina, Coimbra, 2018.

Böckenförde, Thomas – Die Ermittlung im Netz, Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit, Mohr Siebeck, Tübingen, 2003.

Buermeyer, Ulf – Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, *in http://www.hrr-strafrecht.de/hrr/archiv/07-04/index.php?sz=8*, pp. 154 e ss. (consultado em 21/02/2011).

Buermeyer, Ulf/Bäcker, Matthias – Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO, *in http://www.hrr-strafrecht.de/hrr/archiv/09-10/index.php?sz=8*, pp. 329 e ss. (consultado em 11/11/2014).

Clancy, Thomas K. – "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, pp. 193 e ss., *in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1602052* (consultado em 14/07/2020).

Correia, João Conde – "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, pp. 29 e ss., Lisboa, 2014.

Díaz, Shelly Mott, "A Guilty Attorney with Innocent Clients: Invocation of the Fourth Amendment to Challenge the Search of Privileged Information", *in* Mississippi Law Journal, Volume 79, pp. 56 e ss., *in https://studylib.net/doc/8201263/invocation-of-the-fourth-amendment-to-challenge-the-* (consultado em 14/07/2020).

Europol – "Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe" (Press release), *in https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe* (consultado em 20/07/2020).

Hofmann, Manfred – "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, pp. 121 e ss., C. H. Beck'sche Verlagsbuchhandlung, Munique e Frankfurt, 2005.

Hoffmann-Riem, Wolfgang – Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigener informationstechnischer Systeme, *in www.jura.uni-hamburg.de/public/personen/hoffmann-riem/8.pdf* (consultado em 21/11/2014).

Holzner, Stefan – Die Online-Durchsuchung: Entwicklung eines neuen Grundrechts, Centaurus Verlag, Kenzingen, 2009.

Jesus, Francisco Marcolino de – Os Meios de Obtenção de Prova em Processo Penal, Almedina, Coimbra, 2011.

Kemper, Martin – "Die Beschlagnahmefähigkeit von Daten und E-Mails", *in* Neue Zeitschrift für Strafrecht, 2005, pp. 538 e ss., C. H. Beck'sche Verlagsbuchhandlung, Munique e Frankfurt, 2005.

Klesczewski, Diethelm – "Straftataufklärung im Internet – Technische Möglichkeiten und rechtliche Grenzen von Strafprozessualen Ermittlungseingriffen im Internet", *in* Zeitschrift für die gesamte Strafrechtswissenschaft, 2012, pp. 737 e ss., Walter de Gruyter, Berlim, 2012.

Köhler, Marcus – "§ 100a", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, pp. 403 e ss., C.H. Beck, Munique, 2019.

Köhler, Marcus – "§ 100b", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, pp. 420 e ss., C.H. Beck, Munique, 2019.

Krey, Volker/Haubrich, Edgar – "Zeugenschutz, Rasterfahndung, Lauschangriff, Verdeckte Ermittler", *in* Juristische Rundschau, 1992, pp. 309 e ss., Walter de Gruyter, Berlim e Nova Iorque, 1992.

Larenz, Karl – Metodologia da Ciência do Direito, 3.ª Edição (tradução de José Lamego), Fundação Calouste Gulbenkian, Lisboa, 1997.

Lepsius, Oliver – "Die Grenzen der präventivpolizeilichen Telefonüberwachung", *in* Juristische Ausbildung, 2005, pp. 929 e ss., Walter de Gruyter, Berlim, 2005.

Marx, Gary T. – Undercover, Police Surveillance in America, University of California Press, Berkeley e Los Angeles, 1988.

Mayer, Jonathan – Constitutional Malware, *in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2633247* (consultado em 16/07/2020).

McArthur, Eric D. – "The Search and Seizure of Privileged Attorney-Client Communications", *in* University of Chicago Law Review, Vol. 72, *in https://chicagounbound.uchicago.edu/uclrev/vol72/iss2/7* (consultado em 14/07/2020).

Montoya, Mario Daniel – Informantes y Técnicas de Investigación Encubiertas, Análisis Constitucional y Procesal Penal, 2.ª Edição, Ad hoc, Buenos Aires, 2001.

Nack, Armin – "§100a", *in* Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK, 6.ª Edição, pp. 471 e ss., Verlag C. H. Beck, Munique, 2008.

Neves, Rita Castanheira – As Ingerências nas Comunicações Electrónicas em Processo Penal, Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova, Coimbra Editora, Coimbra, 2011.

Nunes, Duarte Rodrigues – Os meios de obtenção de prova previstos na Lei do Cibercrime, Gestlegal, Coimbra, 2018.

Nunes, Duarte Rodrigues – Revistas e buscas no Código de Processo Penal, Gestlegal, Coimbra, 2019.

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

Ortiz Pradillo, Juan Carlos – "El registro «*online*» de equipos informáticos como medida de investigación contra el terrorismo (*online-Durchsuchung*)", *in* Terrorismo y Estado de Derecho, pp. 457 e ss., Iustel, Madrid, 2010.

Ramalho, David Silva – "A investigação criminal na *Dark Web*", *in* Revista de Concorrência e Regulação, Ano IV, n.ºs 14-15, pp. 383 e ss., Almedina, Coimbra, 2013.

Ramalho, David Silva – "O uso de *malware* como meio de obtenção de prova em processo penal", *in* Revista de Concorrência e Regulação, Ano IV, n.º 16, pp. 195 e ss., Almedina, Coimbra, 2013.

Ramalho, David Silva – "The use of malware as a mean of obtaining evidence in Portuguese criminal proceedings", *in* Digital Evidence and Electronic Signature Law Review, 11 (2014), pp. 55 e ss., *in https://journals.sas.ac.uk/deeslr/article/view/2125* (consultado em 10/07/2020).

Ramalho, David Silva – Métodos Ocultos de Investigação Criminal em Ambiente Digital, Almedina, Coimbra, 2017.

Ramos, Armando Dias – "Do *periculum in mora* da atuação da Autoridade Judiciária ao *fumus boni iuris* da intervenção policial", *in* IV Congresso de Processo Penal, pp. 49 e ss., Almedina, Coimbra, 2016.

Rodrigues, Benjamim Silva – Da Prova Penal, Tomo II, Bruscamente…A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal, 1.ª Edição, Rei dos Livros, Lisboa, 2010.

Roggan, Fredrik – "Präventive Online-Durchsuchungen", *in* Online-Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, pp. 97 e ss, Berliner Wissenschafts-Verlag, Berlim, 2008.

Roxin, Claus/Schünemann, Bernd – Strafverfahrensrecht, 27.ª Edição, C.H.Beck, Munique, 2012.

Singelnstein, Tobias – "Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmassnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung&Co", *in* Neue Zeitschrift für Strafrecht, 2012, pp. 593 e ss., C. H. Beck'sche Verlagsbuchhandlung, Munique e Frankfurt, 2012.

Tonini, Paolo – Manuale di Procedura Penale, 12.ª Edição, Giuffrè Editore, Milão, 2011.

Venâncio, Pedro Dias – Lei do Cibercrime, Anotada e Comentada, Coimbra Editora, Coimbra, 2011.

JURISPRUDÊNCIA

Tribunal Europeu dos Direitos Humanos

Acórdão Malone c. Reino Unido (de 2 de agosto de 1984), *in https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57533%22]}* (consultado em 09/07/2020).

Alemanha

Bundesverfassungsgericht

Sentença de 15 de dezembro de 1983 (1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83 e BvR 484/83), *in https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html* (consultada em 09/07/2020).

Sentença do *Bundesverfassungsgericht* de 3 de março de 2004 (1 BvR 2378/98 e 1 BvR 1084/99), *in https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2004/03/rs20040303_1bvr237898.html* (consultada em 09/07/2020).

Sentença de 27 de fevereiro de 2008 (1 BvR 370/07 e 1 BvR 595/07), *in https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html* (consultada em 09/07/2020).

Sentença de 20 de abril de 2016 (1 BvR 966/09 e 1 BvR 1140/09), *in https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html* (consultada em 09/07/2020).

Sentença de 6 de julho de 2016 (2 BvR 1454/13), *in https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/07/rk20160706_2bvr145413.html* (consultada em 09/07/2020).

Bundesgerichtshof

Sentença de 21 de fevereiro de 2006 [3 BGs 31/06, 3 BJs 32/05 - 4 - (12) - 3 BGs 31/06)], *in www.hrr-strafrecht.de/hrr/3/06/3-bgs-31-06.php* (consultada em 09/07/2020).

Sentença de 31 de janeiro de 2007 (StB 18/06), *in www.hrr-strafrecht.de/hrr/3/06/stb-18-06.php* (consultada em 09/07/2020).

Espanha

Tribunal Constitucional de España

Sentença n.º 49/1999, *in https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/3791* (consultada em 09/07/2020).

Estados Unidos

Supreme Court of the United States

Sentença Olmstead v. United States, 277 U.S. 438 (1928), *in* https://supreme.justia.com/cases/federal/us/277/438/ (consultado em 15/07/2020).

Sentença Goldman v. United States, 316 U.S. 129 (1942), *in* https://supreme.justia.com/cases/federal/us/316/129/ (consultado em 15/07/2020).

Sentença Silverman v. United States, 365 U.S. 505 (1961), *in* https://supreme.justia.com/cases/federal/us/365/505/ (consultado em 15/07/2020).

Sentença Berger v. New York, 388 U.S. 41 (1967), *in https://supreme.justia.com/cases/federal/us/388/41/* (consultado em 15/07/2020).

Sentença Katz v. United States, 389 U.S. 347 (1967), *in https://supreme.justia.com/cases/federal/us/389/347/* (consultado em 14/07/2020).

Sentença Chimel v. California, 395 U.S. 752 (1969), *in https://supreme.justia.com/cases/federal/us/395/752/* (consultado em 14/07/2020).

Sentença Coolidge v. New Hampshire, 403 U.S. 443 (1971), *in https://supreme.justia.com/cases/federal/us/403/443/* (consultado em 14/07/2020).

Sentença Couch v. United States, 409 U.S. 322 (1973), *in https://supreme.justia.com/cases/federal/us/409/322/* (consultado em 14/07/2020).

Sentença United States v. Miller, 425 U.S. 435 (1976), *in https://supreme.justia.com/cases/federal/us/425/435/* (consultado em 14/07/2020).

Sentença Andresen *v.* Maryland, 427 U.S. 463 (1976), *in https://supreme.justia.com/cases/federal/us/427/463/* (consultado em 14/07/2020).

Sentença Zurcher v. Stanford Daily, 436 U.S. 547 (1978), *in https://supreme.justia.com/cases/federal/us/436/547/* (consultado em 14/07/2020).

Sentença Rakas v. Illinois, 439 U.S. 128 (1978), *in https://supreme.justia.com/cases/federal/us/439/128/* (consultado em 14/07/2020).

Sentença Smith v. Maryland, 442 U.S. 735 (1979), *in https://supreme.justia.com/cases/federal/us/442/735/* (consultado em 14/07/2020).

Sentença Walter v. United States, 447 U.S. 649 (1980), *in https://supreme.justia.com/cases/federal/us/447/649/* (consultado em 14/07/2020).

Sentença United States v. Jacobsen, 466 U.S. 109 (1984), *in https://supreme.justia.com/cases/federal/us/466/109/* (consultado em 14/07/2020).

Sentença Riley v. California, 134 S. Ct. 2472 (2014), *in https://www.law.cornell.edu/supremecourt/text/13-132* (consultado em 16/07/2020).

United States Court of Appeals

Sentença National City Trading Corp. v. United States, 635 F.2d 1020 (2nd Circuit 1980), *in https://casetext.com/case/national-city-trading-corp-v-united-states-2* (consultado em 14/07/2020).

Sentença De Massa v. Nunez, 770 F.2d 1505 (9th Circuit, 1984), *in https://casetext.com/case/demassa-v-nunez* (consultado em 14/07/2020).

Sentença Klitzman, Klitzman and Gallagher v. Krut, 744 F.2d 955 (3rd Circuit, 1984), *in https://law.justia.com/cases/federal/district-courts/FSupp/591/258/2388284/* (consultado em 14/07/2020).

Sentença United States *v.* Biasucci, 786 F.2d 504 (2nd Circuit, 1986), *in https://casetext.com/case/united-states-v-biasucci* (consultado em 14/07/2020).

Sentença United States *v.* Cuevas-Sanchez, 821 F.2d 248 (5th Circuit, 1987), *in https://casetext.com/case/us-v-cuevas-sanchez* (consultado em 14/07/2020).

Sentença United States v. Lin Lyn Trading, Ltd., 149 F.3d 1112 (10th Circuit, 1998), *in https://casetext.com/case/us-v-lin-lyn-trading-ltd-3* (consultado em 14/07/2020).

Sentença United States *v.* Hall, 165 F.3d 1095 (7th Circuit, 1998), *in https://casetext.com/case/us-v-hall-253* (consultado em 14/07/2020).

Sentença United States v. Carey, 172 F. 3d 1268 (10th Circuit, 1999), *in https://caselaw.findlaw.com/us-10th-circuit/1317424.html* (consultado em 15/07/2020).

Sentença Leventhal v. Knapek, 266 F3d 64 (2nd Circuit, 2001), *in https://caselaw.findlaw.com/us-2nd-circuit/1332549.html* (consultado em 15/07/2020).

Sentença Ferguson v. Charleston, 532 U.S. 67 (4th Circuit, 2001), *in https://supreme.justia.com/cases/federal/us/532/67/* (consultado em 14/07/2020).

Sentença Guest v. Leis, 255 F.3d 325 (6th Circuit, 2001), *in https://caselaw.findlaw.com/us-6th-circuit/1016277.html* (consultado em 14/07/2020).

Sentença United States *v.* Lifshitz, 369 F.3d 173 (2nd Circuit, 2004), *in https://openjurist.org/369/f3d/173/united-states-v-lifshitz* (consultado em 14/07/2020).

Sentença United States v. Heckenkamp, 482 F.3d 1142 (9th Circuit, 2007), *in https://www.casemine.com/judgement/us/5914b43eadd7b0493476b3d9* (consultado em 15/07/2020).

Sentença United States v. Forrester, 512 F.3d 500 (9th Circuit, 2007), *in https://caselaw.findlaw.com/us-9th-circuit/1452307.html* (consultado em 14/07/2020).

Sentença United States v. Ganoe, 538 F.3d 1117 (9th Circuit, 2008), *in https://caselaw.findlaw.com/us-9th-circuit/1169300.html* (consultado em 16/07/2020).

Sentença United States *v.* Perrine, 518 F.3d 1196 (10th Circuit, 2008), *in https://caselaw.findlaw.com/us-10th-circuit/1308994.html* (consultado em 14/07/2020).

United States District Court for the District of Connecticut

Sentença United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001) (2001), *in https://law.justia.com/cases/federal/district-courts/FSupp2/175/367/2419190/* (consultado em 15/07/2020).

United States District Court for the Southern District of New York

Sentença United States v. Wey, 52 F. Supp. 3d 237 (S.D.N.Y. 2017) (2017), *in https://casetext.com/case/united-states-v-wey-3* (consultado em 15/07/2020).

United States District Court for the North District of Ohio, Western Division

Sentença United States *v.* Skeddle, 989 F. Supp. 890 (N.D. Ohio 1997), *in https://law.justia.com/cases/federal/district-courts/FSupp/989/890/1528661/* (consultado em 14/07/2020).

United States District Court for the Southern District of Texas

Sentença In re Warrant to Search Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (2013), *in https://casetext.com/case/in-re-search* (consultado em 14/07/2020).

United States District Court for the District of Vermont

Sentença United States v. Hunter, 13 F. Supp. 2d 574 (1998), *in https://law.justia.com/cases/federal/district-courts/FSupp2/13/574/2311683/* (consultado em 14/07/2020).

United States District Court for the Western District of Washington

Sentença United States v. Gorshkov, 2001 WL 1024026, U.S. Dist. LEXIS 26306 (2001), *in https://itlaw.wikia.org/wiki/U.S._v._Gorshkov* (consultado em 15/07/2020).

Supreme Court of Minnesota

Sentença O' Connor v. Johnson, 287 N.W.2d 400 (Minn. 1979), *in https://www.casemine.com/judgement/us/5914930cadd7b049345a31c4* (consultado em 14/07/2020).

Massachussets Superior Court

Sentença Commonwealth *v.* Cormier, No. 09-1365, 2011, WL 3450643 (2011)¸ *in https://www.casemine.com/judgement/us/59146083add7b0493422ed7e* (consultado em 14/07/2020).

Court of Appeals of Wisconsin

Sentença State *v.* Schroeder, 2000 WI App 128, 613 N.W.2d 911, 237 Wis. 2d 575 (2000), *in https://www.courtlistener.com/opinion/2221561/state-v-schroeder/* (consultado em 15/07/2020).

Itália

Suprema Corte di Cassazione

Jurisprudência fixada

Sentença das *Sezioni Unite* de 28 de abril de 2016 – 1 de julho de 2016, n.º 26889, *in www.archiviopenale.it/intercettazioni--cass-sez-un-1-luglio-2016-(cc-28-aprile-2016)-scurato/contenuti/6142* (consultada em 07/07/2016).

Outra Jurisprudência

Sentença de 30 de maio de 2017-20 de outubro de 2017 (*Sezione* V, n.º 48370), *in www.archiviopenale.it/intercettazioni--cass-sez-v-20-ottobre-2017-(cc-30-maggio-2017)-occhionero-ed-altri/contenuti/6703* (consultada em 07/07/2016).

Sentença de 8 de março de 2018 – 9 de outubro de 2018 (*Sezione* VI, n.º 45486), *in www.archiviopenale.it* (consultada em 07/07/2016).

Sentença de 25 de junho de 2019 – 17 de dezembro de 2019 (*Sezione* I, n.º 50972), *in www.salvisjuribus.it* (consultada em 07/07/2016).

CYBERLAW
by CIJIC

STATE SURVEILLANCE: HOW IS FACE-RECOGNITION TECHNOLOGY IMPACTING THE POLITICO-JURIDICAL LANDSCAPE?

MANUEL POÊJO TORRES *

AFONSO DE FREITAS DANTAS *

* CIEP Ph.D. Grant Researcher, Research Center of the Institute for Political Studies, Catholic University of Portugal; NATO Consultant

* CIJIC Junior Researcher, Faculty of Law, University of Lisbon; Final Year Undergraduate Student

ABSTRACT

The shifting world order and new technological innovations are in the crux of the ongoing revolution on security affairs, reflecting a set of new emerging challenges. Thus, to navigate the political and juridical pitfalls of state surveillance, democracies are challenged in finding the correct security balance within Open Societies.

This paper is centered on the challenges raised by modern State surveillance and explores the post-Snowden age, the lessons learned from mass state surveillance programmes, how government surveillance undermines the democratic core principal liberties, while highlighting important legal changes – mechanism of oversight – setting the change in this field of study.

Face-recognition technologies serve dually as an enabler of security and as a political disruptor of Open Societies. Several examples are observed to illustrate the governments and industry relationships, as well as, the potential pitfalls of 'face surveillance' and 'black-technologies'.

Given the previous considerations, the Portuguese case is examined given particular attention to its upstanding ranking in the Global Peace Index, and the ongoing transformations to its national legal framework.

Keywords: *Cyber Law; State Surveillance; Face-recognition; Face-surveillance; Black-technologies; Cyberspace; Artificial Intelligence; Open Societies; Civil Liberties; Privacy; Anonymity; Obscurity; Security; Defence; Liberalism; Cyber Tyranny; Autocracy; Portugal; China; U.S.A.*

INTRODUCTION

This paper intends to explore some of the most important challenges to Western societies due to the emergence of dual-use face-recognition capabilities. Geopolitics are once again shifting and as China's economic might grows, surveillance technology stress tests the foundations of liberal democracies.

In an era once again threatened by the rise of authoritarian powers, disruptive economic policies and expansion of proxy-sponsored terrorism, democratic nations look to the East seeking sanctuary in autocratic security practices, largely incompatible with the civil liberties and political rights upheld in the West.

Hence, the paper will start by analysing the ongoing changes in the international system, exploring the phenomenon of the '(trans)nationalisation of crime' and how the emergence of cyber-enabled terrorism served as a catalyst for the rise of modern western State surveillance.

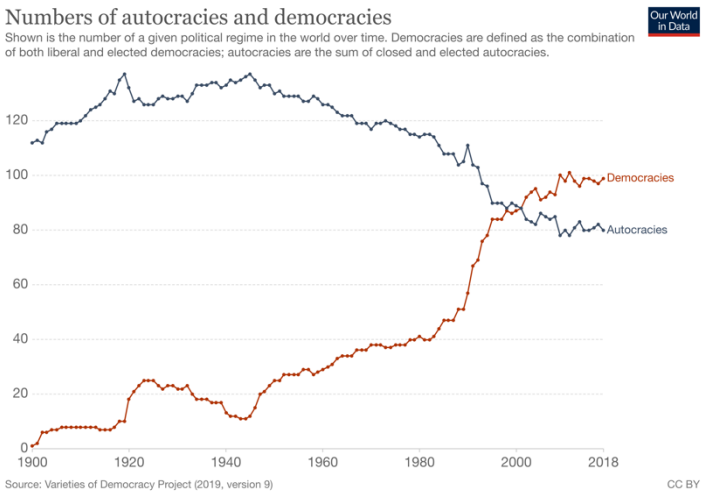
Secondly it will examine the emerging new challenges of surveillance technology, particularly assessing how face-recognition is simultaneously an enabler and a disruptor, while looking as to how the introduction of surveillance technologies may impact legislative changes.

Lastly, this paper will investigate the implementation of facial recognition software in Portugal, analysing the country's legislative stance to new technologies in the past few years and debating the current political and juridical mindset for the advancement or halt of face-recognition state-of-the-art technology.

This study is organized in three main sections respectively: '1. Why is the West introducing State Surveillance?'; '2. Challenges of surveillance technology: is face-recognition an enabler or a political disruptor?'; '3. The impact of face-recognition technologies in the particular case of Portugal'.

1. WHY IS THE WEST INTRODUCING STATE SURVEILLANCE?

After the latest geographical discoveries of the early 20th century, Sir Halford Mackinder, argued that the world had become for the first time, a 'closed system'. Once the globe was mapped, military, political and economic systems closed up on themselves, making it impossible to change a variable without upsetting the whole balance of power in the world[1], in truth,"…no longer exists elasticity of political expansion beyond the conquered territory."[2] Expansions can only occur through the use of force despite the presumptions of legal equality among sovereign states[3], as Cohen adds. In turn, the conclusion of the Cold War not only marked the end of the ideological rivalry between democratic and communist regimes but the implosion of the Union of Soviet Socialist Republics (USSR) allowed new regional competitors to emerge, racing to affirm themselves as regional 'power poles'. The end of the bipolar world and the rise of numerous geopolitical pivots further fragmented the globe, promoting a decentralized power configuration of the world, interlocked by the liberal open market and connected by the *boom* of the cyberspace revolution of the beginning of the 21st century. It is accepted that the fall of the USSR and the emergence of new world actors ignited a fire that ended (with debatable success rates) many autocratic regimes, replacing them with electoral democracies.



Graph 1. – Democracies vs. Autocracies (1900-2018)[4]

1 *In* Mackinder, Halford J. *Democratic Ideals and Reality*, (London: Faber and Finds, 2009), p.29, 200
2 *Ibid.*, p.29
3 Cohen, Saul Bernard. *Geopolitics, the Geography of International Relations*, (Lanham: Rowman and Littlefield Publishers, 2009), p.16
4 Graph from *Our World in Data*, ourworldindata.org/democracy. Accessed 07 June 2020.

Unfortunately, this process also served the agendas of nefarious agents. As foreseen by the Mackinder's inflexible world model, the rise of the cyber globalized world contributed to the upsurge of new international highly organized criminal and terrorist groups, able and willing to exploit the political, economic and security vulnerabilities of liberal democracies. Unlike the organizations of the past, such as the Irish Republican Army (IRA) or Euskadi Ta Askatasuna (ETA), the terrorists of the new era showed prowess in expanding their boundless influence.

Despite terrorists' ability to penetrate air travel was demonstrated by the hijackings in the 1980s, and correlated affinity for mass casualty events established with the attacks to US Marine barracks, African embassies, and to the USS Stark and Cole, the 9/11 events mark a new age for attacks of grand scale and high intensity, changing national and international lawfare forever. The activation of the North Atlantic Treaty's Article V[5] and the adoption of Resolution 1368 (2001)[6] by the United Nations (UN) changed western and global perception on the far-reaching effects of threat networks. To counter this 'new' threat, the UN proposed "preventive measures for combating terrorism which ought to be taken by States at a domestic level"[7] through Resolution 1373[8], but had the misstep of including such vague expressions as the "exchange of information in accordance with international and domestic law", as well as cooperation "on administrative and judicial matters to prevent the commission of terrorist acts". Given the fact that the UN was not to allow unchecked acts of war against third-party states that harboured terrorist organizations, unless duly proven that they were sanctioned by the state itself,[9] the suppression of individual liberties in democratic States was the likeliest of outcomes.

The information outputted through cyberspace, enabled criminal and terrorist groups to build unprecedent coordinated synergies. By winning access to new available open-source intelligence, precise GPS tools, encrypted communications and blockchain-based traceless funds, terrorist groups emulated enough power to combat the Western modern armies. As a

5 The North Atlantic Treaty (1949), 34 UNTS 243, entered into force 24 August 1949
6 United Nations Security Council Resolution (UNSCR) 1368 (2001), "Condemning the terrorist attacks of 11 September 2001 in New York, Washington, D.C. and Pennsylvania, United States of America", UN Doc. S/RES/1368, adopted on 12 September 2001
7 Gasser, Hans-Peter. *Acts of terror, 'terrorism' and international humanitarian law*. International Review of the Red Cross Vol. 84, No. 847 (September 2002), p. 564
8 United Nations Security Council Resolution (UNSCR) 1373 (2001), "On threats to international peace and security caused by terrorist acts", UN Doc. S/RES/1373, adopted on 28 September 2001
9 Guerreiro, Alexandre, "International Law and the Fight Against Terrorism and Cyberterrorism", in *O Direito Internacional e o Uso da Força no Século XXI*, AAFDL Editora, 2018, pp. 327-331

way of counteracting this new reality, national governments enacted legislation that grossly violated individual freedoms.

In the U.S., we saw the creation of the Patriot Act[10], which was set to increase surveillance on individuals that were deemed a threat to the State. As stated by the Department of Justice:

The Act brought the law up to date with current technology, so we no longer must fight a digital-age battle with antique weapons-legal authorities leftover from the era of rotary telephones. (…) Before the Patriot Act, law enforcement personnel were required to obtain a search warrant in the district where they intended to conduct a search. (…) The Act provides that warrants can be obtained in any district in which terrorism-related activities occurred, regardless of where they will be executed, (…) [also allowing] victims of computer hacking to request law enforcement assistance in monitoring the 'trespassers' on their computers.[11]

Alas, the letter and the spirit of the law are not always the same, as the U.S. Government interpretation of the Patriot Act was not necessarily the same as it was written in first place[12].

Mass surveillance has been around the U.S. since the 1920s, but jumped into the public's attention during the wiretapping abuses of the Watergate scandal, culminating with Snowden's revelations[13] of NSA's PRISM[14] programme, upon which the funding of U.S. cyber capabilities dropped sharply in an inverted global trend, as shown in *Graph 2*.

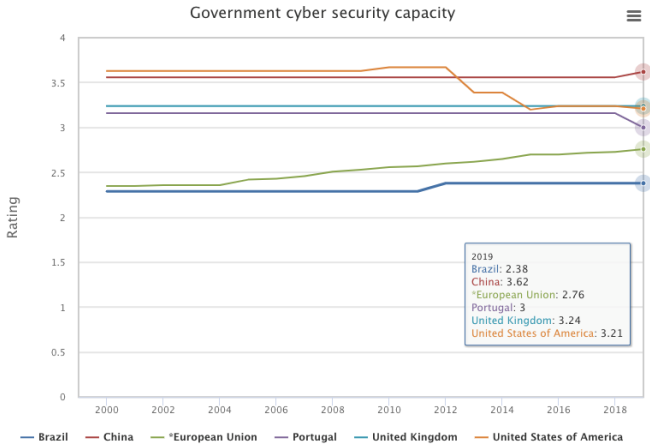
10 U.S. House. 107th Congress. 1st Sess. H.R. 3162, *The USA Patriot Act: Preserving Life and Liberty: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*. Version 1, Oct. 23, 2001

11US Department of Justice. *The USA PATRIOT Act: Preserving Life and Liberty* justice.gov/archive/ll/what_is_the_patriot_act.pdf. Accessed 09 June 2020.

12 Wyden, Ron U.S. Senator. *In Speech, Wyden Says Official Interpretations of Patriot Act Must be Made Public*. Official Press Release, 26 May 2011, wyden.senate.gov/news/press-releases/in-speech-wyden-says-official-interpretations-of-patriot-act-must-be-made-public. Accessed 13 June 2020. In 2011, Senator Wyden warned the U.S. Senate that an extension of the Patriot Act without proper bans on its loose interpretation could lead to public outrage, as it had happened with other surveillance programs in the past.

13 White, April. *A Brief History of Surveillance in the America*. Smithsonian Magazine, April 2018, www.smithsonianmag.com/history/brief-history-surveillance-america-180968399. Accessed 09 June 2020

14 PRISM is a code name given to NSA's SIGAD US-984XN programme used by the Tailored Access Operations' branch, which primary directive was to bypass the privacy laws and remotely access telecommunication companies (Apple, Microsoft, Google, Facebook, Yahoo) raw and complex data packages, retrieving and recording users' personal details.



Graph 2. – Governments Cyber Security Capabilities[15]

In the E.U., legislative approaches to terrorism were left to national governments due to Article 4(2) of the Treaty on the European Union, which states that "national security remains the sole responsibility of each Member State". However, realizing the necessity to create common legal grounds between Member States in the aftermath of 9/11, the European Union created the Framework Decision on Combating Terrorism[16].[17]

At a continental level, the Council of Europe decided than an interstate cooperation was the best way of fighting international terrorism, thereby creating the Council of Europe Convention on the Prevention of Terrorism[18]. Even though its text was very similar to that of the Framework Decision, it was a recognition by all European States that terrorism was now a transboundary threat that required a persistent cooperation and exchange of intel.[19]

The 21st century terrorist groups make use of dual-use technologies to wage modern war and pinpointing targets with precision, setting '*go fund me'* campaigns, through blockchain, engineering successful far reaching strategic communications campaigns, and grow operational cells behind their enemy's lines. The shocking events of 9/11, and the

15 Graph from V-Dem Dataset version 9 (with Polity IV), *Cybersecurity Capacities Index,* www.v-dem.net/en/data/data-version-9. Accessed 09 June 2020.

16 Council of the European Union Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA), OJ L 164 (22 June 2002), p. 3-7, with the following amendments: Council of the European Union Framework Decision 2008/919/JHA and replaced by Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017

17 Immenkamp, Beatrix; Sgueo, Gianluca and Voronova, Sofija. *Briefing: EU Policies – Delivering for Citizens. The fights against Terrorism.* European Parliament Think Tank, 28 June 2019, europarl.europa.eu/RegData/etudes/BRIE/2019/635561/EPRS_BRI(2019)635561_EN.pdf, p. 5. Accessed 09 June 2020.

18 Council of Europe Convention on the Prevention of Terrorism (2005), CETS No. 196, entered into force 01 June 2007

19 Council of Europe, *Explanatory Report to the Council of Europe Convention on the Prevention of Terrorism*, Council of Europe Treaty Series, *No. 196*, 16 of May 2005;

tragedy of *Charlie Hebdo,* are proof of the transfiguration that the world order is suffering. Professor Anne-Marie Slaughter claims, "9/11 was the defining event of the new millennium… [it was] the catalyst for the end of the twentieth-century warfare: large-scale, multi-year deployments requiring the conquest, control and long-term stabilization and reconstruction of foreign territory."[20]

With a death toll of thousands, a new era of hybrid warfare emerges, as the dimensions of war multiplied infiltrating the political society, challenging not only the technological means for its deterrence but for the first time, the legislator himself. As stated by Earle L. Captain Rud and Commander W. Oscar Round the U.S. lost their sanctuary status, which they proudly enjoyed for almost two hundred years[21]. The adversaries of liberalism exploited and corrupted the mechanisms of democracy, supported by a strong cyberspace capability they have expanded the boundaries of the battlespace, infiltrating Western countries and operating from within 'our walls'.

The phenomenon of the '(trans)nationalisation of insecurity', the projections of sharp power and the need to coordinate defences against threats of hybrid natures, pressed the Western democracies to pursue the establishment of State surveillance programmes, involving all sectors of the national defence architecture: the armed forces, national security authorities and joint intelligence agencies.

Democracies are known to react strongly against covert actions of their representatives. One could assume that a secret governmental mass surveillance programme, bypassing privacy laws and used for warrantless criminal investigations, could fail if leaked to the public, but that was not the case. In fact, some lessons were learnt, in 2015 the U.S. passed the Freedom Act[22], ending the bulk collection of data on millions of citizens, but in 2018 the U.S. Congress approved a 6-year extension of the Surveillance Law[23]. Most recently in May 2020, the U.S. Senate approved a revision of the Surveillance Law with sharper privacy safeguards. Since 2013, Western governments increased surveillance transparency by increasing detail granularity within their public national security and strategic intelligence

20 Slaughter, Anne-Marie, et. al. *Reflections on the 9/11 Decade*. RUSI Journal, Vol. 156, No. 4 August-September 2011, p.5

21 Oscar, W., et. al. *Defining Civil Defense in the Information Age*. Strategic Forum No. 46, September 1995, p. 1

22 Sidiqqui, Sabrina. *Congress passes NSA surveillance reform in vindication for Snowden.* The Guardian, 3 June 2015, www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden. Accessed 09 June 2020.

23 Savage, Charlie. *Congress Approves Six-Year Extension of Surveillance* Law. The New York Times, 18 January 2018, www.nytimes.com/2018/01/18/us/politics/surveillance-congress-snowden-privacy.html. Accessed 09 June 2020.

white papers. As investigative journalism graduates the basic 'cyber 101' class, new leaks and reports point towards a sharply increase in the number of known governmental programmes.

The Snowden whistleblowing episode generated global awareness and several NGOs like the Electronic Privacy Information Centre (EPIC) worked actively to keep in check governmental surveillance programmes, however, after Snowden's PRISM came TURBINE, MYSTIC, and countless others. In Europe, the reactions were mixed, as some nations argued that these were common practices in the fight against terrorism, while others felt disrespected and shocked with the NSA's report[24]. The United Kingdom GCHQ's 'Mastering the Internet' programme, launched in 2011, was able to store up to 3 days of national communications and 30 days of metadata from messages, social media posts, and telephone calls[25], later to be distributed to the members of the Five Eyes alliance (intelligence agencies from USA, UK, Canada, Australia and New Zealand). In perspective, PRISM was a massive surveillance endeavour, but not the only one.

Admiral Michael Rogers, director of the NSA (2014-2018) and 2nd Commander of the U.S. Cyber Command expressed that "[t]he increased inter-connectivity of the world we are living in has led to a level of vulnerability that we don't truly understand."[26], which evidently raises legal conundrums on several levels. Truly, the benefit of security has a high cost, mostly paid in freedom, privacy and anonymity. Mass State surveillance cannot be confused – it is on all accounts an instrument of power mostly wielded by authoritarian regimes. The fact that liberal democracies are in the process of implementing it, under the pretence of national security, is as good of a reason as to say that citizens cannot be trusted. Alas, this becomes a categorical defeat for the core principles of democracy, for the civil liberties and liberalism as a whole. In the words of Marc Rotenberg, Professor at Georgetown University Law Centre, "[a] sacrifice of privacy is also a sacrifice of democracy" [27], and adds

Privacy is about accountability. It is about the fairness of decision making. It is about holding large government actors and private companies accountable for their decision

24 Levs, Josh and Schoichet, Catherine E. *Europe furious, 'shocked' by report of U.S. spying*. CNN, 01 July 2013, edition.cnn.com/2013/06/30/world/europe/eu-nsa/index.html. Accessed 09 June 2020.
25 MacAskill, Ewen, et al. *GCHQ taps fibre-optic cables for secret access to world's communications.* The Guardian, 21 June 2013, www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. Accessed 09 June 2020.
26 *in* Shaw, Jonathan. *The Watchers, assaults on privacy in America.* The Harvard Magazine, vol. January-February 2017, harvardmag.com/pdf/2017/01-pdfs/0117-56.pdf, p.59. Accessed 09 June 2020.
27 *Ibid.*, p. 60.

making. It turns out to be an extraordinarily powerful and comprehensive human-rights claim, particularly in the digital age, because so much about us is based on our data[28].

28 *Ibid.*

2. CHALLENGES OF SURVEILLANCE TECHNOLOGY: IS FACE-RECOGNITION AN ENABLER OR A POLITICAL DISRUPTOR?

With the rise of megacities, and high-density population pockets like Tokyo, Shanghai or São Paulo, fighting criminality and ensuring the safety of millions became a herculean task to accomplish. Inserted in a deeply populated, technological and interdependent world, uncoordinated security agencies are rendered inefficient as the dimensions of security multiply. To manage the security threats of the 21st century governments explored new management tools to assess the increasing flow of big data and critically improve the speed of decision-making cycles. Military federated net-centric architectures, incorporating independent sensors, multiple logistic platforms and joint command and control centres, served as a starting point to inspire a revolution in civil security affairs. According to Annette J. Krygiel "[a] system of systems (SoS) is a set of different systems so connected or related as to produce results unachievable by the individual systems alone."[29] Governmental SoS ecosystems (linking security agencies' databases), enabled State authorities to build interconnected infrastructures of surveillance boosting identification, tracing and multi-source information acquisition on their targets and suspects. Consequently, accelerating investigations, neutralizing threat activities and flagging human rights abuses.

Privately developed and commercially available, face-recognition technologies are in high demand by countries with high population densities, but also by Western nations and city officials dreaming of safe, sustainable and efficient smart cities. Titan companies like Hikvision, Huawei, Dahua, NEC, CISCO, Palantir and IBM offer different integration services depending on the client's needs, but work essentially in the same way. The entire process is marketed as seamless and fast with developers assuring a great level of accuracy, despite multiple sources challenging those claims with statistical studies.

When it comes to detection, this phase is normally made in bulk. Faces' passing through a 2D or 3D sensor are automatically aligned, measured and compared to similar or equal

29 Annette J. Krygiel. *Behind the Wizard's curtain: an integration environment for a System of Systems*, Ccrp Publication Series, (Washington DC: National Defence University Press, 1999), p.33

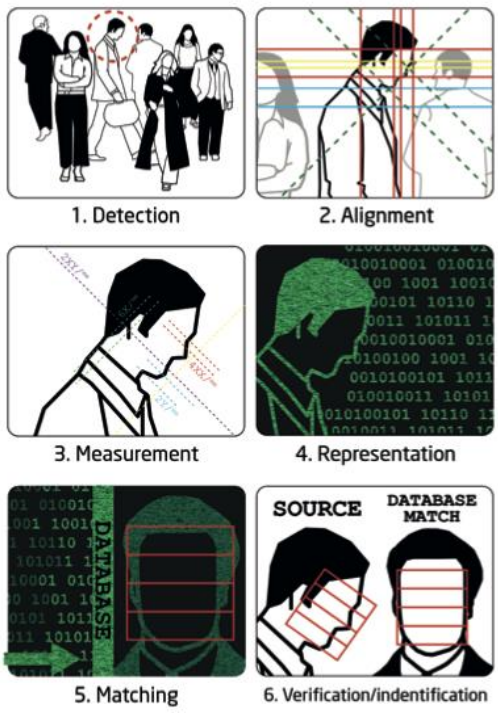


Figure 1. – Face Surveillance ID Steps

digital representations on governmental 'blacklisted' databases. Once a match is acquired, the face shots along with all geospatial metadata associated with it, are stored by the government for validation of 'true-positive' or 'false-positive' match[30]. Face-recognition is powered by A.I. datasets, integrated with deep learning software that learns from millions of face identification iterations, greatly refining its accuracy with time.

In China, face-recognition technology is a hot topic for some time now. In 2018, the Chinese authorities introduced the 'sunglasses program' – a google glasses spinoff – managed by China's 'Skynet Project' and connect to governmental identification digital banks, alerting the authorities whenever a blacklisted individual is detected. The blacklisted citizen is identified in 'augmented reality', by a red box around his face or ID photo, which quickly allows authorities to coordinate a detention. Despite the Hollywood inspired name, the 'Skynet Project', launched in 2011, is a national project led by the Chinese Central Political and Law Commission and jointly initiated by the Ministry of Public Security and the Ministry of Industry and Information Technology. Designed to operate in urban and megacities' environments, Skynet is complemented in rural areas by its sister, the 'Xueliang Project' an investment, part of Chinese 13th quinquennial plan. According to Beijing's 'People's Weekly', Skynet uses HD infrared cameras, which can capture people's facial features and activity trajectories (even at night). It goes on stating that thanks to Skynet, citizens are very happy, as they have found their missing relatives; and that "50,000 surveillance cameras are like 50,000 sleepless police officers always watching, always vigilant" [31]. In an already typical ominous style, Skynet's slogan reads: "20 million shots are guarding you, leaving

30 Krueckeberg, Jennifer et al. *Face Off, the lawless growth of face recognition in the UK policing.* Big Brother Watch, May 2018, bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf, p.11. Accessed 10 June 2020.

31 The source material for this article was 'removed' by People's Weekly and is no longer available. To bypass this 'removal', the authors of this paper suggest using the '*Internet Archive WayBackMachine*' with the People's Weekly link provided, choosing the snapshot of 15th May at 21:59:51. *in* Chen Shixian Li Zhen. *What is Skynet?* Beijing People's Weekly, No. 20, 2017, paper.people.com.cn/rmzk/html/2017-11/20/content_1825998.htm. Accessed 13 June 2020.

criminals nowhere to escape"[32]. In fact, as George Orwell said, "[t]he fallacy is to believe that under a dictatorial government you can be free inside."[33]

While in 2017 there were 176 million cameras estimated in China, now IHS Markit anticipates half a billion active smart cameras until the end of 2020[34]. In this scenario 'Black Tech' is the nickname to remember. It is popularly describes futuristic surveillance technology, and is part of the Hong Kong protestors everyday struggle against the anti-rioter mass surveillance infrastructure. Hence the reason for the protestors' trademark use of reflective sunglasses, face scarfs hiding their ears, nose and mouth, while wielding lasers pointed at buildings, police officers and cars, in a feeble but relentless attempt to blind the cameras sensors distributed around the city.

1.

2.

32 *Ibid.*
33 Orwell, George. *As I Please.* Tribune, 28 April 1944, orwell.ru/library/articles/As_I_Please/english/eaip_04. Accessed 10 June 2020.
34 IHS Markit. *Video surveillance: How technology and the cloud is disrupting the market 2020*. IHS Markit Reports, technology.informa.com/620262/ihs-markit-technology-white-paper-reveals-top-trends-impacting-the-video-surveillance-market-in-2020. Accessed 10 June 2020.

Maps 1. to 4. – Detailed map view of Beijing's Skynet Face-Surveillance cameras[35]

Despite the obvious legal challenges that this technology raises, it is important to stress that in the wake of the 2019 novel coronavirus (2019-nCoV) face recognition technology greatly supported the fight against it. Hikvision's 'Pro Face Access Terminal' is connected online and uses a vanadium oxide uncooled sensor to measure a person's temperature and has integrated multiple alarm mechanisms to ensure the measurements are as precise as possible. This type of technology is now being widely distribute across international organizations, corporations, commercial retailers and even private homes, as temperature checking becomes the first line of defence against this global threat.

In the advent of 5G networks, big data analytics, deepfakes and 'Artificial Internet of Things' (AIoT), face-recognition technology and black-tech keep raising the legal debate over surveillance to new heights. Despite the many efforts of civil liberties' watchdogs and NGOs denouncing the stealthy implementation of face-surveillance in liberal democracies, it rendered only localized effects. Still, there is a vacuum of public-wide debates on the topic of face-recognition, legal constraints and surveillance oversight mechanisms – typical democratic checks and balances, over those that wield authority and power.

35 Maps sourced from the 'Gao De Maps' app – a clone of Google maps, not banned or blocked in China.

Country	Region	Aggregate Regime Score 2018	Regime Type	"Freedom on the Net 2018" Status	"Freedom on the Net 2018" Total Score	Military Expenditures (USD) 2018	Military Expenditures Global Ranking (2018)	Belt & Road Initiative Countries	China ODI - Global Ranking (EIU)	Smart City/Safe City	Facial Recognition	Smart Policing	China AI Tech	US AI Tech	Japan AI Tech	Key Companies
Algeria	MENA	3.32	EA			9583.7	25		56			✓	✓			BAE, Huawei
Argentina	WHA	7.87	ED	FREE	28	4145.0	43		51		✓	✓	✓		✓	Axis, Bosch, Dahua, Huawei, NEC, ZTE
Armenia	EUR	4.94	EA	FREE	27	608.9	81	✓		✓	✓		✓			Hikvision, Huawei
Australia	EAP	9.18	LD	FREE	21	26711.8	13		5	✓	✓	✓	✓	✓	✓	CrowdOptic, Hikvision, Huawei, Infinova, NEC, Palantir
Bahrain	MENA	1.72	CA	NOT FREE	71	1396.8	65	✓			✓	✓	✓			Dahua
Bangladesh	SCA	4.36	EA	PARTLY FREE	51	3894.7	44	✓		✓	✓	✓	✓			Huawei
Bolivia	WHA	6.27	ED			618.8	79	✓		✓	✓	✓	✓			CEIEC, Huawei, ZTE
Botswana	AF	7.33	ED			529.5	86			✓		✓	✓			Huawei
Brazil	WHA	7.30	ED	PARTLY FREE	31	27766.4	12		52	✓	✓	✓	✓	✓		Axis, Dahua, IBMN
Burma/Myan	EAP	4.18	EA	NOT FREE	64	2030.5	58	✓		✓	✓		✓			Hikvision, Huawei
Canada	WHA	9.18	LD	FREE	15	21620.6	14		8		✓	✓		✓		Avigilon, Palantir
Chile	WHA	8.63	LD			5570.7	34		9		✓	✓	✓			Huawei
China	EAP	1.77	CA	NOT FREE	88	249996.9	2			✓	✓	✓	✓	✓	✓	Mult; Axis, Bosch, IBM, Microsoft, Seagate, Qualcomm
Colombia	WHA	6.73	ED	PARTLY FREE	31	10602.9	24		55	✓	✓	✓			✓	NEC
Czech Republ	EUR	8.34	LD			2710.0	53	✓	16		✓	✓				
Denmark	EUR	9.27	LD			4228.2	42		17	✓	✓	✓	✓	✓		Avigilon, BrainChip, Cisco, Hikvision, Palantir
Ecuador	WHA	6.43	ED	PARTLY FREE	40	2549.4	55		57	✓	✓	✓	✓	✓		CEIEC, Cisco, Huawei
Egypt	MENA	2.56	EA	NOT FREE	72	3110.0	51	✓	49		✓	✓	✓	✓		Honeywell, Huawei
France	EUR	8.43	LD	FREE	25	63799.7	5		27	✓	✓	✓	✓	✓	✓	Hikvision, Huawei, Palantir, Teleste, Thales, ZTE
Georgia	EUR	6.19	ED	FREE	25	316.5	100	✓			✓	✓			✓	NEC
Germany	EUR	8.82	LD	FREE	19	49470.6	8		20	✓	✓	✓	✓	✓		Cisco, Huawei, Palantir
Ghana	AF	7.14	ED			218.4	110			✓			✓			Huawei
Hong Kong	EAP	5.14	ED						3		✓		✓			Bosch, Huawei
India	SCA	6.60	ED	PARTLY FREE	43	66510.3	4		36	✓	✓	✓	✓	✓	✓	ADRIN, Hikvision, IBM, Infinova, Microsoft, NEC
Indonesia	EAP	6.63	ED	PARTLY FREE	46	7437.2	26	✓	26	✓	✓	✓	✓	✓	✓	Huawei, NEC, PT Industri Telekomunikasi Indonesia
Iran	MENA	3.57	EA	NOT FREE	85	13194.2	18	✓	19		✓	✓	✓			Hikvision
Iraq	MENA	3.36	EA			6318.0	32	✓		✓	✓		✓			Huawei
Israel	MENA	5.99	ED			15946.8	17	✓	11	✓	✓	✓		✓		AnyVision, BriefCam, Elbit, IBM, NICE, Verint
Italy	EUR	8.45	LD	FREE	25	27807.5	11	✓	50	✓			✓			Huawei
Ivory Coast	AF	5.25	ED			607.8	82			✓			✓			Huawei
Japan	EAP	8.56	LD	FREE	25	46618.0	9		14	✓	✓	✓	✓		✓	Hikvision, NEC

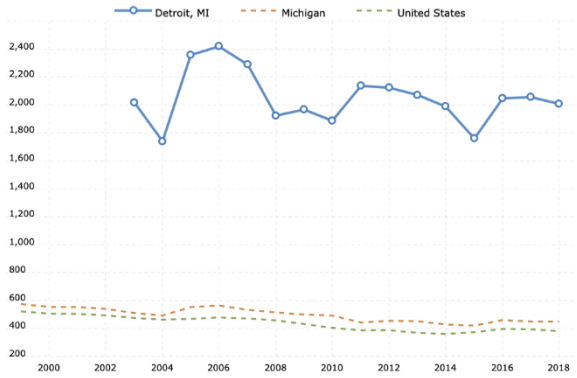
Table 1. – Global A.I. Surveillance Index for 2019[36]

The chart above illustrates a sample of countries that have already implemented face-recognition technology, with black-tech mostly sourced from China, with a visible commercial footprint from titans like Hikvision and Huawei, common suspects in this expanding economic sector. This index shows that the majority of highlighted liberal democracies are in the process of transitioning into a 'smart city', with deployed face-recognition tech supplied from multiple companies, hence ensuring that no single supplier wields technical security monopoly over one's country. Italy, on the other hand, has endorsed the Chinese Belt and Road Initiative and have opted for contracting A.I. surveillance systems from the giant Huawei, even after EU and NATO highly recommending against it. The privatization of a State's security systems is a serious issue, as now, more than ever, the security of one, is in fact the security of all. Professors Evan Selinger and Woodrow Hartzog emphasize the problem of the ghost in the machine, by underlining that "…if facial recognition becomes entrenched in the private sector by procedural frameworks, that means that in addition to a warrant framework's accretion problem, the government will also have a backdoor to retroactive surveillance via the personal data industrial complex."[37]

36 Carnegie Endowment for International Peace: *AI Global Surveillance Index 2019.* carnegieendowment.org/files/AI_Global_Surveillance_Index1.pdf. Accessed 11 June 2020.

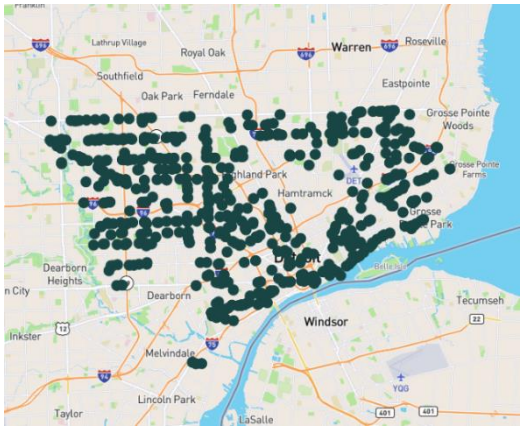
37 Evan Selinger and Woodrow Hartzog. *The Inconsentability Of Facial Surveillance.* Loyola Law Review, vol. 66, no. 101, 2019, p.122.

This has the potential to become an exceptional dangerous technology, as it keeps rendering itself a threat to the legal value of 'privacy'. Moreover, face-surveillance hinders the deep-rooted autonomous behaviour of a society, a distinctive characteristic of liberal democracies. It is also not proven that face-recognition programmes drastically decrease the rate of crimes, or that it is effective in deterring violent behaviours in surveyed cities.

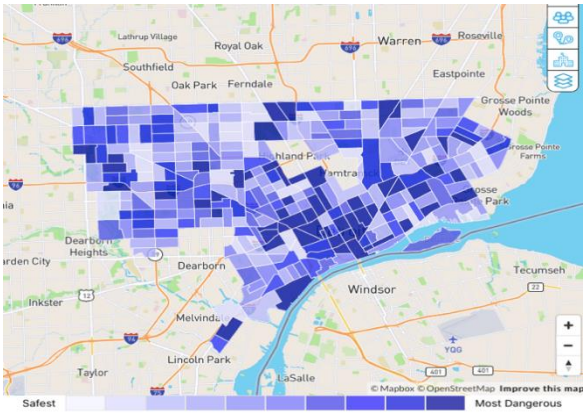


Graph 3. – The Detroit Crime Rate for 2018 was 2007.82 per 100,000 population, a 2.38% decline from 2017[38]

In the city of Detroit, face-recognition cameras were deployed in 2016 as part of the Project Green Light[39] (PGL), however, official crime rate data released by the F.B.I., shows only a 2.38% reduction since 2017 – a decrease, yes but not an easily correlated one with PGL.



Map 5. – Location of PGL Cameras (2020)[40]



Map 6. –Detroit's Neighbourhoods Safety Rate (2020)[41]

38 Federal Bureau of Investigation. *Crime in the United States by Metropolitan Statistical Area, 2018.* ucr.fbi.gov/crime-in-the-u.s/2018/crime-in-the-u.s.-2018/topic-pages/tables/table-6. Accessed 11 June 2020.
39 City of Detroit, Police Department official website. *Project Green Light Detroit.* detroitmi.gov/departments/police-department/project-green-light-detroit#block-views-block-featured-unified-block-1. Accessed 11 June 2020.
40 City of Detroit, Police Department official website. *Project Green Light Detroit.* detroitmi.gov/webapp/project-green-light-map. Accessed 11 June 2020.
41 Neighborhood Scout. *Detroit, MI Crime Rates.* neighborhoodscout.com/mi/detroit/crime. Accessed 13 June 2020.

In a democracy it is expected and rational for people to weight on benefits versus costs of political decisions. The current benefits of Detroit's PGL seem short given its high social cost. As observed in maps 5 and 6, the deployment of PGL face-surveillance cameras did not significantly impact the safety scale of those neighbourhoods.

A 2018 MIT study concluded that several face-recognition algorithms from commercial retailers had an unexpectable high misidentification rate, with 34.7% failure in identifying dark skinned women, with the female gender[42]. Joy Buolamwini, founder of the Algorithmic Justice League, wrote a reminder in an New York Times Op-Ed "…that artificial intelligence, often heralded for its potential to change the world, can actually reinforce bias and exclusion, even when it's used in the most well-intended ways"[43]. In fact, publicly disclosed face-surveillance programmes generate a 'chill effect', momentarily conditioning behaviours and undermining the results of the overt surveillance all together. Conversely, the clandestine use of face-recognition algorithms can become target of public protest and political backlash with severe legal implications, as was the case of the ban of face-recognition software in San Francisco, a technologically friendly city, that fought against a constant state of surveillance[44].

This constitutes a problem of several dimensions, illustrated by the lack of fairness towards those misidentified, which pictures and data are processed and stored in governmental databases without their knowledge[45]; by those that are wrongfully accused of crimes they did not commit, or, unethically flagged by A.I. predictive behaviour software; and lastly by the continuous exploitation of democracy's civil liberties, as Open Societies cannot survive in state of constant surveillance. Selinger and Hartzog go even beyond and stress that the debates over face-surveillance "…are framed around the concepts of 'privacy' and 'anonymity' instead of 'obscurity', [as they propose], framing surveillance issues generally, and facial recognition specifically, as a loss of 'obscurity', a diminution that clearly detracts from many of the goods that autonomy is valued for enabling."[46]

---

42 Hardesty, Larry. *Study finds gender and skin-type bias in commercial artificial-intelligence systems*. MIT News Office, 11 February 2018, news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212. Accessed 11 June 2020.

43 Buolamwini, Joy. *When the Robot Doesn't See Dark Skin.* The New York Times, 21 June 2018, nyti.ms/2MMBFv5. Accessed 12 June 2020.

44 Conger, Kate et al. *San Francisco Bans Facial Recognition Technology*. The New York Times, 14 May 2019, nyti.ms/2VG3Zr9. Accessed 13 June 2020.

45 Krueckeberg, Jennifer et al. *Face Off, the lawless growth of face recognition in the UK policing.* Big Brother Watch, May 2018, bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf, p.11. Accessed 12 June 2020.

46 Evan Selinger and Woodrow Hartzog. *The Inconsentability Of Facial Surveillance.* Loyola Law Review, vol. 66, no. 101, 2019, p.114

In 2016, EUROPOL and the EU Cyber Security Agency, released a joint statement on the issue of 'privacy v. encryption', highlighting that

individual's rights need to be evaluated carefully in relation to the individual rights of others…", thus, "…in the face of serious crimes, law enforcement may lawfully intrude privacy or break into security mechanisms of electronic communication systems. Legislation must explicitly stipulate the conditions under which law enforcement can operate.[47]

In the same way, one could argue that a strong but enabling legal framework needs to be in place to oversee the use of face-surveillance technology, on a tailored case-by-case situation. Ensuring that an undergoing intrusive investigation is proportional to the crime that was committed, solely invading privacy of the strictly necessary people, and in the shortest time-frame possible, in a transparent and traceable manner for those involved.

Face-recognition join a vast list of black-technologies that challenge the convention by concurrently enabling ones, while disrupting others. Whereas some storm the stores to buy the latest smart face thermometers, security cameras or Apple devices – deepening their data-centric immersion – others, cannot escape, or as Chris Gillard puts it, "[a]s one group pays to be watched, other groups continue to pay the price for being watched."[48] Those that chose not to be watched upon, are *quasi* prisoners of the system, as they need to wrestle against a socially and politically disruptive surveillance infrastructure leviathan. As face surveillance generates a chill effect, democratic open societies suffer the most. An Orwellian surveillance mechanism shifts democratic spontaneous orders into artificial, man-made constructions, where its inhabitants behave, not as free men and women, but as slaves of the algorithm, attempting to avoid triggering the system.

If not controlled by an oversight legal framework, black-technology may allow for the public/private industrial complex to abuse the legal right to anonymity and obscurity, eroding the democratic civil liberties such as freedom of assembly and association, freedom of expression, as well as, political and religious liberties. Mapping and tagging citizens association preferences, circles of influence, storing mugshots and geolocation metadata, is a step closer to a 'cyber tyranny' rather than anything else. Democratic people, and citizens of

47 ENISA and EUROPOL. *On lawful criminal investigation that respects 21st Century data protection. Europol and ENISA Joint Statement*. enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection. Accessed 11 June 2020.

48 Gilliard, Chris. *Privacy's Not an Abstraction*, Fast Company, 25 March, 2019, fastcompany.com/90323529/privacy-is-not-an-abstraction. Accessed 10 June 2020.

any law-abiding nation, must not be confused with insurgent fighters in a grand threat network.

3. THE IMPACT OF FACE-RECOGNITION TECHNOLOGIES IN THE PARTICULAR CASE OF PORTUGAL

Following a security trend in the European Union, Portugal has also introduced face-recognition technology in airports, border controls and large public events. Despite the growing maturity of this technology, the Portuguese implementation remains slow, as face-surveillance has been essentially employed by the Police Research Laboratory, in the control of foreign citizens[49] and access to casino game floors[50]. The latter example is an interesting measure, as it blocks blacklisted addicted players from entering, but at the same time it is an example of how 'state paternalism' is gaining physical embodiment and is able to interact in real-time with its citizens. It is not difficult to conjecture on what would happen if the embodied State was able to enforce its power on citizens forgetting to pay their social security contributions, taxes, water bills or parking tickets.

Portugal was not always so willing to implement these new type of security technologies, as to a point of not even contemplating the implementation of video-surveillance in public places. After the toppling of the totalitarian Second Republic (also known as "Estado Novo") by the Carnation Revolution of 1974, social mindset was mostly divided between Democratic Socialism and Communism, with the latter having gained greater political influence, as it was clear in the original version of Article 2[51] and the functions attributed to the Council of the Revolution.

Even after the first constitutional amendment in 1982, that transformed Portugal into a full-fledged democracy,[52] this socio-political mindset never really disappeared and is still very present in the enactment of laws by the legislative bodies, with most interventions that

49 Capucho, Joana. *Na polícia, no carro, no aeroporto, o reconhecimento facial já não é ficção*. Diário de Notícias, 15 January 2018, dn.pt/sociedade/na-policia-no-carro-no-aeroporto-o-reconhecimento-facial-ja-nao-e-ficcao-9047999.html. Accessed 12 June 2020.

50 Trigueirão, Sónia. *Casinos: Turismo de Portugal gastou 338 mil euros mas reconhecimento facial não funciona.* Público, 06 May 2019, publico.pt/2019/05/06/economia/noticia/turismo-gastou-338-mil-euro-reconhecimento-facial-nao-funciona-1871551. Accessed 12 June 2020.

51 "The Portuguese Republic is a democratic state, based on popular sovereignty, respect and the guarantee of fundamental rights and freedoms and pluralism of expression and democratic political organization, which aims to ensure the transition to socialism by creating conditions for the democratic exercise of power by the working classes." *in Decreto de Aprovação da Constituição,* Diário da República n.º 86/1976, Série I de 1976-04-10

52 Freitas do Amaral, Diogo. *A transição para a Democracia – memórias políticas*. Vol. II, Bertrand Editora, 2008, p. 348: "If the Communist-style Revolution, attempted in Portugal, ended in the streets and barracks on November 25, 1975, it remained, however, for about seven more years in the Constitution, the laws, the Council of the Revolution, the self-government of the Armed Forces, the constitutional obligation to walk towards socialism, etc. And it only ended, in the constitutional order, on 30 September 1982: precisely eight years, five months and five days after 25 April 1974." (translated from Portuguese).

attempt to enlarge the State's surveillance and security being perceived, to a certain extent, to be 'fascist' in nature.

Of the seven constitutional revisions made to this day, only the first five approached matters related to the "constitutional regime of security".[53] In the words of Rui Pereira, Professor at the *Instituto Superior de Ciências Sociais e Políticas* (ISCSP) of the University of Lisbon:

In short, after three revisions with a more 'garantistical' imprint, which took the form, for example, of improving the systems of the state of siege and the state of exception and providing for restrictions on individual freedom, the 4th and 5th constitutional revisions already make it possible to identify a 'securitarian' line, dictated by the needs of prevention, repression and investigation into increasingly prolific, serious, violent and complex crime.[54]

In the 4th revision, we saw a reinforcement of legislative power for Parliament, making it the only legislative body that could alter "the regime governing the Republic's intelligence system and state secrets"[55] and the "regime governing municipal police forces and the form in which they are created"[56]. In the 5th revision, the Constitution was adapted in order for Portugal to ratify the Rome Statute of the International Criminal Court and due to the 9/11 attacks, the inviolability of a person's domicile was reduced in the cases of highly organized crime and terrorism[57].[58]

As we can see, Portugal's Constitutional approach to matters of privacy and fundamental rights hasn't changed much over the years, both a reflection of the socio-political mentality of the legislative power and of how the country has been unaffected by acts of domestic and foreign aggression in decades.

The Institute for Economics & Peace reported that Portugal is currently ranking 3rd place in the 2020 Global Peace Index, only behind New Zealand and Iceland, with Syria and Afghanistan ranking last[59]. In a moment when the 2019-nCoV forced the reinstatement of old borders and when Spain, Italy and the U.K. are struggling to contain the social, economic and political implications of the current humanitarian crisis, Portugal keeps to a steady course and

53 Bacelar Gouveia, Jorge. *Direito da Segurança - Cidadania, Soberania e Cosmopolitismo*. Almedina, 2018, p. 188

54 Pereira, Rui. *A Segurança na Constituição*. Estudos de Direito e Segurança, Vol. II, 2nd Edition, Almedina, pp. (p. 414) (translated from Portuguese)

55 Article 164(q) of the Constitution of the Portuguese Republic. Diário da República, *Decreto de Aprovação da Constituição*, n.º 86/1976, Série I de 1976-04-10.

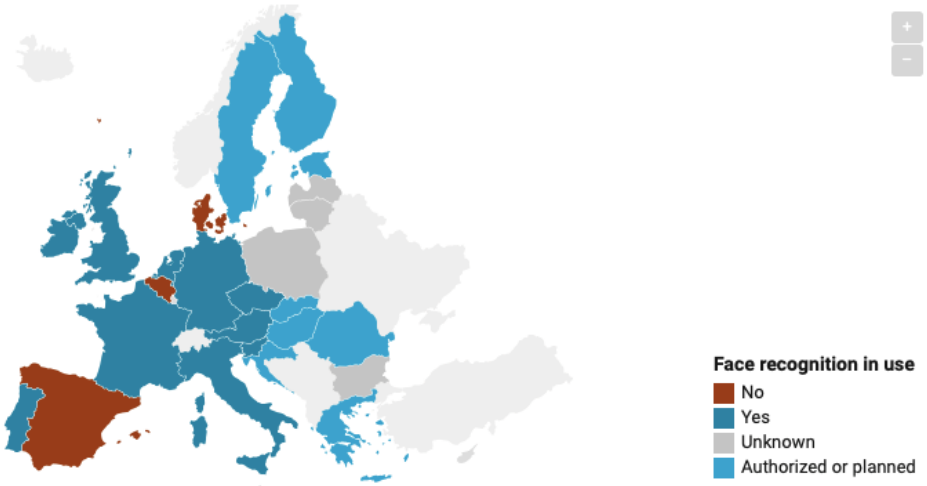
56 Article 165(1)(aa), *Ibid*

57 Article 34(3), *Ibid*

58 Bacelar Gouveia, Jorge. supra note 53, pp. 196-203

59 Institute for Economics & Peace. *Global Peace Index 2020: Measuring Peace in a Complex World*. Sydney, June 2020, visionofhumanity.org/app/uploads/2020/06/GPI_2020_web.pdf, p.8. Accessed 13 June 2020.

rises to the top as the 2nd most peaceful country of Europe[60]. Given that Portugal has ascended to this position without the use of face-surveillance programmes and black-tech, what could be the reason to lobby for its introduction in the Portuguese society?



Map 7. – Face-recognition implemented in the EU[61]

There are five laws regarding video-surveillance in Portugal, as of this moment:

- Law No. 1/2005, of 10 January, that regulates the use of video cameras by security forces and services in public places of common use;
- Decree-Law No. 207/2005, of 29 November, that regulates the means of electronic road surveillance used by security forces;
- Law No. 51/2006, of 29 August, that regulates the use of road surveillance systems by *EP - Estradas de Portugal* (Roads of Portugal company) and road concessionaires;
- Law No. 33/2007, of 13 August, that regulates the installation and use of video surveillance systems in taxis;
- Law No. 34/2013, of 16 May, that regulates the use of video surveillance systems by private security and self-protection services.

60 *Ibid.* p.15
61 Kayser-Bril, Nicolas. *At least 10 police forces use face recognition in the EU, AlgorithmWatch reveals.* Algorithm Watch, 11 December 2019, algorithmwatch.org/en/story/face-recognition-police-europe. Accessed 12 June 2020.

Despite these laws, there is no specific national legislation for facial recognition software or other aspects regarding A.I. that may be implanted. Regulation is, instead, implemented through interpretation and supervision by the National Data Protection Commission (CNPD), the legal body that enacts the General Data Protection Regulation (GDPR) and similar European legal documents in Portugal, in accordance with Article 3 of Law No. 58/2019, of 8 August. For this matter, the CNPD has at its disposal:

- Working Party 29's Opinion 3/2012 on developments in biometric technologies;[62]
- Directive 2016/680 Data Protection Law Enforcement Directive;[63]
- Regulation 2016/679 General Data Protection Regulation (GDPR);[64]
- European Agency for Fundamental Rights paper on "Facial recognition technology: fundamental rights considerations in the context of law enforcement";[65]
- European Commission (EC) White Paper "On Artificial Intelligence – A European approach to excellence and trust".[66]

The CNPD has quite recently made two Opinions relating to the use of facial recognition software in the cities of Portimão[67] and Leiria[68]. The problem pertaining to both cases was not a legal one *per se*, but one of balance between matters of proportionality vs individual privacy and inadequate justification by the authorities when writing the request.

62 Working Party for Article 29 of Directive 95/46/EC. *Opinion 3/2012 on developments in biometric technologies*. Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf. Accessed 13 June 2020.
63 Directive 2016/680/EU 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 199 (4 May 2016), p. 89
64 Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 199 (4 May 2016), p. 1
65 European Union Agency for Fundamental Rights. *Facial recognition technology: fundamental rights considerations in the context of law enforcement*. Publications Office of the European Union, 2020
66 White Paper of 12 February 2020 from the European Commission on Artificial Intelligence – A European approach to excellence and trust [COM(2020) 65 final]
67 Comissão Nacional de Proteção de Dados, Parecer/2019/92, Processo PAR/2019/61
68 Comissão Nacional de Proteção de Dados, Parecer/2019/93, Processo PAR/2019/62

Article 2(1)(c) of Law No 1/2005, of 10 January, states that the implementation of surveillance must be made to protect people and goods and/or to prevent acts that legally constitute as a crime, when there is reasonable risk for such an occurrence.

In the case of Portimão, the Public Safety Police (PSP) requirement indicated that they were to be implemented in certain areas to prevent acts of vandalism and road infractions, with the introduction of 'soft recognition' technology, but lacked to justify its necessity. We believe that this is not even a case that needs a judgment of proportionality in legal terms, as it a mere case of inadequate presentation of a surveillance proposal.

To put in context, Portimão is mostly a holiday destination, with greater affluence during the Summertime. To this extent, some areas may be subjected to vandalism, to which the implementation of 'simple' security cameras were sufficient for the case at hand. But, in the advent of powered A.I. surveillance, the CNPD's justifications on the matter of rights, liberties and guaranties, as mentioned in page 7,[69] appears to be quite excessive as it seems to transpire the idea that giving police access to these types of data would make them similar to that of the Orwellian State embodied by the People's Republic of China (PRC).

The case of Leiria is quite different, given the fact the city already had security cameras in certain areas, with the proposal attempting to triple its number and to introduce A.I. with machine learning, making it a distinct scenario from that of Portimão. Besides, the previous Opinion entirely rejected the introduction of surveillance, while the current one in analysis concluded that further study should be made on the impact of machine learning and 'soft recognition' on fundamental rights.

Given the dangers posed by machine learning, an 'introduction' to the principle of proportionality is in order. The Constitution, through Article 18(2) and (3) and Article 165(1)(b), reserves to the legislator the possibility of constricting fundamental rights, with any interpretation made by a judge or Administrative entity being insufficient to replace the ponderation that befalls on the legislator between conflicting constitutional values.[70]

69Comissão Nacional de Proteção de Dados, supra note 67: "Thus, bearing in mind that this processing involves large-scale systematic monitoring in the city of Portimão and that it promotes the tracking of people and their behaviour and habits, as well as the identification of people from data relating to physical characteristics, it is undeniable that there is a high risk to people's rights and guarantees, in particular the fundamental rights to data protection and respect for private life, as well as to freedom of action and the right to non-discrimination." (translated from Portuguese).

70 Sérvulo Correia, J. M. *Direitos Fundamentais – Sumários*. Escritos de Direito Público: Direito Constitucional, Direito Europeu e Direito Internacional Público, Vol. IV, Almedina, 2019, pp. 77-161 (p. 153)

The principle is divided into three subprinciples: the principle of adequacy (the measures provided for by law must prove to be an appropriate means of protecting the end of the law); the principle of enforceability (restrictive measures must become necessary, since the ends sought by the law would not be achieved by any other means); and the principle of proportionality in the strict sense (the legal restrictive means and ends obtained must be fair, in order to prevent disproportionate measures);[71]

In our case, most common interpretations steer in the immediate direction of individual liberties being a higher value than security. Regarding machine learning, we will also agree, as A.I. bias through any sort of profiling can be highly prejudicial to a democracy through discrimination based on facial expressions, skin color, political ideology, religious group and sexuality. Human bias is damaging as it is, with the recent murder of George Floyd sparking attempts to dissolve police departments in the United States, one of the pillars of any well-established democracy.

It is strange for the CNPD to demonstrate both reasonability and excess on approaching the exact same problem in two distinct cities, however, these are the first cases of implementation of this kind, so further observations are needed to understand how well ponderations will be made regarding surveillance in the future. Even though it is not directly linked to surveillance, the Agency for Administrative Modernization (AMA) has launched a public bid[72] for the implementation of face recognition technology, either through cellphones or personal computers, that would allow the users remote access to the *Chave Móvel Digital* (CMD), a digital signature that "allows the user to access several public or private websites, and sign digital documents, with a single login"[73].[74] When it is time for the CNPD to make its evaluation on the impact to privacy by these services, we can only expect due ponderation on the pros and cons, as ethical hacker groups stress, 'knowledge-based' login credentials are safer than any other type of biometric inputs, like fingerprint scan or face recognition.

71 Canotilho, J. J. Gomes.Vital Moreira. *Constituição da República Portuguesa Anotada*. Vol. I, 4th Edition, Coimbra Editora, 2007, pp. 392-393

72 *Concurso Público N.º 235/19/DCP/GACD/Software de Reconhecimento Facial e Deteção de Vida.* Diário da República, Anúncio de procedimento n.º 13672/2019, Série II de 2019-12-10

73 Agência para a Modernização Administrativa, IP. *O que é a chave-móvel*. autenticacao.gov.pt/a-chave-movel-digital. Accessed 14 June 2020.

74 Séneca, Hugo. *Governo avança com reconhecimento facial, apesar de riscos. AMA não revela participantes do concurso*. visao.sapo.pt/exameinformatica/noticias-ei/mercados/2020-01-13-governo-avanca-com-reconhecimento-facial-apesar-de-riscos-ama-nao-revela-participantes-do-concurso. Accessed 14 June 2020.

Given the fact that this is part of an ongoing effort by the Portuguese Government to modernize Public Administration[75], one can assume a double purpose in the lobbying efforts for the implementation of face-recognition technology, those being: a) the desire to secure and protect the tourism sector's economic national interests; and b) strengthen the efforts to modernize analog public services.

75 Agência para a Modernização Administrativa, IP. *Plano de Atividades 2019.* ama.gov.pt/documents/24077/28687/PA+2019_AMA_20191216_VF.pdf/8c351ce4-4f38-4e10-9245-67e0c3f1353f. Accessed 14 June 2020

CONCLUSIVE REMARKS

As the 21st century bred a hyper wired and interconnected society, eroding the boundaries of battlespace, adversaries of democracy were able to project their power and influence bypassing the most modern defence lines. In a world that has become more opaque, civil-military joint operations based on federated intelligence networks have become vital to prevent threats. As megacities and populations continue to grow, the construction of an A.I. powered surveillance infrastructure could be ever-more enticing to control and predict threats in these new 'urban battlegrounds'.

Despite this, one should not ignore the disruptive impacts of face-recognition technologies in democratic societies. State surveillance is no longer an exclusive characteristic of authoritarian regimes, rather, it is becoming an Orwellian feature of liberal democracies, accompanied by prolific politic and legal pitfalls that if not properly tackled, can surely betray democratic regimes and disrupt the nature of open-societies.

Modern surveillance practices in democracy should be distinctively different from autocratic-based surveillance methods, where covert and overt, warrantless mass investigations take place. 'Security', by itself cannot transcend into a neo-Darwinian dimension, where only those with the best capabilities to adapt, should have the ability to survive. Instead, face-recognition and related State surveillance technologies should be implemented within democratic states in the same way that power is transferred from the People to the figure of the Government - through the rule of law, checks and balances and transparent audit mechanisms.

Portugal is still very 'conservative' on matters related to fundamental rights, as proven by its juridical standpoint on the protection of one's private life, a reality that will hardly change soon. We are now observing an attempt at modernizing services using face-recognition software, but it will be a slow pace until actual changes will be taken into effect. We find that Portuguese regulatory and legislative bodies, should make an approach that is prudent to the protection of personal privacy, but in line with the technological and security necessities of the 21st century.

The creation of oversight commissions is a first step in halting abuses, and ensuring the lawful use of this technology, only then can *we* protect and empower democracies. Innovation in general and technological revolutions, should be implemented slowly, while observing the different national political cultures and respecting core principles of liberty. Democracies should distinguish themselves from autocracies and ensure greater transparency regarding

their surveillance policies. They should facilitate security education by openly discussing rights and responsibilities, before asking their citizens to feed the Big State with more biometric data. While ordered freedom needs security to survive, secure environments thrive in the absence of liberty.

"If you want total security, go to prison. There you're fed, clothed, given medical care and so on. The only thing lacking… is freedom."

– Dwight D. Eisenhower

BIBLIOGRAPHY

Books

- Krygiel, Annette J. *Behind the Wizard's curtain: an integration environment for a System of Systems*, Ccrp Publication Series, Washington DC: National Defence University Press, 1999;
- Bacelar Gouveia, Jorge. *Direito da Segurança - Cidadania, Soberania e Cosmopolitismo*. Almedina, 2018;
- Baylis, John, et. al. *Strategy in the Contemporary World*. Oxford University Press, 2007;
- Canotilho, J. J. Gomes; Vital Moreira. *Constituição da República Portuguesa Anotada*. Vol. I, 4th Edition, Coimbra Editora, 2007;
- Cohen, Saul Bernard. *Geopolitics, the Geography of International Relations*, Rowman and Littlefield Publishers, 2009;
- European Union Agency for Fundamental Rights. *Facial recognition technology: fundamental rights considerations in the context of law enforcement*. Publications Office of the European Union, 2020;
- Freitas do Amaral, Diogo. *A transição para a Democracia – memórias políticas*. Vol. II, Bertrand Editora, 2008
- Gray, Colin S. *Another Bloody Century*. Phoenix Books, 2006;
- Mackinder, Halford J. *Democratic Ideals and Reality*, Faber and Finds, 2009;
- Pereira, Rui. *A Segurança na Constituição*. Estudos de Direito e Segurança, Vol. II, 2nd Edition, Almedina;
- Sérvulo Correia, J. M. *Direitos Fundamentais – Sumários*. Escritos de Direito Público: Direito Constitucional, Direito Europeu e Direito Internacional Público, Vol. IV, Almedina, 2019;

Articles

- Buolamwini, Joy. *When the Robot Doesn't See Dark Skin.* The New York Times, 21 June 2018, nyti.ms/2MMBFv5. Accessed 12 June 2020;

- Capucho, Joana. *Na polícia, no carro, no aeroporto, o reconhecimento facial já não é ficção.* Diário de Notícias, 15 January 2018, dn.pt/sociedade/na-policia-no-carro-no-aeroporto-o-reconhecimento-facial-ja-nao-e-ficcao-9047999.html. Accessed 12 June 2020;
- Chen Shixian Li Zhen. *What is Skynet?* Beijing People's Weekly, No. 20, 2017, paper.people.com.cn/rmzk/html/2017-11/20/content_1825998.htm. Accessed 13 June 2020;
- Conger, Kate et al. *San Francisco Bans Facial Recognition Technology*. The New York Times, 14 May 2019, nyti.ms/2VG3Zr9. Accessed 13 June 2020;
- Evan Selinger and Woodrow Hartzog. *The Inconsentability Of Facial Surveillance.* Loyola Law Review, vol. 66, no. 101, 2019;
- Gasser, Hans-Peter. *Acts of terror, 'terrorism' and international humanitarian law*. International Review of the Red Cross, Vol. 84, No. 847, September 2002;
- Gilliard, Chris. *Privacy's Not an Abstraction*, FAST COMPANY, 25 March, 2019, fastcompany.com/90323529/privacy-is-not-an-abstraction. Accessed 10 June 2020;
- Guerreiro, Alexandre, *International Law and the Fight Against Terrorism and Cyberterrorism*. O Direito Internacional e o Uso da Força no Século XXI, AAFDL Editora, 2018;
- Hardesty, Larry. *Study finds gender and skin-type bias in commercial artificial-intelligence systems*. MIT News Office, 11 February 2018, news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212. Accessed 11 June 2020;
- Kayser-Bril, Nicolas. *At least 10 police forces use face recognition in the EU, AlgorithmWatch reveals.* Algorithm Watch, 11 December 2019, algorithmwatch.org/en/story/face-recognition-police-europe. Accessed 12 June 2020;
- Levs, Josh and Schoichet, Catherine E. *Europe furious, 'shocked' by report of U.S. spying*. CNN, 01 July 2013, edition.cnn.com/2013/06/30/world/europe/eu-nsa/index.html. Accessed 09 June 2020;
- MacAskill, Ewen, et al. *GCHQ taps fibre-optic cables for secret access to world's communications.* The Guardian, 21 June 2013, www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. Accessed 09 June 2020;
- Orwell, George. *As I Please.* Tribune, 28 April 1944, orwell.ru/library/articles/As_I_Please/english/eaip_04. Accessed 10 June 2020;
- Oscar, W., et. al. *Defining Civil Defense in the Information Age*. Strategic Forum No. 46, September 1995;

- Pequenino, Karla. *Reconhecimento facial vai ser testado no acesso a serviços públicos online*. Público, 26 January 2020, publico.pt/2020/01/26/tecnologia/noticia/reconhecimento-facial-vai-testado-acesso-servicos-publicos-online-1901622. Accessed 12 June 2020;
- Savage, Charlie. *Congress Approves Six-Year Extension of Surveillance* Law. The New York Times, 18 January 2018, nytimes.com/2018/01/18/us/politics/surveillance-congress-snowden-privacy.html. Accessed 09 June 2020;
- Séneca, Hugo. *Governo avança com reconhecimento facial, apesar de riscos. AMA não revela participantes do concurso*. visao.sapo.pt/exameinformatica/noticias-ei/mercados/2020-01-13-governo-avanca-com-reconhecimento-facial-apesar-de-riscos-ama-nao-revela-participantes-do-concurso. Accessed 14 June 2020;
- Sidiqqui, Sabrina. *Congress passes NSA surveillance reform in vindication for Snowden.* The Guardian, 3 June 2015, theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden. Accessed 09 June 2020;
- Slaughter, Anne-Marie, et. al. *Reflections on the 9/11 Decade*. RUSI Journal, Vol. 156, No. 4 August-September 2011;
- Shaw, Jonathan. *The Watchers, assaults on privacy in America.* The Harvard Magazine, vol. January-February 2017, harvardmag.com/pdf/2017/01-pdfs/0117-56.pdf. Accessed 09 June 2020;
- Trigueirão, Sónia. *Casinos: Turismo de Portugal gastou 338 mil euros mas reconhecimento facial não funciona.* Público, 06 May 2019, publico.pt/2019/05/06/economia/noticia/turismo-gastou-338-mil-euro-reconhecimento-facial-nao-funciona-1871551. Accessed 12 June 2020;
- White, April. *A Brief History of Surveillance in the America*. Smithsonian Magazine, April 2018, smithsonianmag.com/history/brief-history-surveillance-america-180968399. Accessed 09 June 2020;
- Wyden, Ron U.S. Senator. *In Speech, Wyden Says Official Interpretations of Patriot Act Must be Made Public*, Official Press Release, 26 May 2011, wyden.senate.gov/news/press-releases/in-speech-wyden-says-official-interpretations-of-patriot-act-must-be-made-public. Accessed 13 June 2020;

Reports

- Agência para a Modernização Administrativa, IP. *Plano de Atividades 2019.* ama.gov.pt/documents/24077/28687/PA+2019_AMA_20191216_VF.pdf/8c351ce4-4f38-4e10-9245-67e0c3f1353f. Accessed 14 June 2020
- Carnegie Endowment for International Peace: *AI Global Surveillance Index 2019.* carnegieendowment.org/files/AI_Global_Surveillance_Index1.pdf. Accessed 11 June 2020;
- Council of Europe, *Explanatory Report to the Council of Europe Convention on the Prevention of Terrorism*, Council of Europe Treaty Series, *No. 196*, 16 of May 2005;
- ENISA and EUROPOL. *On lawful criminal investigation that respects 21st Century data protection. Europol and ENISA Joint Statement*. enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection. Accessed 11 June 2020;
- Federal Bureau of Investigation. *Crime in the United States by Metropolitan Statistical Area, 2018.* ucr.fbi.gov/crime-in-the-u.s/2018/crime-in-the-u.s.-2018/topic-pages/tables/table-6. Accessed 11 June 2020;
- IHS Markit. *Video surveillance: How technology and the cloud is disrupting the market 2020.* IHS Markit Reports, technology.informa.com/620262/ihs-markit-technology-white-paper-reveals-top-trends-impacting-the-video-surveillance-market-in-2020. Accessed 10 June 2020;
- Immenkamp, Beatrix; Sgueo, Gianluca and Voronova, Sofija. *Briefing: EU Policies – Delivering for Citizens. The fights against Terrorism.* European Parliament Think Tank, 28 June 2019, europarl.europa.eu/RegData/etudes/BRIE/2019/635561/EPRS_BRI(2019)635561_EN.pdf. Accessed 09 June 2020;
- Institute for Economics & Peace. *Global Peace Index 2020: Measuring Peace in a Complex World*. Sydney, June 2020, visionofhumanity.org/app/uploads/2020/06/GPI_2020_web.pdf, p.8. Accessed 13 June 2020;
- Krueckeberg, Jennifer et al. *Face Off, the lawless growth of face recognition in the UK policing.* Big Brother Watch, May 2018, bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf,. Accessed 12 June 2020;
- White Paper of 12 February 2020 from the European Commission on Artificial Intelligence – A European approach to excellence and trust [COM(2020) 65 final];

Websites

- Agência para a Modernização Administrativa, IP. *O que é a chave-móvel. autenticacao*.gov.pt/a-chave-movel-digital. Accessed 14 June 2020;
- City of Detroit, Police Department official website. *Project Green Light Detroit.* detroitmi.gov/departments/police-department/project-green-light-detroit#block-views-block-featured-unified-block-1. Accessed 11 June 2020;
- City of Detroit, Police Department official website. *Project Green Light Detroit Map.* detroitmi.gov/webapp/project-green-light-map. Accessed 11 June 2020;
- Our World in Data, *Multiple Datasets.* ourworldindata.org/democracy. Accessed 07 June 2020;
- Neighborhood Scout. *Detroit, MI Crime Rates.* neighborhoodscout.com/mi/detroit/crime. Accessed 13 June 2020;
- V-Dem Dataset version 9, *Cybersecurity Capacities Index*, www.v-dem.net/en/data/data-version-9. Accessed 09 June 2020;

Legislation

- Comissão Nacional de Proteção de Dados, Parecer/2019/92, Processo PAR/2019/61;
- Comissão Nacional de Proteção de Dados, Parecer/2019/93, Processo PAR/2019/62;
- Concurso Público N.º 235/19/DCP/GACD/Software de Reconhecimento Facial e Deteção de Vida. *in* Diário da República, Anúncio de procedimento n.º 13672/2019, Série II de 2019-12-10;
- Council of Europe Convention on the Prevention of Terrorism (2005), CETS No. 196, entered into force 01 June 2007;
- Council of the European Union Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA), OJ L 164 (22 June 2002), p. 3-7, with the following amendments: Council of the European Union Framework Decision 2008/919/JHA and

replaced by Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017;

- Diário da República, *Decreto de Aprovação da Constituição*, n.º 86/1976, Série I de 1976-04-10;
- Directive 2016/680/EU 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 199 (4 May 2016);
- Regulation 2016/679/EU of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 199 (4 May 2016);
- The North Atlantic Treaty (1949), 34 UNTS 243, entered into force 24 August 1949;
- United Nations Security Council Resolution (UNSCR) 1368 (2001), "Condemning the terrorist attacks of 11 September 2001 in New York, Washington, D.C. and Pennsylvania, United States of America", UN Doc. S/RES/1368, adopted on 12 September 2001;
- United Nations Security Council Resolution (UNSCR) 1373 (2001), "On threats to international peace and security caused by terrorist acts", UN Doc. S/RES/1373, adopted on 28 September 2001;
- U.S. House. 107th Congress. 1st Sess. H.R. 3162, *The USA Patriot Act: Preserving Life and Liberty: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*. Version 1, Oct. 23, 2001;
- U.S. Department of Justice. *The USA PATRIOT Act: Preserving Life and Liberty* justice.gov/archive/ll/what_is_the_patriot_act.pdf. Accessed 09 June 2020;
- Working Party for Article 29 of Directive 95/46/EC. *Opinion 3/2012 on developments in biometric technologies*. Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf. Accessed 13 June 2020.

CYBERLAW
by CIJIC

DO INTRÓITO À "ENGENHARIA DO DIREITO PENAL SOBRE RODAS" AO AGENTE INTELIGENTE AUTOMÓVEL QUE NÃO (VA'I') À LUZ DO ATUAL DESARRANJO TERMINOLÓGICO

FROM THE "ENGINEERING OF CRIMINAL LAW ON WHEELS" TO INTELLIGENT AGENT AUTOMOBILE (IA-A) WHO DOES NOT ('GO') IN LIGHT TO THE CURRENT TERMINOLOGICAL DERANGEMENT

CESAR ANALIDE *

DIOGO MORGADO REBELO **

* Professor Auxiliar da Escola de Engenharia da Universidade do Minho e Investigador Doutorado em Inteligência Artificial no Laboratório de Inteligência Sintética (ISLab), Centro de Investigação ALGORITMI do Departamento de Informática da Universidade do Minho– http://algoritmi.uminho.pt/research-teams/islab/.

** Mestrando do Curso de Direito e Informática da Escola de Direito da Universidade do Minho. Jurista licenciado pela Faculdade de Direito da Universidade Nova de Lisboa em 2017.

RESUMO

Em matérias de responsabilidade (penal) da circulação verdadeiramente inteligente, o direito ainda não é *prius*, nem *posterius*, não é dado, nem solução, não está no princípio, nem no fim. Desde logo, indaga-se ser inacabada a terminologia que radica a classificação dos Veículos Inteligentes nos 5 níveis de autonomia estabelecidos pela *Society of Automotive Engineers* (SAE) e pela Organização para a Cooperação e Desenvolvimento Económico (OECE). Nesse sentido, o encargo dos signos aprendizagem, raciocínio e interação idónea com o ambiente estradal ponteia primordialmente a manifestação da aptitude que um Agente Inteligente Automóveis (AI-A) manifesta em representar o conhecimento adaptativo dele sobrevindo. Este processo, no seu *corpus*, assume-se também preponderante na operação de condução evolutiva da robótica, enquanto reduto ou pedra basilar da maior proficiência adaptativa nas operações plúrimas e concomitantes de decisão totalmente independentes. Todavia, isto *per si* não faz da autonomia a *key feature* pela qual os veículos automóveis com traços de alguma aprendizagem e reatividade mereçam ser integrados na categoria de AI-A. Antes, estes últimos serão ajuntados numa nova que aqui propomos, a de Veículos Automóveis Quase-inteligentes (VA'I').

Portanto, no atual estado da arte, dir-se-á ser inteligente todo o agente automóvel que se encontra munido de Sistemas Avançados de Assistência ao Condutor (ADAS, *Advanced Driver Assistance Systems*), cujo software processa autonomamente e em tempo real os *outcome(s) algorítmico(s)* que das combinações *deep learning* se extraem, viabilizando a circulação dinâmica, defensiva e antecipatória do automóvel em situações críticas de segurança, prescindindo também da assunção plena de controlo ou direção efetiva por quem deverá ora assumir o *status* de simples ocupante ou passageiro.

E se, por um lado, não é surpreendente que as iniciativas legislativas sobre esta matéria sucedam num motejo tímido, fragmentário e compartimentado, em correspetiva, as novas tecnologias e a inteligência sintética constituem um *tópos* a que o Direito (e, particularmente, o Direito

Penal) não podem nem devem olvidar. Assim, na conjuntura operante de um determinado AI-A, existindo uma afetação de bens jurídicos essenciais dotados de referente constitucional, designadamente defronte casuísticas inopinadas não subsumíveis ao 'Quem' dos tipos de crime homicídio (por negligência) ou ofensa à integridade física, afigura-se hoje existir uma incompletude de pendor lacunoso de terceiro nível. É que o ato sentencioso que apresenta os AI-A por de entre a ciência punitiva não pode, não deve, nem tem de se circunscrever ao sigma consciência humana, e tão-pouco perecerá diante a moralidade distributiva das operações, *máxime*, por referência aos ultrapassados contornos antropopáticos por que são conotados. Connosco, o Direito Penal do Século XXI ficará ancorado na operação escolhida e projetada objetivamente em probabilidades difusas das entidades virtuais, os Agentes de Software.

Engane-se quem julga abispar solucionar um problema sem previamente fundamentar a sua orientação em heurísticas que engendram saberes polímatos. Assim, procurando olhar a 'Engenharia do Direito' de mais sítios e de sítios mais improváveis do que se tornou habitual, vislumbramos tanger o sonho do dia em que, de *jure condendo*, dos bancos da faculdade os estudantes escutarão a *poiesis* que proclama não ser Direito - e muito menos Direito Penal -, todo o conjunto de 'instruções algorítmico-normativas' que, embora expressando a vontade da maioria, implicam também o revés da negação do novo 'Quem' como Agente de Software Inteligente, *in casu*, com feição ciberfísica de veículo automóvel criminoso.

Palavras-Chave: Agente Inteligente Automóvel; Direito Penal; Engenharia do Direito; Veículos Automóveis Quase-inteligentes.

ABSTRACT

In matters of (criminal) liability of truly intelligent self-driving, the law is not yet *prius*, nor *posterius*, it is not given, nor the solution, it is not in the beginning, nor in the end. The terminology used to classify Intelligent Vehicles within the 5 levels of autonomy established by the Society of Automotive Engineers (SAE) and the Organisation for Economic Co-operation and Development (OECE) is imperfect. In this sense, the burden of the signs learning, reasoning and interaction with the driving environment bridges primarily the manifestation of the aptitude that the intelligent automotive agents (IA-A) urge in representing the adaptive knowledge coming from it. This process, in its *corpus*, is also important in the evolved operations of robotics, as a stronghold or cornerstone of the greater adaptive proficiency in the plural and simultaneous operations of a completely independent decision. However, this does not make autonomy the key feature by which a vehicle with attributes of some self-learning and reactivity deserve to be integrated into the IA-A category. Rather, the latter will be brought together in a new one that we propose in this paper, that of Quasi-Intelligent Vehicles ('I'V).

Therefore, in the current state of the art, it will be considered as intelligent any automobile agent that is equipped with Advanced Driver Assistance Systems (ADAS), whose software processes autonomously and in real-time the algorithmic outcome(s) exhorted from deep learning combinations, thus, enabling a dynamic, a defensive and an anticipatory circulation of the self-driving car in critical safety situations and, finally, that foregoes the full assumption of control or effective steering by those who should now assume the status of a simple occupant or passenger.

And if, on the one hand, it is not surprising that legislative initiatives in this regard follow on from a timid and fragmentary motto, in co-respect, the new technologies and synthetic intelligence constitute a *topoi* to which the law (and particularly, the criminal law) cannot and must not forget. Particularly, in the operating spectrum of a given AI-A, if there is an unlawful intrusion of

constitutional values, namely in front of unexpected casuistry not subsumable to the 'Who' of the types of crime homicide (by negligence) or offense to physical integrity, it seems today to exist an incompleteness of legal loophole of third level. Today, the sententious act that presents IA-A among punitive science cannot or must not be limited to the sigma of human consciousness, nor will it perish before the distributive morality of operations, *maxime*, by reference to the outdated anthropopathic contours by which they are known. With us, the Criminal Law of the 21st Century will be anchored in a chosen operation, objectively projected in the fuzzy probabilities of virtual entities, like Software Agents.

It is a misunderstanding to think that a problem can be solved without first grounding its orientation on heuristics that generate multidisciplinary knowledge. Therefore, looking for the 'Engineering of Law' from more places than usual, we foresee the dream of the day in which, de *jure condendo*, from the college seats the students will listen to the *poiesis* that proclaims not to be law - and much less criminal law - the whole set of 'algorithmic-normative instructions' which, while expressing the will of the majority, also implies the negation of the new 'Who' as an Intelligent Software Agent, *in casu*, with the cyberphysical appearance of a criminal motor vehicle.

Keywords: Criminal Law; Intelligent Agent Automobile; Law Engineering; Quasi-Intelligent Vehicles.

1. PROLEGÓMENOS DE UM NOVO DIREITO (PENAL) PARA O SÉCULO XXI: EM ESPECIAL, O CASO DOS AGENTES INTELIGENTES AUTOMÓVEIS (AI-A)

Progredimos hoje para uma democratização urbana concernente à evolução da Circulação XXI que perfilha a indústria automóvel na interação constante entre agentes inteligentes automóveis e o meio circundante. À falta de alma, um grande número de veículos 'nutrirá' inteligência própria, a dos agentes de software, *in casu*, também com configuração de viaturas dotadas de motor de propulsão, de quatro rodas, de sistemas mecatrónicos e eletromecânicos avançados que auxiliam o cérebro sintético [1] do automóvel a percecionar toda a informação sensorial, a planear e a controlar os vários cursos de operação e, *inclusive*, em situações críticas de segurança (sublinhado, a propósito de enaltecer o qualificativo). Estes mesmos veículos encontrar-se-ão munidos da capacidade de executarem decisões típicas de circulação em ambiente dinâmicos, com aspeito antecipatório e defensivo, aliás, também prescindindo na plenitude do quesito de controlo ou direção efetiva por parte daqueles que deverão passar ora a assumir tão-só o *status* de passageiros.

De facto, a revolução tecnológica no setor automóvel surtirá benefícios que se irão repercutir e incrementar ao longo de vários anos. Desde logo, haverá que louvar a "inclusão de cidadãos impossibilitados de conduzir, por limitações de ordem física ou de outra natureza" [2]. Além disso, proporcionar-se-ão "novas e diferentes soluções de mobilidade individual e coletiva, contribuindo para a otimização do parque automóvel e para a redução de deseconomias inerentes ao atual paradigma de mobilidade assente no veículo de propriedade" (sublinhado, nosso) [3]. Ora, é indubitável que os veículos autónomos "irão alterar significativamente a vida quotidiana dos cidadãos, determinar o futuro do transporte rodoviário a nível mundial, reduzir os custos do transporte,

1 Mais uma vez, reitera-se que a Ciência ou Engenharia em voga deve lograr o não tão vulgarizado predicativo 'sintético' em substituição da notação mais comum ou comercial, i.e., o predicativo artificial. É que as atuais demonstrações científicas verificadas denotam ainda pouca semelhança com os processos mentais dos seres humanos. Nesse sentido, cf. J. Haugeland, *Artificial Intelligence: The Very Idea*, The MIT Press, Cambridge, MA, 1985, 255; e J. R. Searle, *Minds, Brains and Science*, Harvard University Press, Cambridge, MA, 1984, 31-34.
2 Cit. Preâmbulo do Despacho n.º 2930/2019, Diário da República n.º 55/2019, Série II de 2019-03-19.
3 Cit. ... *ibidem.*

melhorar a segurança rodoviária, aumentar a mobilidade e reduzir os impactos ambientais" [4]. Estima-se que "os elementos de segurança (...) dos veículos inteligentes desempenhem um papel importante na redução do número de colisões e vítimas mortais (...) uma vez que estas ainda podem ocorrer, especialmente durante uma fase intermédia de tráfego misto" (sublinhados, em ajuste, nosso) [5]. Não obstante, se se reconhece internamente como determinante "a realização de testes de avaliação da maturidade e adequação das soluções, sendo necessário ajustar a legislação às novas realidades" [6], colocam-se os seguintes interregnos: (1) Porque é que os juristas teóricos haverão de começar por engenhar construir a 'casa' da imputação de responsabilidades a partir do 'telhado'? (2) Será a autonomia o reduto uno que viabiliza diferenciar os veículos nestas novas modalidades de condução? (3) Quem será o responsável, a título jurídico-penal, diante casuísticas inopinadas que constituam uma afetação de bens jurídicos com rango *norma normarum* e, além disso, por força das propriedades que os veículos exteriorizam e dos circunstancialismos fáticos adjacentes, se considere ser insuscetível imputar sanções com caraterísticas de Direito Penal à pessoa do fabricante, programador do software (sendo o caso de *outsourcing*) e, também, claro está, ao próprio passageiro do veículo?

São estas e outras as questões que nos propomos responder ao longo de vários escritos nesta matéria. Assim, sem mais delongas, apresentamos o presente ensaio resumidamente em contornos camonianos [7]:

Os veículos e a sua inteligência assinalada,
Que das rodovias Lusitanas,
Por estradas tecnológicas nunca dantes circuladas,
Viajam além da autonomia mundana,
Em propriedades aprendidas,
Raciocinam mais rápido do que a mente humana,
Hoje os agentes de software edificam,
Um Novo Direito (Penal) que só deles promana.

4 Cf. Resolução do Parlamento Europeu, de 15 de janeiro de 2019, sobre a condução autónoma nos transportes europeus (2018/2089(INI)), Alínea B.
5 Cf. Resolução do Parlamento Europeu, de 15 de janeiro de 2019, ... *supra*, Ponto 40.
6 Cit. ... *ibidem*.
7 Cf. L. V. de Camões, *Os Lusíadas de Luís de Camões*, 4.ª ed., Instituto Camões, Ministérios dos Negócios Estrangeiros, 200, Canto I, Estrofe 1, 1 (com as devidas adaptações).

Dir-se-á então que o mote principiológico do presente ensaio será o de o perspetivar os Veículos Inteligentes Automóveis como forças inevitáveis, fazendo uso dos benefícios que a sua utilização pode ter sobre o ambiente rodoviário. Os transeuntes humanos e animais, os ciclistas, bem como quem dirige transportes vários, carecem de se adaptar a uma circulação nova, que se pretende mais cómoda, mais segura e mais eficiente.

Assim, crê-se que se deva começar por balizar tecnicamente conceitos funcionais, pelejando também a jusante pela institucionalização de um novo Direito Penal dos (e não só para os) Agentes Inteligentes Automóveis, estes que amparamos vir a ser os novos 'Quem' destinatários das normas punitivas. Porque - seguindo a linha de pensamento do memorável Professor Doutor Diogo Freitas do Amaral, aquele dos poucos 'quem ser pensante' ciente do seu papel social, que julgara a engenharia enquanto fonte *juris cognoscendi* -, "se uma norma jurídica de conteúdo técnico só pode ser entendida e 'decifrada' por intermédio do contributo decisivo de uma certa ciência, esta torna-se um meio necessário de conhecimento do Direito, e não apenas da sua aplicação" [8].

Em particular, pugnados que, para serem deliberadas, aprovadas e promulgadas leis conotadas pela correção técnico-científica dos seus enunciados gerais e abstratos - aqueles que traçam o caminho-meio do hiato material que vai dos conceitos ao estabelecimento dos deveres de cuidado, e destes, subsequentemente, à resolução do enigma imputação de responsabilidades na circulação inteligente -, conclui-se ser imperativo o recurso à Informática Teórica. Porque também esta ajudará a revelar o Direito e não somente a aplicá-lo.

8 Cit. D. Freitas do Amaral, *Manual de Introdução ao Direito*, vol. I/col. Ravi Afonso Pereira, Almedina, Coimbra, 2012, 559.D. Freitas do Amaral, op. cit., 558.

2. DO PENDOR AUTONÓMICO SUBORDINADO EM APONTAMENTOS CONVENCIONAIS À NOTAÇÃO APRIMORADA AGENTE INTELIGENTE AUTOMÓVEL INTELIGENTE: O AI-A

São, desde logo, algumas as considerações técnico-científicas que importa começar por tecer relativamente a uma conceptualização aprimorada daquele que cremos *dever-ser* o entendimento *jus essendi* conducente à necessária e justificada adoção da nomenclatura Agente Inteligente Automóvel (de ora em diante, abreviadamente, AI-A). O mote principiológico do presente ensaio será então o de pelejar *ab ovo* por um necessário metamorfosear terminológico, de matriz legiferante, ajuizada e designadamente em alusão ao 'desvio-padrão' que denota a aceção imprecisa e comumente propugnada acerca da tipologia de agente em estudo, *rectius*, o comummente intitulado Veículo Autónomo.

Destarte, na atual *leges artis* do setor, dir-se-á ser inteligente todo o agente automóvel – então investido na posição de veículo com motor de propulsão, dotado de pelo menos quatro rodas, que se destina à mobilidade familiar, coletiva ou comercial de pessoas, bens, animais ou mercadorias – que se encontra munido de Sistemas Avançados de Assistência ao Condutor (ADAS, *Advanced Driver Assistance Systems*) habilitantes dos seus elevados níveis de aprendizagem, raciocínio e interação dinâmica nas operações de perceção, planeamento e controlo decisórios em ambiente estradal (v., breves considerações, *infra*). Por conseguinte, estes mecanismos robóticos avançados – os quais incorporam e são configurados no conspecto mecatrónico e eletromecânico de equipamentos ciberfísicos e software - são suplantados *by design* no sistema pelo programador ou fabricante do veículo. E porque processam autonomamente e em tempo real os *outcome(s)* algorítmico(s) que das combinações *deep learning* se extraem, viabilizam a circulação dinâmica, defensiva e antecipatória do automóvel em situações críticas de segurança (i.e., de direção, aceleração ou travagens em eventos de *problem-solving*), prescindindo também concomitantemente da assunção plena de controlo ou direção efetiva por quem deverá ora assumir o *status* de passageiro, excetuando aquelas situações em os próprios veículos antecipam não conseguirem minorar os danos emergentes de uma possível colisão (v. desenvoltura, *infra*) [9].

9 Cf. com algumas adaptações, J. A. Brett, *Thinking local about self-driving cars: A local framework for autonomous vehicle development in the United States*, Tese de Mestrado, Universidade de Washington, Seattle, Washington, 2016, 27-29, https://digital.lib.washington.edu/researchworks/handle/1773/36852.

Da definição explanada, *supra*, proclama-se ser inacabada a terminologia que radica a classificação dos AI-A nos 5 níveis de autonomia estabelecidos pela *Society of Automotive Engineers (SAE)* [10] e pela Organização para a Cooperação e Desenvolvimento Económico (OECE) [11]. Sucede que, de entre os atributivos que possam ser consignados à operação AI-A, a autonomia posiciona-se como consequente dos postulados representação do conhecimento, aprendizagem e mecanização do raciocínio, *qua tale* operantes no conspecto dos signos armazenamento dos dados e atualização destes em tempo real no e pelo sistema programático [12]. Estes traços, *in totum*, reconduzir-se-ão à utilidade augurada e concretizável numa mobilidade mais segura e verdadeiramente independente, dada a inteligência sopesada nas operações de perceção, planeamento e controlo das decisões (v. breves considerações, *infra*). Por conseguinte, quando complementadas, todas estas três caraterísticas balizarão essencialmente a operação de um agente inteligente sintético, i.e., aquele sistema ou *software* em sentido amplo que controla os estados internos e possui uma determinada visão do ambiente estradal, pautando a interação idónea com o universo de discurso circundante – de matriz inacessível, não determinística, não episódica e dinâmica [13] - através da redefinição permanente de estratégias e, aliás, no ímpeto de consecução da multiplicidade de *targets* (por vezes simultâneos), sem qualquer intervenção humana[14].

10 Cf. SAE, *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*, SAE J3016, 2014, 2, https://www.sae.org/standards/content/j3016_201401/preview/, e, também nesse sentido, B. W. Smith, SAE levels of driving automation, *in Center for Internet and Society*, Stanford Law School, http://cyberlaw.stanford.edu/blog/2013/12/sae-levels-driving-automation.

11 Cf. International Transport Forum, *Automated and Autonomous Driving: regulation under uncertainty*, OECE, 2018, 14, https://www.itf-oecd.org/sites/default/files/docs/15cpb_autonomousdriving.pdf.

12 Num prisma técnico, o agente verdadeiramente autónomo deve exteriorizar esquemas de racionalidade própria, mas também "ter ainda a capacidade de aprendizagem e de aquisição de conhecimento (...) . E é com base nesse conhecimento adquirido e armazenado que o agente atua a sua racionalidade, e.g., efetua operações de verdadeiro raciocínio", cit. F. Pacheco de Andrade, *Da contratação eletrónica – em particular, da contratação eletrónica inter-sistémica inteligente*, Tese de Doutoramento, Universidade do Minho, Braga 2008, 170-171, http://hdl.handle.net/1822/10175.

13 E. Costa e A. Simões, *Inteligência Artificial – Fundamentos e Aplicações*, 2.ª ed., revista e aumentada, FCA, Lisboa, 2008, 30-31.

14 Cf. N. Chakraborty e R. S. Patel, Intelligent Agents and Autonomous Cars: A Case Study, *in Internatinal Journal of Engineering Research & Technology* (IJERT), Vol. 2 (1), 2013, 1-2; e S. Russel e P. Norvig, Artificial Intelligence: a modern approach, 3.ª ed., Prentice Hall, Edinburgh Gate, 2010, 34; e, *vide*, para mais desenvolvimentos.

2.1. Veículos Automóveis 'Inteligentes' (Va'I') E A Etiqueta De Objetos No Horizonte Dos Agentes De Software

Ora, a consideração de uma entidade virtual - ou também, *in casu*, o dos carros independentes, de feição ciberfísica - na qualidade de agente inteligente difere da notação objetos, não somente em razão da maior autonomia de que os primeiros dispõem, mas também em função dos centros de controlo decisórios que integram. Demais, não obstante poder ao propósito ser convolável a habilidade que os objetos possuem quanto ao armazenamento e disponibilização de estados internos, bem como quanto ao fluxo elevado concernente ao intercâmbio de *bits* de informação, certo é que estes não dispõem do legado planeamento e controlabilidade das **ações** (negrito nosso, propositado) [15].

"Objects do it for free; agents do it because they want to"[16].

Nessora, defronte uma situação de segurança crítica - na qual tanto os VA'I' ou os AI-A haverão de primar pela minimização dos danos, os primeiros, os VA'I', diferirão dos segundos. Poder-se-á afirmar que os objetos VA'I' computam no sistema a capacidade de representar o meio circundante (*Knowledge Representation*) [17] sob fórmulas de mecanização do raciocínio lógico (*Internal Knowledge*), e fazem-no relativamente à precisão dos dados recolhidos e posteriormente armazenados no universo de discurso (*External Knowledge*) [18]. Todavia, não só se eximem de planear, como nem sequer antecipam ou controlam as possíveis ações de resposta em situações críticas de segurança. Aliás, o desempenho específico do modo de condução em todos os aspetos dinâmicos é efetuado na expectativa de que o condutor humano assuma o controlo e responda adequadamente a um pedido para intervir. Embora se possa considerar que os Veículos com um nível de automação 3 possibilitam ao condutor humano ceder o processo decisório ao objeto mesmo em situações críticas de segurança – defronte determinadas condições de tráfego ou ambientais, refira-se -, em correspetiva requererão sempre a atenção deste, porquanto a qualquer instante pode ser avocada a

15 Cf. M. Wooldridge, *An Introduction to MultiAgent Systems,* John Wiley & Sons, 2002, 25-27.
16 Cit. ... *idem,* 26.
17 Cf. C. Analide, P. Novais, J. Machado e J. Neves, Quality of knowledge in virtual entities, in *Encyclopedia of communities of practice in information and knowledge management*, IGI Global, Hershey, Pennsylvania, 2006, 436-442,https://doi.org/10.4018/978-1-59904-933-5.ch016.
18 Cf. R. C. Schank, What is Artificial intelligence, anyway?, *in* The Foundations of Artificial Intelligence, 3.ª ed/coord. Derek Partridge e Yorick Wilks, 2006, cit. in., G. Hallevy, Liability for crimes involving Artificial Intelligence systems, *in* Springer, Cham Heidelberg, 2015, 9-10.

assunção de controlo ou direção efetiva. Assim, espera-se sempre que o condutor esteja disponível para um controlo ocasional, nem sempre com um tempo de transição suficientemente confortável. Acrescenta-se aqui também que a principal distinção entre os hétero proclamados níveis 2 e o nível 3 de autonomia, i.e., entre os objetos *stricto sensu* e os VA'I', reside no facto de neste último o veículo ser concebido de modo a não se esperar que o condutor monitorize constantemente a estrada enquanto conduz, embora esse continue a ser um dos seus desígnios, caso em que o veículo deverá de ser considerado tão-só quase-inteligente [19].

E se, por um lado – inclusivamente num perspetivar técnico -, só será reputada como autónoma aquela entidade, ou antes, aquele agente de software que opera "sem a intervenção de outros agentes (como os condutores humanos, por exemplo) e tem controlo sobre as suas ações e o seu estado de conhecimento interno" (sublinhado, em acrescento, nosso) [20], por outro, circunscrever a classificação de veículos inteligentes à sua autonomia seria tão só redundar um conceito geral e abstrato em aporias desnecessárias para o Direito. Assim não sucedendo, reconhecer-se-ia como razoável considerar que tanto o hétero proclamado nível de autonomia 3, como os níveis 4 e 5, respetivamente, exteriorizariam a "possibilidade de uma atuação independente, capaz de produzir efeitos jurídicos" [21]. O efeito prestável de definições legais como aquelas que têm vindo a ser pelejadas – embora ainda não consagradas no ordenamento jurídico português - seria nulo, não sendo possível destrinçar convenientemente os pressupostos de imputação das responsabilidades civil e penal numa fase posterior, cumulativamente, em relação ao Direito dos Agentes de Software [22].

Portanto, sugerimos posicionar estes objetos automóveis quase-inteligentes na semiótica da classe agentes inteligentes em interação com o mundo (*agents keeping track of the world*) [23], aqueles que atualizam a informação de que dispõem acerca do seu estado interno, reagindo a título de assistência e somente a determinados tipos de estímulos nas operações de:

19 Cf. SAE, *Taxonomy and Definitions for Terms Related to On-Road … supra,* 2.
20 Cit. P. Novais, *Teoria dos Processos de Pré-Negociação em Ambientes de Comércio Eletrónico,* Tese de Doutoramento, Universidade do Minho, Braga, 2003, 57.
21 Cf. F. Pacheco de Andrade, *Da contratação eletrónica inter-sistémica ... supra,* 170.
22 Cf. B. Schermer, M. Durinck, L. Bijmans, Juridische aspecten van autonome systemen, *in ECP.NL*, 2005, 14, http://www.ejure.nl/mode=display/downloads/dossier_id=156/id=251/Juridische_aspecten.pdf.
23 Cf. N. Chakraborty e R. S. Patel, Intelligent Agents and Autonomous Cars: … *supra*, 3.

– travagem de emergência automática limitada (*Automatic Emergency Braking*);

– assistência de estacionamento (*Angled Parking Assist*);

– assistência na manutenção em pista (*Lane Keeping Assistance)*;

– *cruise control* adaptativo (ACC- *Adaptive Cruise Control*);

– controlo eletrónico de estabilidade (ESC – *Electronic Stability Control*);

– sistema de controlo de tração (TCA – *Traction Control System*); e

– sistema anti-bloqueio de travagem (ABS- *Anti Lock Braking System*) [24].

Avalia-se então, em conformidade com o antedito, predicar estes objetos automóveis na sua quase-inteligência, pois que, em situações daquilo a que se convenciona ser o GPS (*General Problem-Solving*) da IA, o veículo representa o conhecimento que carateriza o meio circunjacente, mas fá-lo sem planear novas e possíveis ações de resposta, não se encontrando imbuído num processo de aprendizagem suficientemente inteligente nessa medida. Em jargão corriqueiro, o funcionamento destes objetos não é desembaraçado. Não evidencia qualquer controlo de muitas situações dinâmicas e requer sempre a atenção do sujeito com a incumbência jurídico-assumptiva de dirigir o veículo, caso em que o nível de automação é tão-só assistido [25].

Assim, neste que é o estado do marketing na indústria automóvel inteligente, uma ação de simples ultrapassagem será demarcada pela circunstância do veículo identificar com margens de erro não satisfatórias um outro que circula em sentido contrário, e não equacionar sequer a possibilidade de conseguir transpor o automóvel sem o embate, requerendo prontamente a intervenção do condutor humano. Defronte a passagem de um transeunte humano ou animal na passadeira, identificá-lo-á e acionará porventura a única operação de resposta tempestivamente, embora somente em razão dos mecanismos de aprendizagem a que haja sido submetido previamente. Todavia, este baluarte não faz do VA'I' por certo o 'Hércules' da condução automóvel.

Dir-se-á então que, neste setor em especial, o encargo dos signos aprendizagem, raciocínio e interação idónea com o ambiente estradal ponteiam principiológica e primordialmente a exteriorização da aptidão que os AI-A manifestam em representar o

24 Cf. A. J. Moreira Lousa, *Veículos Autónomos e Conetados – Tecnologia e Identificação de Possíveis Alterações na Infraestrutura de Transporte*, Dissertação de Mestrado, Universidade de Coimbra, 2018, 19, https://eg.uc.pt/bitstream/10316/84931/1/VEÍCULOS%20AUTÓNOMOS%20E%20CONETADOS%20-%20TECNOLOGIA%20E%20IDENTIFICAÇÃO%20DE%20POSSÍVEIS%20ALTERAÇÕES%20NA%20INFRAESTRUTURA%20DE%20TRANSPORTE.pdf.

25 Cf. SAE, *Taxonomy and Definitions for Terms Related to On-Road … supra,* 2.

conhecimento adaptativo dele sobrevindo. Este processo assume-se também preponderante na operação de condução independente, enquanto reduto ou pedra basilar da maior proficiência adaptativa nas operações de planeamento e controlo decisório, mas isto *per si* não faz da autonomia a *key feature* pela qual os veículos automóveis com traços de alguma aprendizagem e reatividade mereçam ser integrados na categoria de AI-A.

Portanto, estas razões são simultaneamente o *ipso facto* e a *ratio* do AI-A (o *self-driving car sapiens*) não 'ir' - em nosso perspetivar -, à luz do atual desarranjo terminológico, o de veículos autónomos que são tão-só quase-inteligentes. É que não se pode circunscrever diferencialmente objetos de agentes fortes ou fracos automóveis somente de encontro com o atributo autonomia, este que é o consequente lógico das várias propriedades e das várias caraterísticas que aos veículos verdadeiramente inteligentes podem ser 'ensinadas' (v. desenvolvimento, *infra*). Deixa-se, neste seguimento, o seguinte repto:

- É este, afinal, o objeto que ambicionamos denominar veículo autónomo?

2.2. Agentes Inteligentes Automóveis (Ai-A) E A Sua Proeminente Inteligência

Latu sensu, são muitos os sinais distintivos primários que assentem diferenciar com precisão e rigor técnico-científico os veículos automóveis quase-inteligentes - então entendidos na qualidade de objetos, os VA'I' -, dos agentes automóveis inteligentes (AI-A) e, quanto a estes últimos, balizá-los nas suas categorias forte e fraca, respetivamente. Ainda a respeito da bipartição primeira – aquela que distingue os VA'I' dos AI-A - dir-se-á que serão *inclusos* nesta última categoria as entidades automóveis em relação às quais se verificam as seguintes características 'capitais', cumulativamente, como sejam:

(1) a autonomia, porquanto inteligível se concebe a um agente automóvel a capacidade de tomar decisões prescindindo da interface material para com o utilizador final, sendo independente nesse sentido [26]–[27]. A autonomia dos veículos evidencia a

26 Cf. P. M. Freitas, F. Pacheco de Andrade e P. Novais, Criminal Liability of Autonomous Agents: From the Unthinkable to the Plausible, *in AI Approaches to the Complexity of Legal Systems*, Casanovas P., Pagallo U., Palmirani M., Sartor G. (eds.), AICOL 2013, Lecture Notes in Computer Science, vol 8929. Springer, Berlin, Heidelberg, 2014, 146.

27 E não se alvitre, quanto à propriedade autonomia, justapor as técnicas da IA centrada no ser humano (AI *Human-centered*) – que têm vindo a ser aplicadas em veículos automóveis quase-inteligentes, curiosamente, *supra* - em relação às categorias que se convencionara atribuir o intervalo dos níveis [1-5].

tomada de decisões *data-driven*, na medida em que as componentes mecânicas dos agentes recolhem e armazenam os dados à escala *big data* (i.e., perceção via *hardware*) e, subsequentemente, o cérebro sintético aprendiz processá-los-á como preditores em processos de decisão plúrimos, simultâneos e autónomos;

(2) a reatividade, caso em que o agente automóvel encontrar-se-á capacitado a responder apropriadamente defronte circunstâncias prevalecentes em ambientes dinâmicos e imprevisíveis. Aqui, a iteração estímulo-resposta viabiliza executar operações comunicacionais mais complexas no caso dos agentes inteligentes;

(3) a proatividade e a aprendizagem, contanto hábil se conotará o agente na operação de antecipação de metas futuras, por referência a experiências passadas, apresentando a jusante a incumbência de engendrar ulterior e automatizadamente o modo de consecução útil de targets (pré)-determinados (*goal & utility based agents*), i.e., os vários cursos de ação possíveis, antecipando de igual modo os comportamentos vindouros de outrem, sejam agentes similares, VA'I', veículos mais rudimentares, transeuntes humanos, animais ou ciclistas;

(4) a comunicação, a cooperação e a sociabilidade, entendida que seja no desígnio de interação idónea com pessoas, objetos corpóreos ou animais imiscuídos nas áreas circundantes em que o agente circula;

(5) o raciocínio, o comportamento sintético adaptativo em diferentes ambientes;

(6) a colaboração, contanto podem integrar no funcionamento do programa tanto Sistemas Periciais (*Expert Systems*) [28] como Sistemas de Suporte à Decisão (*Decision Support Systems*) [29], esboçando uma atmosfera de sinergia propicia a

---

Tal sucede, na medida em que o propósito concernente à implementação destas *inside vehicle* reporta precisamente às situações em que se reitera a exigência na assunção de controlo ou direção efetiva na pessoa do condutor. Aliás, o Modelo 3 Tesla nas quais estas têm vindo a ser desenvolvidas, na sua habilidade não agente inteligente automóvel, induz a essa mesma consideração. Cf. L. Fridman, Human-Centered Autonomous Vehicle Systems: principles of effective shared autonomy, *in Human-Centered AI & Autonomous Vehicles*, MIT, arXiv preprint arXiv:1810.01835, 2018, https://arxiv.org/pdf/1810.01835.pdf.

28 Os *Expert Systems* representam sistemas de computação avançada com o propósito de mimetizar o processo de tomada de decisão tal qual ele se tem por cognoscível nas atuais demonstrações científicas. Com o propósito de contribuir para uma maior eficiência na resolução de problemas num determinado domínio do conhecimento, estes sistemas representam computacionalmente o meio ambiente envolvente ou o universo do discurso que intentam reproduzir mecanicamente através de *if-then rules*. Contudo, não manipulam diretamente o objeto de incidência nem tangem no imediato o resultado das suas ações. Cf. P. Jackson, *Introduction To Expert Systems*, 3.ª ed., Addison Wesley, 1998, 2.

29 Os Sistemas de Apoio à Decisão (DSS) auxiliam no solucionar de problemas não estruturados ou semiestruturados, instáveis e difíceis de antecipar nesse sentido. Cf. M. Yasmina Santos e I. Ramos, *Business Intelligence: da Informação ao Conhecimento*, FCA – Editora de Informática, Lisboa, 2017, 78-79.

solucionar problemas que apresentam uma estrutura inerentemente distribuída (*Inherent Distributed structure*); e por último,

(7) a interface reduzida ao essencial para com o utilizador-final no curso das operações, ou seja, no sentido de notificar os passageiros tão-só acerca da ocorrência de eventuais intrusões ilegítimas ou falhas mecânicas [30].

Algumas considerações críticas serão ora tecidas relativamente à nomenclatura empregue por referência a esta tipologia de veículos. Primeiramente, se se perfilha um veículo automóvel quanto à "Agência" ou "Agentividade" na Computação, nele incluindo as suas propriedades várias, que não só a autonomia, não se entende o porquê de seguir a qualificação que logra somente uma das apropriações [31]. Em segundo lugar, também não se acolhe a notação de Veículos Autónomos e 'Inteligentes' -, caso em que, posicionando-se a autonomia como um dos consequentes da premissa-mor cujo antecedente se deve à qualidade inteligência, de um ponto de vista lógico, não seria congruente e dedutivamente correto estabelecer uma definição que, em relação a ambos os termos– a melhor ver, a autonomia e a inteligência-, estabelece uma concordância gramatical via conjunção coordenativa copulativa [32]. De outro modo, estar-se-ia a tornar possível computar dentro do mesmo âmbito subjetivo realidades que, num perspetivar técnico, designam entidades diferentes e, por esse mesmo motivo, carecem de tratamentos díspares quanto à imputação de responsabilidades. Ou seja, reconduzir-se-iam quer os VA'I', quer os AI-A, no reduto de objetos, erroneamente.

Em suma, nem toda a inteligência confere graus de autonomia satisfatórios para a substituição do condutor humano. De todo o modo, é axiomática a consideração de que a inteligência se posiciona como antecedente de vários redutos, que não só a autonomia dos veículos automóveis (v. *supra*). Posto isso, crê-se que a terminologia mais precisa

30 Cf. com algumas adaptações, para os devidas efeitos, F. Pacheco de Andrade, *Da contratação eletrónica ... supra*, 165, na esteira de M. Wooldridge e N. R. Jennings, Intelligent agents: theory and practice, *The Knowledge Engineering Review*, Cambridge University Press, vol. 10(2), 1995, 116 – 117; e, quanto à indústria dos AI-A em especial, N. Chakraborty e R. S. Patel, Intelligent Agents and Autonomous Cars: ... *supra*, 4.

31 Crê-se, desta feita, não serem somente quatro, antes sete as caraterísticas ou os atributos que descrevem aquilo que devemos computar no fenómeno "Agência na Computação", cf., embora carecido de alguns aprimoramento concetuais, B. A. Ribeiro, *A Responsabilidade Legal de Veículos Autónomos, Uma Perspetiva da Ciência Cognitiva*, Dissertação de Mestrado, Universidade de Lisboa, 15, 45-46, https://repositorio.ul.pt/handle/10451/39556.

32 Cf. P. Suppes, Introduction to Logic, Littion educational publishing, Van Nostrand Reinhold Company, 1957, xv. e 3-19.

e tecnicamente mais próxima das demonstrações científicas será a de AI-A, vulgamos, Agentes Inteligentes Automóveis [33].

E também se, por um lado, pode asseverar-se que tanto os objetos como os agentes automóveis inteligentes exteriorizam "uma identidade, um estado e comportamentos próprios, por outro, a verdade é que tudo isso se torna mais complexo no caso dos agentes, que podem ser descritos em termos da existência de um conjunto de características que integram, independentemente, conhecimento, crenças, desejos, intenções, objetivos e até obrigações" (sublinhados, a enaltecer os tratos concretizados por alguns modelos no atual estado de arte agentes automóveis inteligentes) [34_35]. Os AI-A representam o conhecimento através da perceção do meio envolto, planeiam os cursos possíveis da operação em razão dos objetivos que o passageiro lhes incute, denotam a intenção de os concretizar, e ademais, fazem jus aos ditames plasmados nas obrigações legais resultantes das regras estradais fixadas no e pelo Código da Estrada (doravante, abreviadamente, CE) [36], *et alii* (v. *infra*).

Não obstante, além de exteriorizarem as características *ante* mencionadas, manifestam também propriedades mais complexas, geralmente mais próximas da cognição humana e típicas da hegemonia inteligência computacional (o *soft computing*) em decisões tomadas exclusivamente com base na deteção (*image recognition*), e prospeção (*machine learning*) de dados recolhidos, armazenados e processados autonomamente [37]. Expressam, a bem dizer, os traços metacognitivos [38] que à IA têm

33 Cf. expressões empregues por P. M. Freitas, Veículos Autónomos e "Inteligentes" perante conflitos de interesses: uma visão a partir do Direito de Necessidade, in *CyberLaw (CIJIC)*, ed. n.º V, 2018, 10, https://www.cijic.org/wp-content/uploads/2018/03/VEÍCULOS-AUTÓNOMOS-E-INTELIGENTES-PERANTE-CONFLITOS-DE-INTERESSES_UMA-VISÃO-A-PARTIR-DO-DIREITO-DE-NECESSIDADE-JURÍDICO-PENAL.pdf.

34 Cit. F. Pacheco de Andrade, Da contratação eletrónica … *supra*, 164, na esteira de C. Analide, P. Novais, J. Machado e J. Neves, Quality of knowledge in virtual entities, ... *supra*, 436-442; e *vide* ainda, M. Wooldridge e N. R. Jennings, Intelligent agents … *supra*, 117.

35 No atual estado da arte AI-A, é já possível ousar a personalização de agentes, este fenómeno que agrega, além da inteligência, ainda a valência da intencionalidade. Cf., F. Pacheco de Andrade, *Da contratação eletrónica inter-sistémica ... supra*, 178.

36 *Vide*, redação atual do Decreto-Lei n.º 114/94, de 03 de maio - diploma originário que aprovara o CE.

37 Cf. E. Corchado, P. Novais, C. Analide, J. Sedano, Soft Computing Models in Industrial and Environmental Applications, *in Advances in Intelligent and Soft Computing*, 5.º Workshop Internacional, vol. 73, Springer-Verlag, Berlin Heidelberg, 2010, [Prefácio]; e *vide*, C. Analide e D. Morgado Rebelo, A Inteligência Artificial na era *data-driven*, A lógica fuzzy das aproximações de soft computing e a proibição de sujeição a decisões tomadas exclusivamente com base na exploração e prospeção de dados pessoais, *in Forum de Proteção de Dados*, n.º6, CNPD, Lisboa, 2019, 60-91, https://www.cnpd.pt/home/revistaforum/forum2019_6/index.html.

38 No prisma da computação, a "Metacognição estará ligada a uma introspeção, no sentido de a máquina ser capaz de ter uma crença sobre os seus próprios estados mentais, mais do que apenas fazer considerações sobre o meio envolvente", cit. B. A. Ribeiro, *A Responsabilidade Legal de Veículos Autónomos … supra,* 62.

vindo a ser associadas, porquanto, além de representarem em tempo real o conhecimento do meio rodoviário envolvente (*declarative knowledge*), sabem como agir, quando e porque o hão-de fazer (*procedural* e *conditional knowledge*, respetivamente) [39].

Na qualidade de processador cognitivo, o cérebro sintético de um AI-A reconhece as suas capacidades, revelando desta feita conhecimento metacognitivo [40]. Outrossim serão algumas as situações dilemáticas em que, representando e planeando o curso da suputação, os AI-A anteciparão com determinados *standards* probabilísticos que não concretizarão a tarefa dinâmica que lhes é designada, *at least*, com a segurança augurada. Este é o âmbito regulatório da cognição e aprendizagem, alicerçada naquilo que o sistema tem noção não saber [41]. E, de suma importância, em razão das experiências perpetradas no passado, o AI-A criará expetativas daquilo que poderá acontecer [42]. Assim, pode-se asseverar que somente os AI-A exteriorizam uma atuação verdadeiramente inteligente e independente em sentido amplo.

A partir daqui se deduz que serão consignados à tipologia de agentes automóveis AI-A todas as entidades artificiais ou sistemas do veículo automóvel conexos à habilidade inteligência fraca ou forte, respetivamente, correspondentes aos níveis 4 e 5. Nos dias de hoje, os AI-A são já hábeis em substituir integralmente o condutor através da observação e experiência, executando otimizada e eficientemente a função de transitar na via pública, galgando ou ajustando automatizadamente rotas em função do tráfego, antecipando também situações não passíveis de serem cognoscíveis pelo ser humano. E fazem-no num hiato espácio-temporal prévio à existência de sinais objetivos de perigo e à sequer possível tomada de consciência destes por parte dos passageiros. Não obstante, somente num estádio situacional ulterior ao treino, teste e inserção dos agentes em ambiente rodoviário, e por de entre a delonga espaço-tempo que sinaliza períodos de simulação e teste tanto em ambientes fechados como abertos, também

39 Cf. J. Crowder, S. Friess e M. NCC, Metacognition and metamemory concepts for AI systems, *in Proceedings on the International Conference on Artificial Intelligence (ICAI)*, The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2011, s.p, https://search.proquest.com/openview/7f3758944801234b137b25813441813d/1?cbl=1976349&pq-origsite=gscholar.

40 *Vide*, Kosko, G., Fuzzy Cognitive Maps, *in* International Journal of Man-Machine Studies, 24 (1), 1986, 65-75, https://leszeksykulski.pl/wp-content/uploads/2018/10/Kosko_FCM_Fuzzy_Cognitive_Maps.pdf; cit. *in* J. Crowder, S. Friess e M. NCC, Metacognition and metamemory concepts … *supra,* s.p.

41 *Vide,* K. S. LaBar e Roberto Cabeza, Cognitive neuroscience of emotional memory, *in Nature Reviews Neuroscience*, n.º 7 (1), 2006, 54-64, https://www.nature.com/articles/nrn1825, cit. *in* . J. Crowder, S. Friess e M. NCC, Metacognition and metamemory concepts … *supra,* s.p.

42 Cf. J. Crowder, S. Friess e M. NCC, Metacognition and metamemory concepts … *supra,* s.p.

dependendo dos vários modelos e das várias tecnologias a eles aplicadas, os AI-A operarão com elevados níveis de segurança.

Ademais, a conceção operacional destes agentes abrange, designadamente, a circulação em condições atmosféricas adversas, percursos com trilhos desestruturados, pisos sinuosos com declive variável e sobretudo defronte casuísticas às quais convencionamos ora atribuir a designação de SPS (*Super Problem-Solving*). Estas, por conseguinte, decorrerão em conjunturas de congestionamento no tráfego e de perigos inopinados de colisão eminente com outros veículos, transeuntes (humanos ou animais), assim como avante o possível embate com objetos corpóreos. Diante tais eventos sinistrais, nem o homem-médio mais prudente, assumindo as vestes monopolistas sob direção efetiva de um AI-A – mediante solicitação volitiva e planeada, mas não controlável com segurança pelo agente 'maquinizado'– conseguiria acautelar ou sequer evitar a ocorrência de danos, atenta a inexistência do pendor incognoscibilidade dos elementos prescritos pelo tipo incriminador, antepondo este como quesito de uma ação jurídico-penalmente relevante.

Face ao exposto, tanto os AI-A fracos como os AI-A fortes subsumir-se-ão às classes dos agentes automóveis inteligentes orientados a objetivos (*Goal based agents*) e baseados na utilidade (*Utility based agents*), cumulativamente, sendo capazes de controlar as suas decisões.

Quanto ao primeiro prisma– o do *goal based* - porque almejam executar os objetivos que lhe foram confiados pelo proprietário ou passageiro, além do conhecimento atualizado acerca dos estados, estes agentes representam heuristicamente os cursos de operação de forma a executarem *targets* prévios ou concomitantes em contornos otimamente combináveis, obedecendo às obrigações legais. Através destes traços personalísticos de pendor eletrónico em especial, os AI-A exteriorizam cognição e volição, respetivamente, manifestando o conhecimento acerca da realidade e intenções de concretizar determinados objetivos [43].

43 *Vide*, para mais aprofundamentos, G. Hallevy, op. cit., 37, não obstante destituirmo-nos a este propósito de integrar estes redutos no tipo de ilícito subjetivo ou na culpa, ora para efeitos de se considerarem preenchidos os pressupostos de imputação definidos doutrinalmente pela e na Teoria Geral do Crime. Por exemplo, o veículo Waymo consegue já, tal qual o ser humano encontra-se habilitado – com maiores margens de erro, refira-se – a: (1) determinar a localização precisa do via mapas tridimensionais; (2) através da sensorização e processamento de dados via hardware e software, respetivamente, identificar o meio envolvente num raio de 300 metros; (3) prever a dinâmica futura dos objetos móveis, pessoas e ciclistas, em contornos preditivos; (4) selecionar a operação de resposta mais útil, em função de variáveis como a trajetória, a velocidade, e mudanças de direção necessárias. Cf. Waymo Safety Report, On the Road to Fully Self-driving, 2009, 8-9, https://waymo.com/safety/.

No que concerne ao segundo ângulo – o da *utility based* – alegar-se-á que estes agentes não só projetam a execução das suas operações no alicerce sem-par dos objetivos, outrossim em função do custo-benefício que as suputações racionais por estes levadas a cabo acarretam [44]. Neste campo de operação, defronte situações dilemáticas não "*The Runaway Trolley*" [45], o ativar autonómico da função utilidade engendrará solucionar estas proficuamente, de forma segura e confiável, designadamente:

(1) defronte dois *targets* conflituantes, onde se conjetura a antítese no *trade-off* de entre os valores velocidade e segurança. Nestas conjeturas, as valorações próprias e intrínsecas ao AI-A, resultantes do processo de aprendizagem *by design* e *by default*, impelir-lho-ão a conceder primazia aprioristicamente ao segundo – a segurança -, mas em razão da experiência perpetrada nas fases de treino e teste, destituindo aqui quaisquer valorações intrínsecas concernentes ao raciocínio jurígeno que estabelece a hierarquia de entre as normas no ordenamento jurídico português [46]; e

(2) nas situações em que o agente automóvel, meditando sobre os vários objetivos que vaticina concretizar, reconhece de todo o modo difícil conseguir realizar a totalidade sem despoletar a ocorrência de danos patrimoniais ou não patrimoniais, preterindo pelo menos um deles ou executando todos em contornos incompletos. Nesta senda, será a função utilidade (*happiness function*) a responsável por acautelar e ponderar as probabilidades de sucesso de cada combinação *Big Data*. A título de exemplo, cogitemos a situação em que o agente automóvel ajusta a rota em função do tráfego rodoviário, ultrapassando a sinalização vermelha do semáforo e os dois camiões que circulam numa marcha lenta à sua frente, de forma a cumprir o *target* de fazer com que o advogado, ora passageiro, patrocine o seu cliente na sessão de julgamento

44 Cf. N. Chakraborty e R. S. Patel, Intelligent Agents and Autonomous Cars: *... supra,* 3.

45 Cf., P. Foot, *The Problem of Abortion and the Doctrine of Double Effect, in Virtual and Vices and Other Essays in Moral Philosophy*, Oxford, UK, Basil Blackwell, 1978, 19; e J. J. Thomson, The Trolley Problem, *in Yale Law Journal*, n.º 91, 1985, 1395-1415, cit. in. M. Sandel, Justice, *What is the Right Thing To Do?*, Penguin Books, London, England, 2009, 21-24. Sobre a temática dos carros autónomos, vide, A. Renda, Ethics, algorithms and self-driving cars – a CSI of the 'trolley problem', in CEPS Policy Insights, 2.ª ed, 2018, http://aei.pitt.edu/93153/.

46 Cf. N. Chakraborty e R. S. Patel, Intelligent Agents and Autonomous Cars: *... supra,* 3. E todo este *check & balance* será sisudo autonomamente. Aliás, esta é a preponderância que as fases de treino e teste poderão assumir quanto aos valores confiança e segurança das operações AI-I. Na área do Direito Constitucional, clarividente, estando em causa um valor consagrado numa norma superior, *in casu*, o artigo 27.º da Constituição da República Portuguesa (doravante, abreviadamente, CRP), a opção a induzir o veículo a aprender será sempre a escolha racional primeira pelo segurança, independentemente da não satisfação que o ocupante possa manifestar, nomeadamente quando não cumpra um compromisso que assumira quotidianamente. Todavia, este é um processo de aprendizagem levado a cabo nas fases de treino e teste, pelo que o agente cumprirá as obrigações supra-legais a que se encontra adstrito, nos termos da *norma normarum*, por força das simulações, treinos e atualizações do software, denote-se.

atempadamente. Existem riscos associados a cada combinação, uma delas pressupondo mesmo o incumprimento de regras estradais, pelo que o agente fiar-se-á naquela cujo custo-benefício apresente uma maior fiabilidade na prevenção dos danos. De facto, aqui o utilitarismo afigura-se ser uma aproximação computacional fácil de reproduzir via suputação. Todavia, como não existe bela sem senão, quando reduzida à prognose de minimização dos danos, esta abordagem ética pode implicar a tomada de decisões injustas *in natura* [47].

Portanto, esta é, *hoc sensu*, a razão da preponderância que estas etapas precípuas – a melhor ver, que a simulação, o treino e o teste do cérebro sintético do veículo - assumem quanto à prevenção dos danos e minimização do risco (*fallback* ou *minimal risk condition*). A este respeito, consideramos que a tecnologia da Google se apresenta na vanguarda da extensão AI-A, sendo também aquela que orienta o seu público-alvo - i.e., a todos nós, consumidores -, com os fios-condutores mais transparentes e úteis na diferenciação entre os AI-A fracos e fortes, respetivamente. Enquanto AI-A, o desenvolvimento e implementação do sistema ciberfísico e software Waymo obedece a políticas rigorosas de treino e teste, naquele que se crê ser um ambiente de segurança conducente a uma condução mais inteligente, mais confiável e, acima de tudo, mais transparente [48].

Ora, os estágios de preparação destes agentes reconduzem-se às seguintes fases: simulação, treino e testes em ambientes fechados e abertos, sequencialmente. Senão repare-se:

1. Primeiramente, são efetuadas alterações e atualizações ao sistema em cenários virtuais, tal-qual este haja iniciado autonomamente o processo de aprendizagem *fuzzy* e em função das informações recolhidas ou disponibilizadas, constituindo ou materializando esta a fase da simulação (*simulation testing*) [49];

2. Em segundo lugar, implementadas que sejam as correlações virtuais no agente, segue-se a fase de testes em percursos fechados (*closed-course testing*), aquela

47 Cf. B. A. Ribeiro, *A Responsabilidade Legal de Veículos Autónomos ... supra,* 35-39.

48 Estas particularidades são corroboráveis pela publicitação das Políticas de Segurança suficientemente detalhadas, *vide*, mais detalhadamente, Waymo Safety Report, ... *supra*, 1-43.

49 O período de simulações Waymo, além de reproduzir as várias milhas percorridas pelos carros que compõem a frota no mundo real, constrói também cenários virtuais completamente novos – embora próximos da realidade – os quais, por conseguinte, virão numa fase ulterior a ser objeto de testes. Todos os dias 25.000 veículos percorrem percursos virtuais, perfazendo no total de 8 milhões de milhas, num ímpeto de aperfeiçoar capacidades antigas e de testar novas manobras, cf. Waymo Safety Report, ... *supra*, 23. Nestas fases de preparação, os engenheiros responsáveis observam as situações do mundo real, instruindo concomitantemente comandos computacionais *soft* de modo a que o agente alvitre otimizar as várias tarefas num enjeito de *reinforcement learning*.

que permite integrar diferentes versões para cada agente, caso em que serão verificadas novas ou específicas características aplicáveis nos diferentes domínios da conceção operacional;

3. Somente numa fase posterior – ainda que antecedendo a colocação do agente à venda no mercado automóvel – serão efetuados treinos de condução inteligente em ambiente estradal aberto (*public roads*), nas mais variadas e adversas condições atmosféricas, bem como em diferentes pisos [50]. Ora, neste hiato último, o veículo terá de exteriorizar já traços de grande apetência para uma condução consistente e segura. Neste processo, as atualizações do software aprendidas serão também integradas na frota, refira-se a título de apontamento [51_52].

Portanto, em alusão ao protótipo da Google Waymo, pode-se concluir que as fases de simulação, treino e teste em ambientes fechados e abertos, cumulativamente, fornecem um *loop* de *feedback* contínuo que habilitará o fabricante a refinar o sistema do agente inteligente, tornando-o mais seguro nessa medida. E é esta abordagem iterativa dos ensaios e validação rodoviária que viabilizará expandir os domínios de conceção operacional e as capacidades de circulação inteligentes dos AI-A, ajustando ao máximo as margens de erro aquando da circulação em ambientes reais, consequentemente, reduzindo a jusante a possibilidade da ocorrência de eventos sinistrais.

Toda a tecnologia dos AI-A deverá ser construída ou configurada de forma suficientemente robusta para lidar independentemente com situações dinâmicas, conforme aos 5 corolários que ora teorizamos relativamente ao processo de validação multifacetado de uma condução automóvel inteligente, a melhor ver: a segurança comportamental (*behavioural safety*); a segurança funcional (*functional safety*); a segurança em caso de colisão (*crash safety*); a segurança operacional (*operational safety*); e, por último, a segurança de não colisão (*non-colision safety*) [53].

A melhor ver:

50 Cf., Waymo Safety Report, ... *supra*, 28.
51 Cf., Waymo Safety Report, ... *supra*, 22.
52 Ambas as fases de testes são demarcadas pela monitorização dos veículos por parte de especialistas com uma extensa formação em ambiente de aula, aos quais lhe são ministradas valências para interagem com o agente de forma segura nas estradas públicas, *inclusive*, contando com a realização de cursos de condução defensiva. Se necessário, estes monitores humanos assumirão a direção efetiva, de forma a que se evite a ocorrência de danos na sequência de algum acidente, cf. Waymo Safety Report, ... *supra*, 26.
53 Cf., Waymo Safety Report, ... *supra*, 11.

(a) No prisma comportamental, os AI-A deverão revelar aptidão para a tomada de decisões em ambiente estradal, fazendo jus às regras de trânsito [54] e navegando com segurança numa grande variedade de cenários [55];

(b) Funcionalmente, a segurança dos AI-A deverá ser exteriorizada sob a forma da capacidade que o automóvel apresenta em colmatar falhas no sistema, construindo sistemas de apoio redundantes de forma a resolver o inesperado, p.ex., através da ativação dos computadores secundários na direção e travagem de reserva que viabilizem uma paragem segura[56];

(c) Quanto à segurança em colisão – *crashworthiness* – os veículos AI-A operarão num ímpeto de protegerem os passageiros que se encontrem no interior, p.ex., ativando os encostos dos bancos e o sistema de *airbags* para atenuar os ferimentos ou até mesmo, em *ultima ratio*, para prevenir o resultado morte [57];

(d) Operacionalmente, o interface veículo-passageiros reconduz-se ao conjunto de informações que devem ser prestadas diante do consumidor, designadamente, análises de risco, normas de segurança, testes extensivos, bem como as melhores práticas a adotar. Ao proprietário ou passageiro do automóvel inteligente deve ser concedida a faculdade de indicar claramente o destino, dirigir o veículo para encostar em locais muitos apertados, sendo-lhe ainda facultada a possibilidade de contactar a qualquer momento a linha de apoio Waymo; e

(e) por último, os AI-A deverão ainda adotar políticas de segurança máxima de forma a preservar a integridade física daquelas pessoas que com o veículo podem interagir no exterior [58].

---

54 Cf., linha n.º 19 da tabela que elenca o conjunto de competências comportamentais, Waymo Safety Report, ... *supra*, 36.

55 Para além das competências comportamentais recomendadas pela Administração Nacional de Segurança e Trânsito Rodoviário norte-americana - a *National Highway Traffic Safety Administration* (NHTSA) – a Waymo agrega operacionalmente mais 19 habilidade, num total de 47. São de salientar, a título exemplificativo, a mudança para uma condição de risco mínimo quando não é possível sair da faixa de rodagem, a deteção e resposta a pedestres, o providenciar distâncias seguras aos ciclistas que viajam na estrada, a deteção e resposta de animais, a realização de inversões de marcha apropriadas, *et alii.*, cf. ... *ibidem,* 36-37.

56 Cf., linha n.º 42 da tabela relativa ao conjunto de competências comportamentais, Waymo Safety Report, ... *supra,* 37.

57 Os veículos da Google Waymo encontram-se habilitados a prevenir ou mitigar colisões traseiras, demonstram capacidade em detetar veículos que circulam num ângulo perpendicular, acionando o sistema de travões automaticamente, seguem a trajetória em função das linhas divisórias e minimizam os riscos correspondentes quando estas não se encontram nas melhores condições. Evitam ainda o embate com os veículos que circulam noutras faixas de rodagem, cf., Waymo Safety Report, ... *supra,* 38-39.

58 Cf. Waymo Safety Report, ... *supra,* 11.

Ora, em conformidade com o exposto, *supra,* é-nos consabido que também os AI-A deverão ser bifurcados nas categorias fraca e forte, respetivamente, em alusão - se assim se intentar continuar a relutar -, aos níveis 4 e 5 da hétero proclamada autonomia automóvel. O mote pelo qual se diferenciam uns de outros residirá sob o prisma operacional *fallback,* bem como no seu limitado âmbito geográfico operante. Em relação ao primeiro, quando o AI-A não conseguir prosseguir uma viagem previamente planeada – porque antecipa o perigo iminente de colisão, deteta falhas no sistema ou atenta nas mudanças das condições atmosféricas que poderão interferir na conceção de uma condução prudente -, deverá ser capaz de efetuar uma paragem segura. Este é *per si* o bastião da manobra "condição mínima de risco ou de retirada" da inteligência máxima concretizada até aos dias de hoje numa condução automóvel dinâmica e inteligente. Em função da gravidade destes fatores, o cérebro sintético do AI-A irá determinar a resposta adequada de forma a manter o veículo, os seus passageiros e, *inclusive,* as pessoas, animais ou objetos envolvidos no exterior, em condições de segurança, optando por encostar e chegar a um porto-seguro [59]. Ademais, uma das limitações relativas ao fenómeno *on the road to fully self-driving* tem que ver com a circunscrição do âmbito territorial no qual estes veículos encontram-se habilitados a operar, quer em termos legais, quer em termos técnicos. Assim, os passageiros não poderão selecionar um destino que não se encontre abrangido na área 'geo-certificada', pelo que, sendo esse o caso, o software requererá ao condutor a assunção de controlo do automóvel, não mapeando novas rotas. E fá-lo porque não dispõe de informação suficiente para preconizar os desígnios que lhe estão a ser confiados [60].

Portanto, num enjeito de sinopse deste pequeno começo concetual, urge-se prescrever não *a la Hollywood* que só aqueles veículos automóveis que preconizam os seus desígnios funcionais em ambientes dinâmicos e improváveis, representando o conhecimento envolvente, planeando e controlando os cursos das operações decisórias em ambiente rodoviário, bem como reagindo consecutivamente aos estímulos que destes são continuamente recebidos através da ativação dos efetores, num aspecto seguro e antecipatório, poderão ser qualificados como AI-A (sublinhado, a enaltecer expressões, nosso). Como elementos lógicos antecedentes da alegada axiomática autonomia dos veículos, e por de entre a equação cujo produto igualará a inteligência sintética, as proposições complexas aprendizagem, raciocínio e idónea aptidão iterativa com o meio

59 Cf. Waymo Safety Report, ... *supra,* 16-17
60 Cf. Waymo Safety Report, ... *supra,* 16.

estradal designarão aquela que é tida como a funcionalidade de um agente aprendiz inteligente.

Assim, julga-se que a evolução da Sociedade XXI para uma indústria automóvel totalmente inteligente pressuporia uma subversão completa do mote como a mobilidade urbana tem-se por demarcada segundo o prisma de tráfego misto. Se é certo, por um lado, que o poder económico das famílias não lhes assinte suportar a aquisição de AI-A, por outro, são robustas as razões para se crer que uma interação crescente *M2M* (*Machine-to-machine*) em ambiente estradal poderá contribuir significativamente para reduzir a sinistralidade rodoviária e o número de vítimas mortais, aumentando a jusante a qualidade de vida dos utilizadores finais e, aliás, tornando o ecossistema mais sustentável [61].

Por ora, embora sendo dúbia, incerta e árdua a tarefa de categorizar os modelos dos veículos conforme aos níveis de maturação na IA, aclamamos à cautela ser o protótipo desenvolvido pela Google Waymo o vanguardista da condução objetivamente inteligente, i.e., aquela que não se cinge somente à incompletude do sigma autonomia [62]. São então, como se acaba de constatar, pelo menos três os modelos de veículos – computando no âmbito material desta anotação o projeto Volvo *DriveMe* [63] – que balizam a rota da condução inteligente na IA para o Século XXI. Aclama-se, contudo, ser metaforizada, ou antes, exacerbada e comercial, a fábula que exorta os vários modelos TESLA e o classe S 400 D da mercedes no qualificativo 'autónomo'.

2.3. Breves Considerações Sobre O *Modus Operandi* De Uma Decisão Inteligente À Escala Circulação Automóvel

A condução inteligente pode ser fragmentada em três fases, sequencialmente funcionais e relativas à multiplicidade dos processos perceção, planeamento e controlo decisórios que às várias operações complexas como esta subjazem.

61 Resolução do Parlamento Europeu, de 15 de janeiro de 2019, ... *supra*, Alínea B.
62 *Vide*, Waymo Safety Report, … *supra*, 1-43 https://waymo.com/safety/. É de referir ainda, a título de apontamento secundário, que o projeto "*Volvo DriveMe"* ambiciona colocar nas estradas de Gotemburgo (Suécia) uma série de VAI, com o intento de exteriorizar a capacidade relativa ao *standard* de autonomia 4 em estradas certificadas, augurando em simultâneo avaliar a importância, bem como impactos respetivos que esta tipologia de agentes surtirá na qualidade de vida do cidadão e na alegada transformação para um ambiente urbano mais sustentável e mais seguro, cf. A. J. Moreira Lousa, *Veículos Autónomos e Conetados* ... *supra*, 16.
63 Cf. ... *ibidem*, acerca do projeto Volvo *DriveMe*, em particular.

Primeiramente, o sistema do veículo deve encontrar-se dotado da capacidade de selecionar e recolher toda a informação que possa relevar para melhor interpretar o ambiente que o rodeia, desenvolvendo um contexto e uma compreensão específicos acerca do tipo de clima, estados das estradas, intensidade do trânsito, existência de obstáculos, posicionamento da sinalização, também de mote a calcular com precisão as velocidades de outrem ou até mesmo prever estados futuros dos objetos, pessoas e animais, etc., tudo isto através da captação, interpretação e processamento dos dados via sensores externos. Um veículo inteligente reconhecerá ainda a sua posição – através do uso do *General Positioning System* (GPS) ou de Sistemas de Navegação por inércia (*Inertial Navigation Systems*) [64] – assim como a sua velocidade, os níveis de pressão nos pneus, entre outros, ora através dos seus sensores internos [65]. Neste período assumirá especial preponderância a operação de processamento de imagens, captadas continuamente por câmaras, radares e lidares [66], e ulteriormente processadas de mote a que sejam extraídos os traços essenciais para efetivar a sua classificação, deteção e reconhecimento via *Deep Learning* [67].

Na fase de planeamento, os AI-A delineiam os vários cursos da operação com a **intenção** de concretizarem determinados **objetivos** (sublinhados, a propósito, nosso). E

64 Os Sistemas de Navegação por Inércia fazem uso de instrumentos como acelerómetros, giroscópios e técnicas várias de processamento de sinais, calculando as biométricas de movimento, orientação, inclinação, bem como a altitude a que o veículo se encontra, prescindindo nesse sentido de aparelhos externos ao veículo, como o GPS, cf. B. A. Ribeiro, A Responsabilidade Legal de Veículos Autónomos ... *supra*, 23.

65 Cf. B. A. Ribeiro, A Responsabilidade Legal de Veículos Autónomos ... *supra*, 19-23.

66 Através de milhares de pulsares de luz por segundo, o LIDAR encontra-se habilitado à deteção de luz e alcance, medindo a reflexão para determinar a distância num eixo rotativo, disponibilizando ao utilizadores um mapa dinâmico e tridimensional do ambiente envolto aos Veículos *quase*-inteligentes (VA'I')ou aos Agentes Inteligentes Automóveis (AI-A) Cf. S. Lonita, Autonomous Vehicles: From Paradigms to Technology, *in IOP Conference Series*, vol. 252, 5, http://iopscience.iop.org/article/10.1088/1757-899X/252/1/012098.

67 Já no que concerne à Aprendizagem Profunda, ou antes, *Deep Learning*, dir-se-á que as suas técnicas se posicionam dentro do cômputo material *Machine Learning*, projetando ou avaliando a precisão das configurações algorítmicas relativas a incomensuráveis Multicamadas (*layers*) das arquiteturas de Redes Neuronais Artificiais (RNAs'). Cf. J. D. Kelleher, *Deep Learning*, The MIT Press Essential Knowledge Series, The MIT Press, Cambridge, MA, 2019), 6 e 252. Por conseguinte, as RNA corporizam estruturas interconectadas de unidades computacionais com capacidade de aprendizagem, frequentemente designadas por neurónios ou nodos, com arquiteturas desde as entradas (*inputs*) até às saídas (*outputs*), perpassando por de entre pelo menos mais de duas camadas intermédias ou ocultas (as *hidden layers*). Materializam processadores eminentemente paralelos que integram simples unidades de processamento (sinais) com propensão ao armazenamento e previsão de conhecimento aproximado, sujeitos a margens de erro nessa medida. Por conseguinte, as arquiteturas RNA potenciam a mimetização do processo sináptico até então cognoscível do cérebro humano, processando informação e manipulando conhecimento através das conexões ou ligações que integram a sua arquitetura base, normalmente com mais de duas camadas intermédias, cf. P. Cortez e J. Neves, Redes Neuronais Artificiais, Apontamentos de apoio à disciplina de Sistemas Inteligentes, Departamento de Informática, Universidade do Minho, Braga, 2010, 3-4, http://repositorium.sdum.uminho.pt/bitstream/1822/158/1/redes.pdf; A. Oliveira, *The Digital Mind: how science is Redefining Humanity*, The MIT Press: Cambridge, MA (2017), 267 [versão iBook].

fazem-no em razão da missão, do comportamento, do movimento e num ângulo dinâmico. Assim, de forma a que seja esboçada a melhor rota que o agente deva percorrer para chegar ao destino, o sistema representa as redes de estradas através de um gráfico dirigido, computando os custos associados – como sejam, os quilómetros a percorrer, dispêndios monetários com combustíveis, a intensidade do tráfego ou a possibilidade de existir um acidente -, tudo isto numa ótica de perfilhar a solução otimamente combinável para o problema da Missão. Este sistema terá de exteriorizar ainda aprendizagem comportamental coadunável com o cumprimento das normas estradais, assim como deverá ser capaz de manifestar uma interação idónea com os outros agentes que dele se aproximam, quer seres vivos, quer agentes de software. Terá também a incumbência adicional de executar trajetórias seguras, confortáveis e dinamicamente possíveis, designadamente por referência à configuração previamente realizada no prisma comportamental. A findar, defronte a ocorrência de falhas que possam despoletar danos, o veículo primará a todo o custo por acionar o efetor apropriado, v.g., reordenando a direção, a pressão ideal dos pneus ou até mesmo escolhendo a utilização da sinalização por piscas, entre outros [68].

Por último, o controlo das próprias ações, por seu turno, prende-se com a habilidade que o AI-A evidencia em executar ações *stricto sensu*, otimizando a trajetória na delonga do tempo limitado que possui, de maneira recursiva e tendo em consideração a atualização da informação de que dispõe. No atual estado da arte AI-A o desígnio previsão dos estados futuros de outros veículos assume especial proeminência, contanto o AI-A possui já a capacidade de antecipar a trajetória de outros veículos através da recolha e processamento dos dados provindos do ambiente estradal e implementação de técnicas de Aprendizagem Automática, *et alii*[69].

68 Cf. B. Paden [et.al], A Survey of Motion Planning and Control Techniques for Self-Driving Urban Vehicles, *in IEEE Transactions on Intelligent Vehicles,* 33-55, https://ieeexplore.ieee.org/abstract/document/7490340/?casa_token=Niet16myTTwAAAAA:O8nItwarMNORQCfzjqI6RIntxXh-nRGKzPJRey9UcrPtTAY91qoMs4wH8_STIcglGgWyGAw1Gog.
69 *Vide*, B. A. Ribeiro, *A Responsabilidade Legal dos Veículos Autónomos ... supra,* 24-26,

3. SER OU NÃO SER IDÓNEO NA RESERVA DE COMPETÊNCIA RELATIVA: EIS A LÓGICA DO DEIXA ANDAR E ESPERAR POR ACONTECER NO ÓCIO '*NEM, NEM, NEM*' DA ENGENHOCA LEGIFERANTE

Ora, em consonância com a *praxis* legiferante precária, fragmentária, desatualizada e (leigo)rítmica, tanto as instituições da União Europeia - inobstante tendo centrando o foco de alguns dos seus trabalhos em matérias de imputação de responsabilidade automóvel no horizonte da IA [70]- , como a Assembleia da República (doravante, abreviadamente, AR) denotam alguma indiligência nas necessárias adaptações subsumíveis defronte ao Conceito Material e à Teoria Geral do Crime, quando aplicável, *mutatis mutandis,* ao fenómeno AI-A.

Se, por um lado, "não é (...) particularmente surpreendente que as poucas iniciativas legislativas surjam timidamente, de modo fragmentário e compartimentado" [71], em correspetiva, "as novas tecnologias e a inteligência sintética constituem um *tópoi* a que o Direito (e, particularmente, o Direito Penal) não podem nem devem olvidar" (sublinhados, em acrescento, e ajuste, nossos) [72].

---

70 São várias as comunicações, relatórios e projetos desenvolvidos a nível europeu no âmbito da implementação de um Sistema de Transportes Inteligentes e Cooperativos (STIC), aliado ao fomento dos mecanismos de segurança rodoviária, designadamente aqueles que se focalizam na imputação de responsabilidade civil, a melhor ver, *vide*: (1) Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Economico e Social Europeu e ao Comité das Regiões, de 30 de novembro de 2016, sob o tema: "Uma estratégia europeia relativa aos sistemas cooperativos de transporte inteligentes, uma etapa rumo a uma mobilidade cooperativa, conectada e automatizada", https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A5; (2) Relatório da Comissão ao Parlamento Europeu e ao Conselho [COM/2016/0787 Final], de 12 de dezembro de 2016, sob o tema Salvar Vidas: reforçar a segurança dos veículos na UE Relatório sobre o acompanhamento e a avaliação dos dispositivos avançados de segurança dos veículos, a sua relação custo-eficácia e a sua exequibilidade, tendo em vista a revisão dos regulamentos relativos à segurança geral dos veículos e à Protecção dos peões e outros utilizadores vulneráveis da estrada, https://www.europarl.europa.eu/doceo/document/A-8-2017-0330_PT.html.; (3) Resolução do Parlamento Europeu que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica [2015/2103/INL], de 27 de janeiro de 2017, https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_PT.html; (4) Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, com recomendações da Comissão Europeia relativamente a Matérias de Responsabilidade Civil dos Robôs (2915/2103 INL), https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_PT.pdf.; (5) Parecer do Comité das Regiões Europeu, de 10 de outubro de 2017, relativo à fixação de uma estratégia europeia para os sistemas de transporte inteligentes e cooperativos [STIC] (2018/ C 054/06), em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017IR2552&from=EN; (6) Relatório do Parlamento Europeu, de 23 de fevereiro de 2018, Estratégia Europeia para os Sistemas de Transporte Inteligentes e Cooperativos (STI-C) (A8-0036/2018), https://www.europarl.europa.eu/doceo/document/A-8-2018-0036_PT.pdf; também (7) Parlamento Europeu, *Relatório sobre condução autónoma nos transportes europeus* (2018/2089(INI)), Comissão dos Transportes e do Turismo, de 5 de dezembro de 2018, https://www.europarl.europa.eu/doceo/document/A-8-2018-0425_PT.pdf; (8) Resolução do Parlamento Europeu, de 15 de janeiro de 2019, sobre a condução autónoma nos transportes europeus (2018/2089(INI)), ... *supra*.

71 Cit. P. M. Freitas, Veículos Autónomos e "Inteligentes" ... *supra*, 13.

72 Cit. P. M. Freitas, Veículos Autónomos e "Inteligentes" ... *supra*, 12.

Atualmente, os VA'I' circulam já nas estradas nacionais e os AI-A a curto ou médio prazo serão introduzidos no mercado automóvel europeu e nacional, sucessivamente [73]. Ora, o ócio "nem, nem, nem" então em exame exprime a ataraxia exortada na necessária adoção de políticas 'neo-legiferantes' jamais à flor da máquina e por de entre o prisma condução inteligente. A semiótica da *praxis* a que ora se alude traduz-se no seguinte enunciado complexo: "nem" a lei classifica as diferentes categorias de veículos (quase) inteligentes à escala IA, "nem" os quiméricos enunciados gerais e abstratos desta conotam qualquer determinação acerca da posição que o condutor deverá assumir em razão das várias categorias correspondentes, "nem" tão-pouco se encontram reunidas as condições para, no atual estado da arte condução inteligente, se considerarem preenchidos os pressupostos de imputação de responsabilidade jurídico-penal defronte casuísticas que envolvam os VA'I', e, via *argumentum ad minus, ad maiori,* os AI-A.

A respeito do primeiro teorema – aquele que versa sobre a ausência de classificações quanto às categorias várias de veículos inteligentes - a redação atual do Decreto-Lei n.º 114/94, de 03 de maio - diploma originário que aprovara o CE -, dispõe nos seus n.^{os} 1 e 2 do artigo 11.º que "todo o veículo (...) que circule na via pública deve ter um condutor" (n.º 1), este que por sua vez se encontra investido no dever de, "durante a condução, abster-se da prática de quaisquer atos que sejam suscetíveis de prejudicar o exercício desta com segurança" (n.º 2). No Capítulo I do Título IV do CE, o artigo 106.º - cuja epígrafe versa sobre as classes e tipos de automóveis -, inexiste qualquer definição legal, quer de veículo parcialmente autónomo (o VA'I'), quer de agente inteligente automóvel (o AI-A), nem tão-pouco é autorizada a utilização destes agentes inteligentes em ambiente rodoviário nacional. Também o Regulamento do Código da Estrada, aprovado pelo Decreto n.º 39 987, de 22 de dezembro de 1954, dispõe no seu n.º 1 do artigo 23.º que "o lugar do condutor deve estar colocado de forma a permitir que este disponha de boa visibilidade e maneje todos os comandos com facilidade e sem prejuízo da vigilância continua do caminho". Atentos os enunciados *ante* plasmados, não se nos afigura qualquer verosimilhança dos conceitos legalmente consagrados para com realidades emergentes como os VA'I' e AI-A, cumulativamente. E não se ouse de modo algum alvitrar subsumir os AI-A ao conceito de produto, *qua tale* previsto no artigo 3.º

73 "Nos próximos anos, estarão comercialmente disponíveis veículos totalmente autónomos ou altamente automatizados (...), (7) Parlamento Europeu, *Relatório sobre condução autónoma nos transportes europeus ... supra,* 8 (Ponto 19).

do Decreto-Lei n.º 383/89, de 06 de novembro, redação atual, segundo o qual "entende-se por produto qualquer coisa móvel". Na esteira da douta Professora Doutora Ana Isabel Lois Caballé, também os autores do presente escrito consideram que o enunciado legal não deve ser entendido como uma definição, ao invés, o seu teor materializa uma "indicação de classes (...) que (...) acaba por ser insuficiente e perigosa [74] pelo simples facto de não designar que tipo de bens estão abrangidos" [75] (sublinhado, a título de acrescento, nosso). Já o Parlamento Europeu observara em 2018 que "as atuais regras em matéria de responsabilidade, nomeadamente a Diretiva 85/374/CEE do Conselho, de 25 de julho de 1985 – transposta para o ordenamento jurídico português pelo Decreto-Lei n.º 383/89, de 6 de novembro, *supra* -, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros em matéria de responsabilidade decorrente dos produtos defeituosos (Diretiva relativa à responsabilidade decorrente dos produtos) (...) não foram desenvolvidas para abordar os desafios colocados pela utilização de veículos autónomos e salienta que existem dados crescentes que demonstram que o atual quadro regulamentar, especialmente no que diz respeito à responsabilidade (...)" [76] . Ora, na medida em que o software dos AI-A ou dos VA'I' comunga uma sequência de instruções, formuladas numa notação linguagem-máquina, que especificam com a ambiguidade e imprecisão típicas das técnicas de inteligência computacional (*soft computing*) [77] a multiplicidade de ações pretendidas em ambiente estradal, consubstanciam bens incorpóreos ou imateriais que não são considerados em si mesmo abrangidos pela noção de produto [78]. Portanto, no

74 Esta definição é perigosa, porquanto - na qualidade de norma não autónoma e não completa que há-de integrar e ser complementada por outras disposições legais – constitui hipóteses a que se ligam consequências jurídicas, designadamente em matérias de responsabilidade civil e penal quando da ocorrência de danos que configuram a afetação de bens jurídicos pessoais. Ora, esta falta de consideração de uma inteligência sintética para os carros supõe a reserva tradicional de que, mais uma vez, em e no direito, *omnis definitio periculosa*. Cf. J. Batista Machado, Introdução ao Direito e ao Discurso Legitimador, Almedina, Coimbra, 2017, 192, 110-111.

75 Cit. numa abordagem mais abrangente sobre as matérias de responsabilidade, V. L. P. Coelho, Responsabilidade do produtor por produtos defeituosos, "Teste de resistência" ao DL n.º 383/89, de 6 de novembro, à luz da jurisprudência recente, 25 anos volvidos sobre a sua entrada em vigor, *in Revista Eletrónica de Direito (RED)*, n.º 2, 2017, 14, https://dialnet.unirioja.es/servlet/articulo?codigo=6425866.

76 Cit. Parlamento Europeu, *Relatório sobre condução autónoma nos transportes europeus ... supra*, 8 (Ponto 20).

77 *Vide*, C. Analide e D. Morgado Rebelo, Inteligência Artificial na era *data-driven... supra*, 69-73.

78 Cit. V. L. P. Coelho, Responsabilidade do produtor por produtos defeituosos, "Teste de resistência" ... *supra*, 16. "A responsabilidade do produtor por bens defeituosos ou perigosos confina-se às coisas móveis, nos termos em que são definidas pelo direito comum, ou seja, de acordo com o disposto nos artigos 204.º e 205.º do CC", cit. S. A. de Sousa, *A Responsabilidade Criminal pelo Produto e o Topos Causal em Direito Penal – Contributo para uma proteção penal de interesses do consumidor*, Coimbra Editora, Coimbra, 2014, 105. Ora, como veremos, *infra*, o AI-A não são não deverá de ser considerado como coisa nos termos

que à condução inteligente concerne, ostenta-se não ser boa a prática que espelha uma assimilação fictícia de realidades ou posições factuais manifestamente diferentes - como sejam, a condução humana, a circulação quase-inteligente e aquela outra de maior vanguarda preconizada por agentes inteligentes, ao regime da responsabilidade criminal ou até mesmo civil pelo produto defeituoso [79].

Conclui-se, portanto, que não se pode ficcionar sujeitar os utilizadores finais ou os fabricantes dos veículos inteligentes ao regime jurídico sancionatório tradicional, o da responsabilidade por produtos defeituosos. Aqui, a *ratio* verosímil quanto à tutela ou proteção da posição do consumidor não se sobrepõe ao prisma sancionatório e compensatório, que subjazem à responsabilidade civil e criminal, respetivamente [80].

Aclama-se, quanto ao segundo teorema, que no vindouro ambiente urbano de condução inteligente baseado exclusivamente em sistemas ciberfísicos ou software de Inteligência Sintética será impreterível a adoção de medidas legislativas suportadas em processos mais flexíveis e multidisciplinares, e sobretudo, mais inclusivos das partes interessadas, sejam elas, os proprietários, os fabricantes ou até, inclusive, os próprios programadores, na malha em que não deverão estas ser responsabilizadas a título sancionatório [81].

---

e para efeitos dos anteditos normativos, como ademais merecerá a qualificação de agente que perpetra delitos criminais.

79 Concordamos em discordar do ponto 11 plasmado no trabalho da Comissão de Ética do Ministério Federal dos Transportes e Infraestruturas Digitais e apresentado em agosto de 2017, aquele que aliás veio a ser contrariada no Relatório do Parlamento Europeu em 2018, acima referido. Este ponto indica que "a responsabilidade por danos causados por sistemas de condução automáticos ativados é regida pelos mesmos princípios que a responsabilidade por outros produtos", cit. P. M. Freitas, Veículos Autónomos e 'Inteligentes'... *supra*, 24. Ora, esta orientação destoa por completo daquela que é a linha de raciocínio que tem vindo a ser por nós seguida no presente escrito.

80 Cf. J. Batista Machado, op. cit., 108-109.

81 Clarividente que, no caso dos VA'I', ocorrerão casuísticas que pressuporão a assunção de controlo ou direção efetiva por parte do condutor humano, então investido na posição de vigilante. E tal cominar-se-á defronte a verificação subsuntiva dos restantes pressupostos de atribuição de penas doutrinados nos termos da Teoria Geral do Crime, designadamente no que concerne ao tipo de ilícito subjetivo, caso em que poderá ser invocada negligência na assunção ou aceitação, cujo substrato "reside essencialmente na assunção de tarefas ou na aceitação de responsabilidades para as quais o agente não está preparado, porque lhes faltam as condições pessoais, os conhecimento ou mesmo o treino necessários ao correto desempenho de atividades perigosas", Cit. F. Dias, *Direito Penal, Parte Geral, Questões Fundamentais, A Doutrina Geral do Crime*, 3.ª ed./col. Maria João Antunes, Susana Aires de Sousa, Nuno Brandão e Sónia Fidalgo, Gestlegal, Coimbra, 2019, 35.º Capítulo, §25, 1024. Mas esta sujeição deduzir-se-á somente quanto a ação por omissão, decorrente da preterição de um dever de cuidado (cf. artigo 10.º, n.º 2 do Código Penal, doravante, abreviadamente, CP, e tipos incriminadores da parte especial, Livro II CP) seja controlada ou controlável pela vontade, sobrevindo à existência de sinais objetivos de perigo e à cognoscibilidade destes por parte do agente humano. Segundo a douta Professora Doutora Maria Fernanda Palma, "a ação é (...) um critério essencial de um sistema que faz depender a responsabilidade penal de uma ideia de autonomia e de responsabilidade pessoal", cit. M. Fernanda Palma, *Direito Penal, Parte Geral, A teoria da infração como teoria da decisão penal*, 5.ª ed., AAFDL Editora, 2020, 63. No mais, só será passível de pena o comportamento que, quando enquadrado na antedita conjetura, se tem por reportado ao momento em que o agente assumiu ou aceitou o desempenho – i.e., aquele em que o condutor do VA'I' principia a viagem

Nesse mesmo sentido, o Parlamento Europeu sublinhara no dia 5 dezembro de 2018 que "é necessário criar, o mais rapidamente possível, quadros regulamentares adequados, garantindo o funcionamento seguro dos AI-A e disponibilizando um regime não ambíguo referente à responsabilidade, de modo a fazer face às alterações daí resultantes, incluindo a interação entre os AI-A, as infraestruturas e os outros utilizadores" (sublinhados, em ajuste, nosso) [82]. Sem mais delongas, assevera-se não fazer sentido, não ter qualquer sentido e ser racionalmente incongruente atribuir personalidade jurídica aos agentes de software (i.e., as vulgarizadas pessoas eletrónicas) [83], *in casu*, com materialização física de veículo automóvel e, concomitantemente, prescrever as mesmas políticas estradais que obstinam perpetuar pugnar a assunção de controlo ou direção efetiva por parte do passageiro, aquele que deverá assumir ora o *status* de utilizador final em relação aos AI-A[84–85]. Aliás, este é precisamente o motivo pelo qual o protótipo de AI-A da Google Waymo se diferencia dos restantes que se encontram à venda no mercado, propiciando-nos – a todos nós, consumidores – uma experiência verdadeiramente inteligente. As tecnologias avançadas de assistência ao condutor (i.e., com o hétero asseverado nível de automação 3), foram as primeiras a

quase-inteligente -, sabendo todavia, ou sendo-lhe pelo menos cognoscível, que para tanto lhe faltavam os pressupostos anímicos (espirituais) e/ou corporais necessários. Por exemplo, o automobilista de um VA'I' que mata um peão preenche o tipo de ilícito de homicídio negligente quando – apesar de munido com a licença administrativa necessária – se sente incapaz de dominar as situações de tráfego rodoviário altamente complexas. Recorde-se, para os devidos efeitos, que se diz ser crime todo o "facto típico, ilícito, culposo e punível, expressando um conjunto de exigências e uma ordem do juízo na apreciação de tais elementos", cit., M. Fernanda Palma, *Direito Penal, Parte Geral,* op. cit., 16.

82 Cit. Parlamento Europeu, *Relatório sobre condução autónoma nos transportes europeus ... supra,* 8 (Ponto 19).

83 O Parlamento Europeu, na Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, ainda que versando sobre as matérias de Direito Civil sobre Robótica – legitimamente extensível ao âmbito da imputação de responsabilidade criminal, nesse sentido -, instou a Comissão Europeia a explorar, analisar e ponderar, na avaliação de impacto que fizer do seu futuro instrumento legislativo, as implicações de todas as soluções jurídicas, como releva para o efeito, a criação de um "estatuto jurídico específico para os robôs a longo prazo, de modo a que, pelo menos, os robôs autónomos mais sofisticados possam ser determinados como detentores do estatuto de pessoas eletrónicas responsáveis por sanar quaisquer danos que possam causar e, eventualmente, aplicar a personalidade eletrónica a casos em que os robôs tomam decisões autónomas ou em que interagem por qualquer outro modo com terceiros de forma independente". Cf. alínea f) do ponto 59.

84 Cf. conceito geral e abstrato empregue no artigo 503.º do Código Civil (doravante, abreviadamente, CC). Para os devidos efeitos, "*a expressão direção efetiva do veículo significa ter um poder de facto ou exercer controlo sobre o veículo, independente da titularidade ou não de algum direito sobre o mesmo",* cit., L. M. Teles de Menezes de Leitão, *Direito das Obrigações,* 11.ª ed., vol. I, Almedina, Coimbra, 2014, 337.

85 Também a este respeito, o Código da Estrada alemão (*StraBenverkehrsgesetz*), inobstante ter diligenciado por apresentar os conceitos de veículos parcialmente e totalmente autónomos – carentes de alguns ajustes, como vimos, *supra*– peca por defeito. Sucede que, nos seus §1a, §1b, §1c, §63ª e §63b da 8.ª alteração, datada de 16 de junho de 2017, insiste em prescrever o assegurar a presença permanente de um condutor que possa assumir o controlo do veículo a qualquer momento, cf. P. M. Freitas, Veículos Autónomos e 'Inteligentes' ... *supra*, 21.

serem testadas pela equipa no ano de 2012. Todavia, a circulação autónoma em ambiente de autoestrada, mesmo por de entre a transição para outra faixa de rodagem, exigia sempre a assunção de controlo por parte do condutor. Na delonga da fase de testes, a Waymo também averiguou que os motoristas depositavam excesso de confiança na tecnologia, caso em que, defronte uma casuística de problem-solving a exigir o interface conducente à assunção de direção efetiva, o ser humano mais prudente não se encontraria capacitado a assumir o controlo do automóvel com segurança. À medida que os Sistemas de Assistência ao Condutor (ADAS) se tornam mais avançados, os indivíduos são frequentemente solicitados a fazer a transição de passageiro para condutor numa questão de segundos, muitas vezes em desafios complexos e em situações não antecipáveis a priori. Assim, quanto mais tarefas o veículo for responsável, mais complicado e vulnerável isto torna-se o momento de transição. Evitar este "problema de entrega" faz parte do razão pela qual o Waymo tem vindo a trabalhar em veículos totalmente inteligentes e, por conseguinte, independentes, mas não somente autónomos[86].

Deixa-se, neste seguimento, mais uma vez, um outro desafio:

- Qual seria a utilidade em 'apelidar-se' esta tipologia de automóveis no reduto da sua 'autonomia' e 'inteligência' se se perpetua obstinar exigir a assunção de controlo ou direção efetiva por parte de um condutor humano? Quais os incentivos que um consumidor teria para adquirir um AI-A?

Porque a *ratio* de tal ficção é tão-só a de procurar negar o inevitável, solucionando. Dilema da responsabilidade do modo mais fácil, assim, escapando à institucionalização de um novel Direito Penal Automatizado para os agentes de software [87], ajuizando-se renitente e erroneamente como possível a imputação de responsabilidade ao condutor humano, ao produtor do software ou fabricante do automóvel. Verifica-se mais um caso em que "o modelo de lei e de decisão que o princípio da legalidade pretende instituir funciona até certo ponto (o dos VA 'I'), mas tende a criar algumas ficções" [88] que,

86 Cf. Waymo Safety Report, ... *supra*, 13. "*Our technology takes care of all the driving, allowing passengers to stay passengers"*, cit., *... ibidem,* 13.

87 Um Direito Penal Automatizado para este tipo de agentes na IA materializar-se-ia na institucionalização de um sistema computadorizado que faz uso de informação sensorial não assistida para determinar se uma entidade virtual ou ciberfísica cometera ou premedita o cometimento de um delito criminal e, em seguida, toma uma ação de resposta, informando os órgãos policiais e judiciários de forma a sujeitar a pessoa eletrónica a penas, como sejam, a título exemplificativo, a destruição física ou reaprendizagem do AI-A. Cf. , R. Calo, A. M. Froomkin e I. Kerr, *Robot Law*, Edward Elgar Publishing, 2016, 239.

88 Cit. M. Fernanda Palma, Direito Penal, *Conceito material de crime, princípios e fundamentos, Teoria da lei penal: interpretação, aplicação no tempo, no espaço e quanto às pessoas*, 4.ª ed., AAFDL, Lisboa, 2019, 88.

realizando-se numa senda *law in action*, serão deveras desproporcionais, desnecessárias e não coadunáveis com a estrita medida, conforme aos corolários do artigo 18.º, n.º 2 da Constituição da República Portuguesa (de ora em diante, abreviadamente, CRP), sendo dirigidas sanções aos fabricantes ou as passageiros dos veículos.

Sucede que, face ao exposto, na conjuntura operante de um determinado AI-A, existindo uma afetação de bens jurídicos essenciais dotados de referente constitucional, designadamente defronte uma casuísticas inopinadas não subsumíveis ao 'Quem' dos tipos de crime homicídio (por negligência) ou ofensa à integridade física, perpetrados na forma simples ou qualificada pelo próprio automóvel – e dos quais resulte uma interferência ilegítima nos bens jurídicos vida [89] ou até mesmo na integridade física dos transeuntes humanos [90] - afigura-se uma incompletude de pendor lacunoso de terceiro nível, i.e., transcendente ao quadro teleológico da lei positiva [91]. Também todos os demais elementos hermenêuticos conducentes a uma correção no ato de interpretação das normas relativas ao CE e ao Código Penal (doravante, abreviadamente, CP), conforme ao ditames gerais artigo 9.º do Código Civil (doravante, abreviadamente, CC) – a melhor ver, o elemento literal, histórico e sistemático -, apontam não só no sentido de que a legislador nacional não diz menos do que queria dizer, como mais crítico, nem sequer preceitua aquilo que deve quanto à consideração dos AI-A na qualidade de agentes [92_93]. Embora seja consabido que o legislador penal se exprime através de palavras polissémicas, caso em que o ato subsuntivo carece de interpretação teleológica, primordialmente, *in casu*, o dos veículos inteligentes VA'I' e AI-A, não se afigura verosímil um sentido comum e literal, aquele "quadro de significações dentro do qual o

89 Cf. artigo 24.º da Constituição da República Portuguesa, de ora em diante, abreviadamente, CRP, e também, artigos 131.º, 132.º e 137.º do Código Penal (na sua redação atual).
90 Cf., artigo 25.º da CRP, e artigos 143.º e 144.º da redação atual do Código Penal, respetivamente, nas suas formas simples e agravada.
91 Cf., acerca do conceito de "Lacuna de Direito" enquanto referência à unidade da ordem jurídica, J. Batista Machado, op. cit.,192, 197-199. In casu, "a expressão lacunas da lei ou, com mais propriedade, lacunas da ordem jurídica designa a situação – carecidas de regime jurídico – que a lei ou uma norma jurídica não legal não prevê e, consequentemente, não regula", cit. A. Prata, C. Veiga, J. Manuel Vilalonga, *Dicionário Jurídico, Direito Penal, Direito Processual Penal*, 2.º vol., 2.ª ed., Almedina, Coimbra, 2014, 293.
92 Cf. J. Falcão, F. Casal, A. Sarmento de Oliveira, P. Ferreira da Cunha, Noções Gerais de Direito, 1.ª ed., Calendário de Letras, Vila Nova de Gaia, 2014, 80-84.
93 Em Direito Penal vale o princípio da proibição da analogia, conforme ao preceituado no artigo 1.º do Código, segundo o qual "não é permitido o recurso à analogia para qualificar um facto como crime, definir um estado de perigosidade ou determinar a pena ou medida de segurança que lhes corresponde". Assim, defronte casuísticas sinistrais em ambiente estradal, a partir das quais seja da incumbência do Ministério Público dar impulso a um processo na fase de inquérito, estes mesmos encontrarão um vazio legal., cf. F. Dias, op. cit., 221-227.

aplicador se pode mover e pode optar sem ultrapassar os limites legítimos da interpretação" [94].

É da incumbência, no âmbito da reserva de competência relativa da AR- conforme o consagrado nas alíneas c) e d) da *norma normarum* -, prescrever as operações levadas a cabo pelo novo 'Quem' do Direito Penal, estas que configurarão os delitos criminais ou os ilícitos de mera ordenação social que se compaginam com este tipo de realidades tecnológicas, designadamente em razão da perigosidade que ao seu funcionamento e escolhas subjaz. Para o efeito, terão de ser observados os ditames consonantes com as exigências do princípio da legalidade, designadamente na sua feição *nullum crimen, nulla poena sine lege certa* e *praevia*. Não se esqueça que à luz do n.º 1 do artigo 1.º do CP, na sua redação atual, "só pode ser punido criminalmente o facto descrito e declarado passível de pena por lei anterior ao momento da sua prática". Também o n.º 1 do artigo 29.º da *norma normarum* consagra que "ninguém pode ser sentenciado criminalmente senão em virtude de lei anterior que declare punível a ação ou a omissão (...)" [95].

Caso será para indagar que o legislador nacional, em relação a esta questão da imputação de responsabilidade jurídico-penal em particular, não quer ainda decidir-se diretamente, por displicência ou na medida em que não se sente habilitado a estabelecer para os VA'I' ou AI-A uma disciplina geral e abstrata suficientemente definida e conforme aos saberes que têm sido sinfonizados na e pela academia. As razões acima plasmadas, *supra*, parecem ser suficientemente robustas para que se possa afiançar, contrariamente aos ditames civilistas, que a imputação de responsabilidade jurídico-penal não é de modo algum suportada pelos benefícios que a utilização dos VA'I' ou AI-A pode surtir na esfera do utilizador final, ora passageiro, nem ao propósito destes últimos será colacionada a assunção do dever de guarda ou vigilância, sob a forma de omissão quando *sub judice* esteja em causa a averiguação de delitos com natureza criminal [96]. Peleja-se, assim sendo, pela adoção de uma nomenclatura mais próxima da realidade científica dos agentes de software na Inteligência Sintética, pois, só assim, conseguiremos solucionar alguns dos estraves despoletados, reprimindo os veículos nesse sentido de adotarem comportamentos desviantes.

94 Cit. F. Dias, op. cit., Capítulo 8.º, §20, 321.
95 *Vid*e, para mais aprofundamentos acerca da temática, M. Fernanda Palma, Direito Penal, *Conceito material de crime*, op. cit., 130-140; e Figueiredo Dias, op. cit., 212-213.
96 Cit. M. Fernanda Palma, Direito Penal, *Conceito material*, op. cit., 88.

A ciência do Direito Penal não pode mais 'procrastinar' os desafios despoletados pela sociedade de risco, mormente no que concerne aos desafios suscitados pelas tecnologias de ponta. Na área do Direito e Tecnologia Punitivo em especial, as partes interessadas e, em particular, o legislador têm de entender que o paradigma da regulação perpassa hoje pela decisão baseada em evidências tecnológicas autónomas, em relação às quais, a aplicação dos cânones tradicionais será deficiente [97]. O vindouro Direito Penal dos agentes inteligentes não pode mais ficar à espera de que se verifiquem resultados lesivos das condições de vida da humanidade – *in casu*, emergentes a curto ou médio prazo pela introdução no mercado de AI-A – para só então fazer intervir o arsenal punitivo. Porque "nem sempre será cristalina a determinação do responsável (...) pela atuação do agente", (omissão do termo "humano", propositadamente, e sublinhado em substituição, nosso), e algumas serão as casuísticas em que não resta se não imputar a responsabilidade ao AI-A[98]. Aqui, a cominação de sanções com características punitivas, "se quiser ser minimamente eficaz, logo relativamente a qualquer contributo significativo para o potencial de perigo do qual o resultado lesivo irá (...) derivar, por mais quotidiano e anódino que esse contributo pareça, em si mesmo considerado" [99].

É que toda esta inoperância surtirá por certo repercussões nefastas que na prática obstaculizam o estabelecimento de pontes sinergéticas pretensamente profícuas na área do Direito e Tecnologia e que, aliás, em alguns casos, tão-só abalroam a subsunção fático-normativa num beco lacunoso de pendor punitivo sem saída, do qual os órgãos judiciários não se poderão eximir por força da proibição de *non liquet* (i.e., obrigação de julgar), prescrita pelo n.º 1 do artigo 8.º do CC e [100]. Alvitramos, assim sendo, enjeitar num todo-poderoso e sem quaisquer pretensiosismos, enunciar categoricamente: mudaram-se os tempos, desconsidere-se a consciência e a vontade antropopáticas como estados antropomórficos. Conjeture-se um novel Direito Penal dos (e para os) agentes inteligentes. "Precisamos é de repensar as nossas conceções tradicionais de agência moral e consciente" (sublinhado, em acrescento, nosso) [101]. Todavia, não se baseiem as possíveis solucionar o problema de imputação de responsabilidades no prisma jurídico-

97 Cf. M. Fenwick, W. A. Kaal e E. P. Vermeulen, E. P, *Regulation tomorrow: what happens when technology is faster than the law*, *in* American Business Law Review, n.º 6, 2016, 593, https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1028&context=aublr.
98 Cit., P. M. Freitas, Veículos Autónomos e "Inteligentes" ... *supra*, 14.
99 Cit., F. Dias, op. cit., 156-157 (adaptação temática, nossa).
100 *Vide*, J. Batista Machado, op. cit., 193-194.
101 Cf. S. S. Gouveia, O Problema da Lacuna da Responsabilidade na Inteligência Artificial, *in Vanguardas da Responsabilidade*/ coor. Manuel Curado, Ana Elisabete Ferreira e André Dias Pereira, Petrony, Centro de Direito Biomédico, Faculdade de Direito da Universidade de Coimbra, 2019, 183.

penal com base na Moralidade Distribuída (MD) [102]. Porque mesmo que a moral desempenhe "um papel preponderante em fixar na regulamentação jurídica o potencial positivo destas tecnologias, ao mesmo tempo que as deve mitigar", temos para nós – mais uma vez legando como exemplo as palavras do douto Professor Doutor Diogo Freitas do Amaral que "(...) ambos os sistemas são independentes, cada um na sua esfera própria – o que não quer dizer que o Direito não possa incorporar no seu domínio regras morais. Pode fazê-lo, mas também pode impor normas jurídicas contrárias à Moral ou, pelo menos, a uma certa moral tradicional em dado país" [103]. Porque, ora em prolepse, o ardil da vindoura Engenharia do Direito conduzir-nos-á, em ensaios ulteriores, a perspetivar a operação como uma opção, um produto de um processo lógico, nele não importando o caminho que traça o ponto de chegada que se pretende alcançar. Envés, relevará o ato de escolha e o conteúdo material dos *outcomes* em conexão com os danos sofridos e, só assim, aferiremos a necessidade de adoção de medidas com características de Direito Penal. Connosco, o Direito do Século XXI ficará ancorado sob a projeção objetiva e probabilística de entidades virtuais, os agentes da Inteligência Sintética.

Em sinopse, é da nossa incumbência, jurisconsultos da Engenharia do Direito, fornecer ao legislador nacional um guião rigoroso em termos técnico-científicos acerca do modo como este deve instituir as novas políticas em áreas que imbricam o Direito na Tecnologia [104]. Engane-se quem julga abispar solucionar um problema sem previamente fundamentar a sua orientação em heurísticas que engendram saberes polímatos, aqueles que destoam e em muito daquela que é a *barbárie* exortada na e pela autopoiese jurídica, que tantas permite que se possa utilizar a "lei como instrumento de arbítrio e de poder bastardo" (sublinhado, em acrescento, nosso) [105].

102 *Vide*, L. Floridi, Distributed Morality in an Information Society, *in Science and Engineering Ethics*, nº 19(3), 727-743.
103 Cit. D. Freitas do Amaral, op. cit., 103.
104 Cf. M. Goodman, *Future Crimes, Inside the Digital Underground and the Battle for our Connected World*, Penguin Random House, London, 2015, 440 (com as devidas adaptações temáticas).
105 C. Pinto de Abreu, *Casos e Causas*, Petrony, 2016, [Sinopse].

4. AS CONSIDERAÇÕES FINAIS NO *COSMO NOVO* DIREITO PENAL DOS (E NÃO SÓ PARA OS) AGENTES INTELIGENTES AUTOMÓVEIS (AI-A)

Sinfonias autopoiéticas à parte, certo é que os AI-A circularão a curto ou médio prazo nas estradas portuguesas, a não ser que o Direito assuma – como tantas vezes sucede – as vestes acríticas, altivas e tecnofóbicas de óbice intransponível ao desenvolvimento tecnológico.

Por ora, o legislador nacional aparenta seguir quase como que uma exposição que corrobora as políticas do nada fazer. Eis que aqui urge a reiterada lógica do deixa andar e esperar por acontecer, mais-querendo procrastinar a adoção de soluções néscias aos desafios despoletados pela sociedade de risco, esta sectorialmente cada vez mais condenada ao enigma *ad impossibilita nemo tenetur*, assim se molestando os lhanos sabedores - os engenheiros informáticos -, que se veem ora em mais uma das tantas encruzilhadas exortadas pela dilação propositada de quem faz as leis. Sem revezamentos à vista, no atual estado da inércia legiferante, o campo da inteligência automóvel tem por enquanto que se reconduzir a um direito que "não é elemento, nem síntese, não é premissa de validade, nem validade cumprida, que destoa do sentido útil e viável de que o julgador deverá decidir na sua concreta realização (...). Em matérias de responsabilidade na circulação inteligente, o direito ainda não é *prius*, nem *posterius*, não é dado, nem solução, não está no princípio, nem no fim" (sublinhados, num enjeito de adaptação e a propósito nosso) [106].

Sucede que o *homo modernus* e o Direito Penal dos Agentes Inteligentes não pode mais aguardar que se verifiquem resultados lesivos das condições de vida da humanidade em detrimento de suputações probabilísticas cujo *outcome* haja sido escolhido pelos VA'I'e AI-A, para só então, numa fase ulterior, fazer intervir o arsenal punitivo, tendo assim como destinatários quem verdadeiramente opera e não quem se julga erroneamente agir. Ao propósito, invocamos o seguinte brocardo latino: *lex injusta non est lex*, porque nem sempre *ubi commoda ibi incomodda*. Mais uma vez, aclama-se de 'peito feito' que detetar problemas é depurável. Difícil será apresentar soluções otimamente combinadas sem suportar (como muitas vezes acontece) toda a argumentação em regras *communis opinio doctrum* manifestadas em instrumentos de

106 Cit. A. Castanheira Neves, *Questão-de-facto - Questão-de-direito ou o Problema metodológico da juridicidade: ensaio de uma reposição crítica*, Coimbra, Almedina, 1967, 586, http://hdl.handle.net/10316/12576 (adaptações temáticas, nossas).

arbítrio e de poder altruísta recalcado dos académicos do Direito. Caso será para asseverar, num enjeito de ajuste propositado, nosso: *ignorantia doctrum* ou *ignorantia legislatoris neminem excusat*.

Em qualquer dos talhos *ante* examinados, é indubitável que realidades digitais como aquela que ora vos apresentamos influirão no nosso quotidiano e, por certo, situações haverá em que estas interferirão no círculo da tutela de bens jurídicos fundamentais e pessoalíssimos, com rango *norma normarum,* objeto de proteção reforçada no ou pelo artigo 18.º, n.º 2, e que, aliás, serão dignos de uma 'legiferação jamais à flor da máquina'. O futuro da mobilidade automóvel verdadeiramente *smart,* aquela que prescinde na plenitude da direção antropomórfica junto ao volante, está a chegar a Portugal, mais ano, menos ano. Indubitavelmente, os AI-A operarão, não só autonomamente, mas de forma bastante inteligente (sinteticamente, articulando). É inevitável! O ato sentencioso que apresenta os AI-A por de entre a ciência punitiva não pode, não deve, nem tem de se circunscrever ao sigma consciência humana, e tão-pouco perecerá diante a moralidade distributiva das operações, *máxime*, por referência aos ultrapassados contornos antropopáticos por que são conotados. A este respeito, acompanhamos num trejeito de 'engenho' adaptativo, as reflexões tecidas pelos doutos Professores Doutores Paulo Novais e Pedro Miguel Freitas. Sucede que também aqui se pode subscrever a ideia de que, à parte do Quociente de Inteligência Sintética do agente automóvel, não se deve deixar espaço para as ficções do Direito, "da mesma forma que para voar como os pássaros, os aviões não batem as asas, pois ao contrário, levantam voo e circulam via aérea em linha plana *"* (sublinhado, a título de acrescento, nosso) [107]. Vede que estes veículos - os AI-A - não carecem de ser construídos com asas, antes de rodas, de carroçaria equipada com sistemas mecatrónicos e eletromecânicos, de hardware e de software intrínsecos que lhes conferirão – nas fases mais ou menos delongadas de simulação, treino, teste e aplicação - inteligência sintética suficiente para circularem em ambiente estradal, substituindo o utilizador final na íntegra, aponte-se. Deixam a findar, num perspetivar *outlier*, tanto os passageiros como os produtores, fora das contas neste que será o nosso – o de académicos progressistas, como sucede na Universidade do Minho - novo mote de imputação de responsabilidade jurídico-penal anti ou para-dogmática (v. próximos capítulos da série). De facto, o homem-médio, ou antes, os jurisconsultos do e no Direito Penal só perceberão isso quando prescindirem

107 Cf. P. Novais e P. M. Freitas, ... *supra,* 14.

de tentar subsumir falaciosamente a ‘operação’ (em jargão deles, ação) jurídico-penalmente relevante às aporias reinantes nos cânones tradicionais – adjetivo empregue por referência singular à ‘simbiose’ Direito e Tecnologia em setores não precavidos como este.

Julgamos, pois bem, que o rumo a seguir é dissemelhante: hoje, a institucionalização de um Direito Penal dos (e para os, mas não só) AI-A desenrola-se como um passo impreterível a ser dado. Posto isto, procurando olhar a ‘Engenharia do Direito’ de mais sítios e de sítios mais improváveis do que se tornou habitual, vislumbramos tanger o sonho do dia em que, de *jure condendo*, dos bancos da faculdade os estudantes escutarão a *poiesis* que proclama não ser Direito - e muito menos Direito Penal -, todo o conjunto de ‘instruções algorítmico-normativas’ que, embora expressando a vontade da maioria, implicam também o revés da negação do novo ‘Quem’ como Agente de Software Inteligente, *in casu*, com feição ciberfísica de veículo automóvel criminoso. Peleja-se ora conceber uma lei geral e abstrata mais inteligível, detalhada e não tecnofóbica, nesse sentido, também mais próxima de análises empiricamente concretizáveis segundo e por referência àquela que é a verdade mais material e menos *barbárie* das ciências.

REFERÊNCIAS

Analide, C., Novais, P., Machado, J. e Neves, J., Quality of knowledge in virtual entities, *in Encyclopedia of communities of practice in information and knowledge management*, IGI Global, Hershey, Pennsylvania, 2006, 436-442, DOI: https://doi.org/10.4018/978-1-59904-933-5.ch016.

Analide, C., e Morgado Rebelo, D., A Inteligência Artificial na era data-driven, A lógica fuzzy das aproximações de soft computing e a proibição de sujeição a decisões tomadas exclusivamente com base na exploração e prospeção de dados pessoais, in *Forum de Proteção de Dados*, n.º6, CNPD, Lisboa, 2019, 60-91, https://www.cnpd.pt/home/revistaforum/forum2019_6/index.html (consultado a 24 de julho de 2020).

Batista Machado, J., *Introdução ao Direito e ao Discurso Legitimador*, Almedina, Coimbra, 2017.

Brett, J. A. *Thinking local about self-driving cars: A local framework for autonomous vehicle development in the United States*, Tese de Mestrado, Universidade de Washington, Seattle, 2016,

https://digital.lib.washington.edu/researchworks/handle/1773/36852 (consultado a 21 de setembro de 2019)

Camões, Luís de Vaz, *Os Lusíadas de Luís de Camões*, 4.ª ed., Instituto Camões, Ministérios dos Negócios Estrangeiros.

Castanheira Neves, A, Q*uestão-de-facto - Questão-de-direito ou o Problema metodológico da juridicidade: ensaio de uma reposição crítica*, Coimbra, 1967, http://hdl.handle.net/10316/12576 (consultado a 26 de julho de 2020).

Chakraborty, N. e Patel, R. S., Intelligent Agents and Autonomous Cars: A Case Study, *in Internatinal Journal of Engineering Research & Technology* (IJERT), Vol. 2 (1), 2013. ISSN: 2278-0181.

Coelho, V. L. P., Responsabilidade do produtor por produtos defeituosos, "Teste de resistência" ao DL n.º 383/89, de 6 de novembro, à luz da jurisprudência recente, 25 anos volvidos sobre a sua entrada em vigor, *in Revista Eletrónica de Direito*, n.º 2, 2017, https://dialnet.unirioja.es/servlet/articulo?codigo=6425866 (consultado a 25 de maio de 2020).

Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Economico e Social Europeu e ao Comité das Regiões, de 30 de novembro de 2016, sob

o tema: "Uma estratégia europeia relativa aos sistemas cooperativos de transporte inteligentes, uma etapa rumo a uma mobilidade cooperativa, conectada e automatizada".

Corchado, E., Novais, P., Analide, C., e Sedano, J., Soft Computing Models in Industrial and Environmental Applications, in *Advances in Intelligent and Soft Computing, 5.º Workshop Internacional*, vol. 73, Springer-Verlag, Berlin Heidelberg, 2010.

Cortez, P., e Neves, J., Redes Neuronais Artificiais, Apontamentos de apoio à disciplina de Sistemas Inteligentes, Departamento de Informática, Universidade do Minho, Braga, 2010, http://repositorium.sdum.uminho.pt/bitstream/1822/158/1/redes.pdf (consultado a 18 de maio de 2019).

Costa, E. e Simões, A., *Inteligência Artificial – Fundamentos e Aplicações*, 2.ª ed., revista e aumentada, FCA, Lisboa, 2008.

Crowder, J., Friess, S., e NCC, M., Metacognition and metamemory concepts for AI systems, *in Proceedings on the International Conference on Artificial Intelligence (ICAI)*, The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2011, https://search.proquest.com/openview/7f3758944801234b137b25813441813d/1?cbl=1976349&pq-origsite=gscholar (consultado a 25 de julho de 2020).

Dias, F., *Direito Penal, Parte Geral, Questões Fundamentais, A Doutrina Geral do Crime*, 3.ª ed./col. Maria João Antunes, Susana Aires de Sousa, Nuno Brandão e Sónia Fidalgo, Gestlegal, Coimbra, 2019.

Falcão, J., Casal, F., Sarmento de Oliveira, A., e Ferreira da Cunha, P., *Noções Gerais de Direito*, 1.ª ed., Calendário de Letras, Vila Nova de Gaia, 2014.

Fenwick, M., Kaal, W. A., e Vermeulen, E. P., Regulation tomorrow: what happens when technology is faster than the law, in *American Business Law Review*, n. º 6, 2016, 561-594, https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1028&context=aublr (consultado a 12 de maio de 2019).

Fernanda Palma, F., *Direito Penal, Parte Geral, A teoria da infração como teoria da decisão penal*, 5.ª ed., AAFDL Editora, 2020.

Fernanda Palma, M, *Direito Penal, Conceito material de crime, princípios e fundamentos, Teoria da lei penal: interpretação, aplicação no tempo, no espaço e quanto às pessoas*, 4.ª ed., AAFDL, Lisboa, 2019.

Floridi, L., Distributed Morality in an Information Society, in *Science and Engineering Ethics*, nº 19(3), 727-743.

Freitas do Amaral, D., *Manual de Introdução ao Direito*, vol. I/col. Ravi Afonso Pereira, Almedina, Coimbra, Reimp., 2012.

Freitas, P. M., Veículos Autónomos e "Inteligentes" perante conflitos de interesses: uma visão a partir do Direito de Necessidade, *in CyberLaw* (CIJIC), ed. n.º V, 2018, 10-30,

https://www.cijic.org/wp-content/uploads/2018/03/VEÍCULOS-AUTÓNOMOS-E-INTELIGENTES-PERANTE-CONFLITOS-DE-INTERESSES_UMA-VISÃO-A-PARTIR-DO-DIREITO-DE-NECESSIDADE-JURÍDICO-PENAL.pdf (consultado a 13 de novembro de 2018).

Freitas, P. M., Pacheco de Andrade, F., e Novais, P., Criminal Liability of Autonomous Agents: From the Unthinkable to the Plausible, *in AI Approaches to the Complexity of Legal Systems*, Casanovas P., Pagallo U., Palmirani M., Sartor G. (eds.), AICOL 2013, Lecture Notes in Computer Science, vol 8929. Springer, Berlin, Heidelberg, 2014.

Fridman, L., Human-Centered Autonomous Vehicle Systems: principles of effective shared autonomy, in *Human-Centered AI & Autonomous Vehicles*, MIT, arXiv preprint arXiv:1810.01835, 2018, https://arxiv.org/pdf/1810.01835.pdf (consultado a 21 de maio de 2019).

Froomkin, A. M., e Kerr, I., *Robot Law*, Edward Elgar Publishing, 2016.

Goodman, M., *Future Crimes, Inside the Digital Underground and the Battle for our Connected World*, Penguin Random House, London, 2015.

Gouveia, S. S., O Problema da Lacuna da Responsabilidade na Inteligência Artificial, *in Vanguardas da Responsabilidade*/ coor. Manuel Curado, Ana Elisabete Ferreira e André Dias Pereira, Petrony, Centro de Direito Biomédico, Faculdade de Direito da Universidade de Coimbra, 2019, 171 e ss.

Hallevy, G., Liability for crimes involving Artificial Intelligence systems, in *Springer*, Cham Heidelberg, 2015.

Haugeland, J, *Artificial Intelligence: The Very Idea*, The MIT Press, Cambridge, MA, 1985.

International Transport Forum, *Automated and Autonomous Driving: regulation under uncertainty*, OECE, 2018,

https://www.itf-oecd.org/sites/default/files/docs/15cpb_autonomousdriving.pdf (consultado a 21 de setembro de 2019).

Jackson, P., *Introduction to Expert Systems*, 3.ª ed., Addison Wesley, 1998.

Kelleher, J. D., *Deep Learning*, The MIT Press Essential Knowledge Series, The MIT Press, Cambridge, MA, 2019.

Lonita, S., Autonomous Vehicles: From Paradigms to Technology, in *IOP Conference Series*, vol. 252, 2017,

http://iopscience.iop.org/article/10.1088/1757-899X/252/1/012098 (consultado a 23 de julho de 2020).

Moreira Lousa, A. J., *Veículos Autónomos e Conectados – Tecnologia e Identificação de Possíveis Alterações na Infraestrutura de Transporte*, Dissertação de Mestrado, Universidade de Coimbra, 2018,

https://eg.uc.pt/bitstream/10316/84931/1/VEÍCULOS%20AUTÓNOMOS%20E%20CONETADOS%20-%20TECNOLOGIA%20E%20IDENTIFICAÇÃO%20DE%20POSSÍVEIS%20ALTERAÇÕES%20NA%20INFRAESTRUTURA%20DE%20TRANSPORTE.pdf (consultado a 15 de julho de 2020).

Novais, P. e. Freitas, P. M, Inteligência artificial e regulação de algoritmos, *in Diálogos União Europeia*, Ministério da Ciência, Tecnologia, Inovações e Comunicações do Brasil, 2018,

http://www.sectordialogues.org/documentos/noticias/adjuntos/ef9c1b_Inteligência%20Artificial%20%20Regulação%20de%20Algoritmos.pdf (consultado a 25 de junho de 2019).

Novais, P., *Teoria dos Processos de Pré-Negociação em Ambientes de Comércio Eletrónico*, Tese de Doutoramento, Universidade do Minho, Braga, 2003.

Oliveira, A., *The Digital Mind: how science is Redefining Humanity*, The MIT Press, Cambridge, MA (2017).

Pacheco de Andrade, F., *Da contratação eletrónica – em particular, da contratação eletrónica inter-sistémica inteligente*, Tese de Doutoramento, Universidade do Minho, Braga 2008, http://hdl.handle.net/1822/10175 (consultado a 22 de julho de 2020).

Paden, B. [et.al], A Survey of Motion Planning and Control Techniques for Self-Driving Urban Vehicles, *in IEEE Transactions on Intelligent Vehicles*, 33-55,

https://ieeexplore.ieee.org/abstract/document/7490340/?casa_token=Niet16myTTwAAAAA:O8nItwarMNORQCfzjqI6RIntxXh-nRGKzPJRey9UcrPtTAY91qoMs4wH8_STIcglGgWyGAw1Gog (consultado a 18 de julho de 2020).

Parecer do Comité das Regiões Europeu, de 10 de outubro de 2017, relativo à fixação de uma estratégia europeia para os sistemas de transporte inteligentes e cooperativos [STIC] (2018/ C 054/06).

Parlamento Europeu, *Relatório sobre condução autónoma nos transportes europeus* (2018/2089(INI)), Comissão dos Transportes e do Turismo, de 5 de dezembro de 2018.

Pinto de Abreu, C., *Casos e Causas*, Petrony, 2016, [Sinopse].

Prata, A., Veiga, C., Manuel Vilalonga, J., *Dicionário Jurídico, Direito Penal, Direito Processual Penal*, 2.º vol., 2.ª ed., Almedina, Coimbra, 2014.

Relatório do Parlamento Europeu, de 23 de fevereiro de 2018, Estratégia Europeia para os Sistemas de Transporte Inteligentes e Cooperativos (STI-C) (A8-0036/2018).

Relatório da Comissão ao Parlamento Europeu e ao Conselho [COM/2016/0787 Final], de 12 de dezembro de 2016, sob o tema Salvar Vidas: reforçar a segurança dos veículos na UE Relatório sobre o acompanhamento e a avaliação dos dispositivos avançados de segurança dos veículos, a sua relação custo-eficácia e a sua exequibilidade, tendo em vista a revisão dos regulamentos relativos à segurança geral dos veículos e à Protecção dos peões e outros utilizadores vulneráveis da estrada.

Resolução do Parlamento Europeu, de 15 de janeiro de 2019, sobre a condução autónoma nos transportes europeus (2018/2089(INI)).

Resolução do Parlamento Europeu que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica [2015/2103/INL], de 27 de janeiro de 2017.

Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, com recomendações da Comissão Europeia relativamente a Matérias de Responsabilidade Civil dos Robôs (2915/2103 INL).

Ribeiro, B. A., *A Responsabilidade Legal de Veículos Autónomos, Uma Perspetiva da Ciência Cognitiva*, Dissertação para obtenção do grau de mestre, Universidade de Lisboa, 45-46, https://repositorio.ul.pt/handle/10451/39556 (consultado a 21 de junho e 2020) Russel, S., e Norvig, P., *Artificial Intelligence: a modern approach*, 3.ª ed., Prentice Hall, Edinburgh Gate, 2010.

SAE, Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, SAE J3016, 2014,

https://www.sae.org/standards/content/j3016_201401/preview/ (consultado a 21 de setembro de 2019).

Sandel, M., Justice, *What is the Right Thing To Do?*, Penguin Books, London, England, 2009.

Searle, J. R., *Minds, Brains and Science*, Harvard University Press, Cambridge, MA, 1984.

Schermer, B., Durinck, M., Bijmans, L., Juridische aspecten van autonome systemen, *in ECP.NL*, 2005,

http://www.ejure.nl/mode=display/downloads/dossier_id=156/id=251/Juridische_aspecten.pdf (consultado a 23 de julho de 2020).

Smith, B. W., *SAE levels of driving automation*, Center for Internet and Society, Stanford Law School,

http://cyberlaw.stanford.edu/blog/2013/12/sae-levels-driving-automation (consultado a 21 de setembro de 2019).

Sousa, S. A. de, *A Responsabilidade Criminal pelo Produto e o Topos Causal em Direito Penal – Contributo para uma proteção penal de interesses do consumidor*, Coimbra Editora, Coimbra, 2014.

Suppes, P., *Introduction to Logic*, Littion educational publishing, Van Nostrand Reinhold Company, 1957.

Teles de Menezes de Leitão, L., *Direito das Obrigações*, 11.ª ed., vol. I, Almedina, Coimbra, 2014.

Waymo Safety Report, *On the Road to Fully Self-driving*, Waymo, 2009, https://waymo.com/safety/ (consultado a 20 de julho de 2020).

Wooldridge, M., e Jennings, N. R., Intelligent agents: theory and practice, *in The Knowledge Engineering Review*, Cambridge University Press, vol. 10(2), 1995.

Wooldridge, M., *An Introduction to MultiAgent Systems*, John Wiley & Sons, 2002.

Yasmina Santos, M., e Ramos, I., *Business Intelligence: da Informação ao Conhecimento*, FCA – Editora de Informática, Lisboa, 2017.

CYBERLAW
by CIJIC

FAKE NEWS AND THE LIABILITY OF SOCIAL NETWORKS

DANIEL FREIRE E ALMEIDA *

* Postdoctoral researcher at Georgetown University (Washington-DC- USA) (2015-2017).
-Ph.D. in International Law, Faculty of Law, Coimbra University (Portugal- EU).
-Professor at Catholic University of Santos (Brazil) - Ph.D. and Master's Program.
-Professor and International Lawyer. -E-mails: lawyer@adv.oabsp.org.br, da616@georgetown.edu.

ABSTRACT

The main objective of this Article is to analyze the liability of digital social networks in relation to the contents known as fake news, when disseminated from their digital platforms. To this end, the Article is divided into two parts.

In the first session, it raises some of the main aspects of the digital environment, especially social networks. In the second session, on a purposeful basis, and in view of the challenges presented by fake news, address the responsibility of social networks on fake news.

Keywords: Fake News. Social Networks. Facebook. Twitter. Liability.

INTRODUCTION

The global configuration of social networks, which stand out on the Internet today, presents a digital environment that strongly represents the different segments of society.

In this context, the use of formidable programming tools (software) can attract, integrate and make enjoyable the digital life of billions of people around the world.

On the other hand, it also uses the whirlwind of information conveyed by users, duly registered in the domains of social networks, to sell highly profitable marketing services, based on the purposeful treatment of data available by users.

To achieve these goals, networks such as Facebook, Instagram, or Twitter, *in exemplis*, collect data ranging from publications, photos, videos, likes, comments, friends, events, profile information, among many others. From there, it promotes this content to other users with the initial intention of increasing even more their contacts and, consequently, their digital activities.

In this sequence, after collecting and processing the data resulting from the countless digital interactions, the management companies of the referred social networks provide this data to third parties, at high remuneration. We must mention, right now, that due to the advanced treatment of the information collected, it is possible to achieve high levels of return, making digital data a valuable asset.

It happens that, to further boost the interactions and enable the increase of data to be handled, is that social networks eventually edit content primarily served by the users, making them even more attractive. Then, they spread the information to thousands of other users, also disseminating posts, news, publications, comments, photos, likes, reactions, and videos, which fall, also, under the fake news.

Therefore, this article seeks to analyze the responsibility of social networks for the referred content called fake news.

1. THE DIGITAL ENVIRONMENT OF SOCIAL NETWORKS

The social transformations experienced today are strongly promoted by the diverse uses of the Internet and the digitization of content.

Indeed, people can opt for new forms of relationship and identification with digital, *deterritorialized* networks, of a cultural, social, professional, and political nature.

In fact, the possibilities leveraged by the Internet, of which the multiple uses of digital social networks are a recent example, are automatically connecting people and the world.

In this line, in addition to the potential and great opportunities that we find in these networks, there are implications for society, due to the profound changes in individual and collective behavior, arising from fake news, for example.

We are currently in the midst of a time of change. In this perspective, one of the most impactful and revolutionary transformations is constituted by the activities of society on the Internet.

In this sense, information technologies have been used by society to obtain, manipulate, organize, store, and transmit information in digital form.

Indeed, innovations leveraged by different uses of the Internet have brought changes in the way people relate. In fact, we are experiencing the assumptions, as well as the first impacts, of this inexhaustible source of innovation that has transformed technological development into social transformation.

In short, the Internet and digital communications are opening new paths to transform the way we live, work, learn and relate. The Internet has been a virtual space of convergence and concentration, unprecedented, of the most varied forms of information, communication, commercialization of products, services, and entertainment.

We can risk saying that if everything is not on the Internet, at some stage the subject, the product, or whatever it is, goes through the Internet. Therefore, the data transmitted by digital networks reveal habits and preferences that can, and are, used to influence users' next clicks.

The Internet revolution has changed, and continues to change, the ways in which we organize the world, how we give it meaning, how we interact, and how we look at ourselves and others.

In this context, a factor that contributes to the dissemination of information, content and contacts has been the digitization of data. The possibility of digitizing messages, information, documents, music, videos, software, has facilitated the communication between users.

Accordingly, GIDDENS argues that the traditional communication system has been replaced by integrated systems, where large amounts of information are compressed and transferred in digital format[1]. In pertinent conclusion, and as noted, the various conditions of connection increase the number of users and relationships that result from it.

We should also note that the dissemination and spreading of content transmitted over the Internet reaches levels never confronted by law, potentiating the harmful effects of false content, or fake news.

Continuing, in this line, the influence that the Internet causes in the social environment is unprecedented, when compared to any other previous means of communication.

Having said all that, it is worth emphasizing the countless possibilities of using the Internet, such as e-mail, www., texts, e-commerce, and digital social networks. Therefore, the generation of data and relationships arising from this frantic interaction contextualize a new environment, the digital environment.

Such conditions, in fact, make the contexts of interaction and communication over the Internet universal, immediate, simultaneous, and incredibly fast.

On the other hand, the resource of making information available (publishing) can be more easily performed by people. Unlike the previous restricted possibilities (tv, radio, newspaper - in the hands of a few), now anyone can have their profile, and publicize their subjects of interest, in the most varied areas, all over the world.

Messages, posts, music, videos, and images can establish communications between users across the planet. These resources have never been closer to people and companies, and in such a massive and dispersed way, as they are now. So, once again, we must mention that the search and dissemination of information and knowledge is easier with the Internet.

The biggest highlight in this segment is Google, a well-known global search engine that seeks to shorten Internet users to the task of reaching new Web sites through the world wide web. In fact, in the company's own words, Google's corporate mission is "*to organize the world's information and make it universally accessible and useful."*.

Therefore, from now on, the treatment of data is a basic activity of these companies, as mentioned above.

In continuation, for the first time in history, an ordinary citizen or a robot can, easily and at a very low cost, not only have access to information located in the most distant point of the globe, but also create, manage, post, make available and distribute digital content,

1 *Cfr.* GIDDENS, Anthony. *Sociologia*. Lisboa: Fundação Calouste Gulbenkian, 2009, p. 53.

worldwide, something that only a large organization could do previously, using conventional means of communication. In fact, technological advances leveraged by the Internet make the world increasingly one, bringing individuals and groups together through supranational relations.

Currently, many of us spend more time using new Internet services, connecting with friends on social networks like WhatsApp, Facebook, Instagram, TikTok, QQ, Snapchat, Twitter, among others.

Issues such as marketing, business, community, privacy, politics, sex, love, campaigns, are also issues that are associated with the concept of popular social media platforms. Indeed, there is a profound relationship between online communication tools and the changes in our social relationships.

All these services and utilities have revolutionized the potential for using digital information and relationships. It should be added that this phenomenon of digital social networks currently involves billions of people on the planet.

Therefore, the consequences for society promise to be profound, due to the way we live, work, learn, communicate, entertain, influence, and think.

However, it is important to emphasize that the consequences of these changes are enormous for the future of our societies, which are increasingly digital. However, it is not an evidence that it will prove to be only for good. In the context of fake news, for example, influences can lead to serious consequences.

Having said all that, we conclude that new technologies are not only tools, they form our ways of communication, and the processes of some of our thoughts, and part of our potential attitudes.

2. FAKE NEWS AND THE LIABILITY OF SOCIAL NETWORKS

Initially, at this point, we can state that the digital society is the result of activities, communications and interactions carried out by people and based on the Internet and new technologies.

So, undoubtedly, the change to the abundance of information when we decide what to read, listen to, buy, or watch on the Internet is much greater than what our parents or grandparents had without it. Before, few influences defined our culture. Now, millions of information (data) can form our culture, in a world of infinite varieties and sources.

However, in the professional selection of such influences are the digital social networks, with computer programs that are able, from the treatment and editing of data, to make content available to users.

Within this context, the transfer of information from one individual to another is crucial in any society. Digitization, in the same way, makes it possible to increase the interactive means of communication, allowing an active participation of users.

In social networks, such occurrences are constant.

In this segment, therefore, the impact, influence, and integration power of social networks are enhanced by its activities such as promoting, publishing, editing, controlling content, using data, organizing, listing, sharing, instigating, and promote users to online and offline activities.

Never in history an entity, such as digital platforms, had the power to influence users to do or stop doing something.

Therefore, the publication of an offensive rumor on a page on the social network, with due editing and control by a social network, its consequent organization, listing, promotion, instigation, and requested reaction, quickly spread through the networks, inducing an action by its users, which can lead to serious consequences.

These networks raise their large funds with the services they offer, among others (according to Facebook's "Terms of Service", *in exemplis*, such as: [2],

- "Facebook builds technologies and services that enable people to connect with each other, build communities, and grow businesses. These Terms govern your use of Facebook, Messenger, and the other products, features, apps, services, technologies, and software we offer."

2 *Vide* FACEBOOK. Terms of service. Available at: https://www.facebook.com/terms (09.11.2020).

-”We don’t charge you to use Facebook or the other products and services covered by these Terms. Instead, businesses and organizations pay us to show you ads for their products and services. By using our Products, you agree that we can show you ads that we think will be relevant to you and your interests. We use your personal data to help determine which ads to show you.” (control, Editing).

- “We provide advertisers with reports about the performance of their ads that help them understand how people are interacting with their content.” (organization, listing).

- “Our Data Policy explains how we collect and use your personal data to determine some of the ads you see and provide all of the other services described below.” (promotion, instigation, and requested reaction).

- “Provide a personalized experience for you”

- “Connect you with people and organizations you care about”.

- “Empower you to express yourself and communicate about what matters to you”.

- “Help you discover content, products, and services that may interest you”.

- “Combat harmful conduct and protect and support our community”.

- “Use and develop advanced technologies to provide safe and functional services for everyone”.

- “Research ways to make our services better”.

- “Provide consistent and seamless experiences across the Facebook Company Products”.

- “Enable global access to our services.”

It does not take much effort to denote that the referred platforms have the capacity to edit the data, controlling, editing, organizing, promoting, instigating, encouraging, asking for reactions, sharing, spreading through the network, inducing user´s actions and reactions, among others.

Therefore, the responsibility advocated in this Article is explicitly described in Facebook's terms of service, for example, by providing that:

“We use the data we have to make suggestions for you and others - for example, groups to join, events to attend, Pages to follow or send a message to, shows to watch, and people you may want to become friends with. Stronger ties make for better communities, and we believe our services are most useful when people are connected to people, groups, and organizations they care about.”.

"Your experience on Facebook is unlike anyone else's: from the posts, stories, events, ads, and other content you see in News Feed or our video platform to the Pages you follow and other features you might use, such as Trending, Marketplace, and search. We use the data we have - for example, about the connections you make, the choices and settings you select, and what you share and do on and off our Products - to personalize your experience."

In other words, the company promotes, instigates, and requests reactions based on the treatment of data.

In fact, it makes no mention of whether what it promotes is good or bad. But even so, it promotes, taking responsibility for what it does.

In continuation, we can still mention, the "**sharing status updates, photos, videos, and stories across the Facebook Products you use, sending messages to a friend or several people, creating events or groups, or adding content to your profile**".

In the same sense, sending messages instigating users to reactions, such as: "reply", "react", "share", "comment", "click". In other words: "do something" about it.

Obviously, many users actually do...

In brief summary, what seems clear is that the activities normally developed by social networks, when it comes to fake news, end up increasing the problem, causing effects for everyone, amplifying the consequences for the promotion that they do. Therefore, they must answer for that, too.

In addition to direct and objective liability, for the actions they promote in their tools, social networks, in many cases, also fail to act.

In effect, offensive publications and fake news that generate actions by its users, have not deserved, usually, activity, control, censorship, or removal by those social networks.

Therefore, they violate the "Terms of Service" of these networks by not "Combat harmful conduct and protect and support our community"[3].

It is necessary to emphasize that the control of content editing is ensured in Facebook's "Terms of Service", for example, in these words:

"Combat harmful conduct and protect and support our community:

People will only build community on Facebook if they feel safe. ***We employ dedicated teams around the world and develop advanced technical systems to detect misuse of our Products, harmful conduct towards others, and situations where we may be able to help***

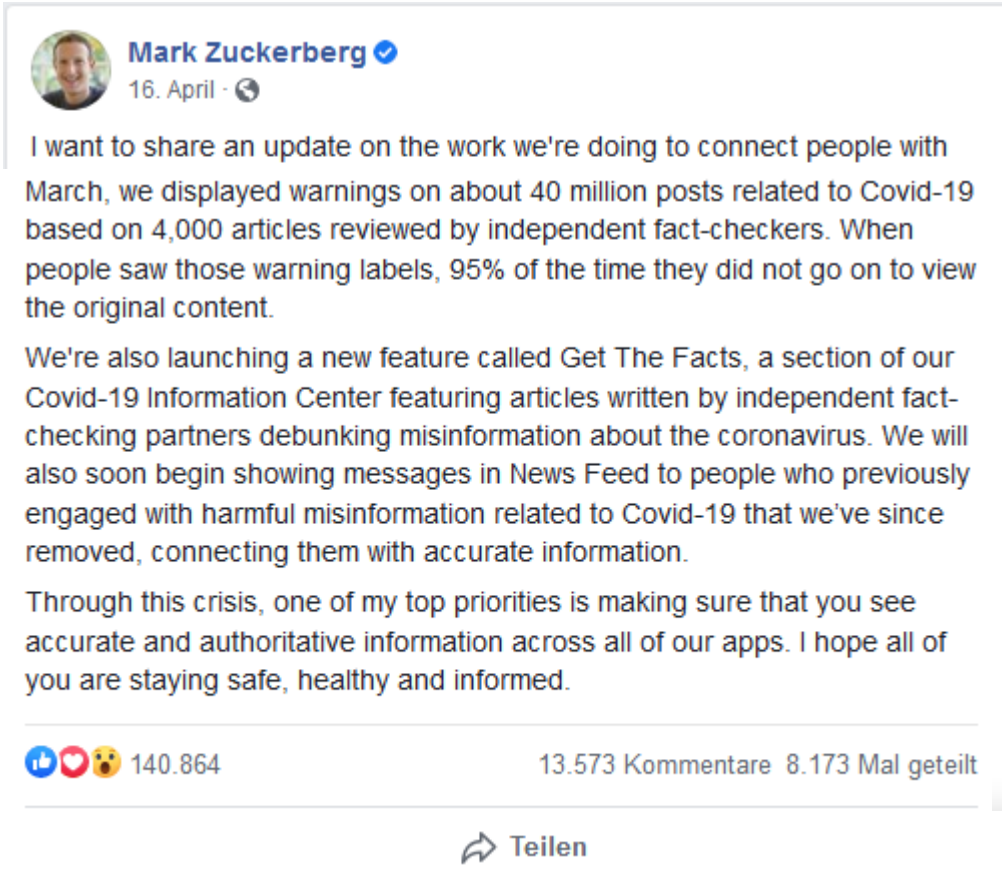
3 *Vide* FACEBOOK. Terms of service. Available at: https://www.facebook.com/terms (09.11.2020).

support or protect our community. *If we learn of content or conduct like this, we will take appropriate action - for example,* ***offering help, removing content, removing or restricting access to certain features, disabling an account, or contacting law enforcement.*** *We share data with other Facebook Companies when we detect misuse or harmful conduct by someone using one of our Products."*

Regarding social networks, in general, claim that they have not been "judicially notified" of fake news and offensive content, to do something, and in other cases that only protect the "freedom of expression", reality shows the opposite: in many cases the networks act on their own and remove famous content when they are "interested" in it, forgetting freedom of expression or any previous judicial manifestation about it.

In other words, social networks have decided what they want to remove, what they want to promote, edit, boost, list, organize, regardless of a court order. In short, they have control over the edition of the contents. They use the need for a judicial decision and freedom of expression only in what they "judge" convenient.

On this subject, the Facebook CEO, below, demonstrates the power to direct its 2 billion users to real news, and to ward off the so-called fake news.



4

4 Available at: https://www.facebook.com/zuck/posts/10111806366438811 .

The illustration above demonstrates the company's editorial power, demonstrating its ability, when it wishes, to remove content called fake news. Therefore, the social network´s liability is assumed.

Now, for all the titles, companies, such as Facebook, exercise editorial control over the contents of their digital environments. In this step, must be remembered, that Facebook itself explicitly promotes these qualities of control of the contents and data of users, to the companies that hire its services:

"We don't charge you to use Facebook or the other products and services covered by these Terms. Instead, businesses and organizations pay us to show you ads for their products and services. ***By using our Products, you agree that we can show you ads that we think will be relevant to you and your interests. We use your personal data to help determine which ads to show you."***

In the sense of the aforementioned, and corroborating what we have alluded to in the introductory section of this Chapter, is that social networks such as Facebook, Instagram or Twitter, collect data ranging from publications, photos, videos, likes, comments, friends, events , profile information, and more. From there, the networks promote this content to other users to increase their contacts and, consequently, their digital activities. Then, after collecting and processing the data resulting from the countless digital interactions, the referred social networks provide this data to third parties, at high remuneration. Therefore, to further boost interactions and enable the increase of data to be processed, it is that social networks end up editing content, first broadcast by users, making them even more attractive. Then, social networks spread the information to thousands of other users, disseminating posts, news, publications, comments, photos, likes, reactions, and videos, including fake news.

In this table below, considering what happens inside Facebook, for example, it is evident that the Company has strict liability when it transmits fake news:

Timely and necessary, the appreciation in this plan, that international jurisprudence has been gradually accepting, and insofar as they understand what networks do, the thesis that social networks are responsible for offensive content and fake news that cause damage to others.

In a direct approach, media companies have the responsibility to moderate the content when they assume in their "Terms of Service", or in fact carry out activities, in which they edit, control, organize and disseminate the content initially generated by their users, through “password” to enter the website, inside the digital environment of the companies.

What is beginning to be recognized is that social networks are responsible for entering and editing information in the first place. That is really the main difference. The current situation is that media companies are responsible not only for canceling comments or posts when they notice them, but for preventing them from uploading in the first place, or from continuing online, or even from the social networks themselves continuing to disseminate the content. This places a significantly greater burden, of responsibility, on what social networks profit, than was previously in force and understood.

In our understanding, as social networks use the pages from the perspective of their own commercial interests, they effectively assume the risks of defamatory comments, and

fake news that cause harm, made initially by their users, but controlled, promoted and edited by these networks.

FINAL CONSIDERATIONS

For everything analyzed, we found the liability of social networks on the content called fake news, when broadcast in their digital environments, duly controlled by them, through passwords.

In an identical angle to what we defend in this Article, there are the judicial positions taken, increasingly, in Australia, India, United Kingdom, United States, Germany, and France when it comes to the strict responsibility to Content Editors and controllers, such as digital social networks.

Indeed, leading Internet companies, such as Facebook, Twitter, and Instagram, are operators of social media platforms, publishers of editorial content.

If not, in fact, the platforms then offer open access and "free" of any legal and judicial limitations.

In the digital environments of networks, platforms must follow the rules and, yes, insofar as they gain the financial benefits of data processing, they must restrain criminal practices carried out within the networks themselves, managed by passwords granted by the networks (environment controlled by the networks).

If the social network controls the digital environment, then it is responsible for the same space.

No environment, however "cool", can serve to cover up, or even "leave", criminal practices to thrive, like many fake news.

Social networks have the power to transmit and process data. With that power came the responsibilities.

However, networks want to reap the financial benefits of being Content Editors and Controllers, **without being responsible**.

So, if it is true that networks have editorial power, as they decide which specific news, research results, reactions and posts will show us in our timelines (and that of all other users), among the billions of people and possibilities, then we should treat them legally as such. In other words, as responsible.

In fact, the liability must be recognized.

Freedom of speech is not above crimes. Whoever disseminates fake news and who drives fake news, must be responsible for that.

Indeed, the alleged prohibition on freedom of expression cannot be a subterfuge for the promotion of crimes.

Social networks are “no man's land”, where everyone can carry out criminal activities freely, and only after a court decision, and if there is time, something will be restrained.

For the same reasons explained above, companies can remove content - if they can do it through a court order, they can do it without the same order.

This is because, when editing the content, the networks assume the function of supervising it, under penalty of being co-authors.

Consequently, what are the “Terms of Service” for, if not to enforce them?

On the contrary, instead of controlling what is shown in their digital environments, social networks handle information, edit, control, profit and encourage reactions: “like”, “comment”, “share”. But they do not accept to be held responsible for the consequences.

Therefore, after careful analysis, we conclude that social networks are responsible for fake news, when networks disseminate the content in their own digital environments.

REFERENCES

BAKARDJIEVA, Maria. Internet Society: The Internet in Everyday Life. London: SAGE, 2005.

BRAZIL. General Data Protection Law. Law number 13.709 (08.14.2018), Available at: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm .

CARR, Nicholas G. The Big Switch: Rewiring the World, from Edison to Google. New York: Norton & Company, 2008.

CASSESE, Sabino. Regulation, Adjudication and Dispute Resolution Beyond the State. Heidelberg: Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht, Fall, 2008.

CASTELLS, Manuel. The Internet Galaxy: Reflections on the Internet, Business, and Society. Oxford: Oxford University Press, 2003.

COUNCIL OF EUROPE. Convention on Cybercrime, Budapest, 2001.

DIXON, Helen. Regulate to Liberate. Can Europe Save the Internet? New York: Foreign Affairs. September 19, 2018. Accessed September 19, 2018. Available at https://www.foreignaffairs.com/articles/europe/2018-08-13/regulate-liberate .

DRAETTA, Ugo. Internet et Commerce Électronique en Droit International des affaires. Paris: Forum Européen de la Communication, 2003.

DUTTON, William. Social Transformation in an Information Society: Rethinking Access to You and the World. Paris: United Nations Educational, Scientific and Cultural Organization, 2004.

FACEBOOK. Terms of service. Available at: https://www.facebook.com/terms (09.11.2020).

FREIRE E ALMEIDA, Daniel. A Global Digital Society. LAWINTER REVIEW, v. VII, p. 458-498, 2016.

FREIRE E ALMEIDA, Daniel. An International Tribunal for the Internet. São Paulo: Almedina, 2016.

FREIRE E ALMEIDA, Daniel. International Law under a New Digital Dimension. CIFILE- JOURNAL OF INTERNATIONAL LAW (CANADA), v. I, p. 001-008, 2019.

FREIRE E ALMEIDA, Daniel. The Taxation of Electronic Commerce in The United States of America And in The European Union. 1. ed. São Paulo: Almedina, 2016.

FREIRE E ALMEIDA, Daniel (Org.). Os Cybercrimes na Perspectiva do Direito Internacional na Internet. 1. ed. New York: Lawinter Editions, 2020.

GIDDENS, Anthony. Sociologia. Lisboa: Fundação Calouste Gulbenkian, 2009.

GOOGLE SPAIN SL AND GOOGLE INC. V AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ, Available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=153853&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=380763 .

INTERNATIONAL TELECOMMUNICATION UNION- ITU. Digital.life. Genebra: ITU, 2006.

KHOR, Zoe, MARSH, Peter. Life online: The Web in 2020. Oxford: The Social Issues Research Centre, 2006.

LESSIG, Lawrence. Free Culture. How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity. New York: The Penguin Press, 2004.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons regarding the processing of personal data and on the free movement of such data. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=PT .

SEGAL, Adam. When China Rules the Web. New York: Foreign Affairs. September 19, 2018. Available at https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web .

THE FOUNDER TREATY OF AN INTERNATIONAL TRIBUNAL FOR INTERNET, in FREIRE E ALMEIDA, Daniel. An International Tribunal for the Internet. São Paulo: Almedina, 2016.

UERPMANN-WITTZACK, Robert. Internetvölkerrecht. Archiv des Völkerrechts, Volume 47, Number 3, September 2009.

UERPMANN-WITTZACK, Robert. Principles of International Internet Law. German Law Journal, Volume 11, nº 11, 2010.

CYBERLAW by CIJIC

THE BRAZILIAN OPEN BANKING, THE EUROPEAN PSD2 DIRECTIVE & COMPETITION IN THE BRAZILIAN PAYMENT SERVICES MARKET

ULISSES DE ARAÚJO GAGLIANO *

* Assistant Professor at the Faculty of Law, University of Lisbon; PhD student in Historical-Legal Sciences at the Faculty of Law of the University of Lisbon. Lawyer.

ABSTRACT

BACEN instituted Resolution nº 1, of 12 August 2020, which creates its own payment arrangement for the Open Banking market called "PIX". In this Resolution, BACEN is the "payment arrangement institute" itself – however, it would be up to BACEN to encourage new market entrants and promote competition in the sector. More importantly, BACEN, as a regulator and federal authority, does not have the competence or legal authorization to operate in the private market and license the PIX brand as an exclusive private brand: Resolution nº 1, of August 12nd, 2020, creates a public monopoly of dubious legality. Most worrying is that BACEN will have, within the scope of this monopoly, an "advisory committee" formed by the large Brazilian financial conglomerates and large technology groups, to assist in the formulation of the only brand for payment service markets in Brazil. As BACEN is, at the same time, a regulator and antitrust authority for the Brazilian financial market, the PIX arrangement will be an insurmountable barrier to any other possible payment service brands, in particular medium and small enterprises. Finally, this paper offers a comparative perspective of the foregoing vis a vis the Payment Services Directives (Directive 2007/64/EC) and the Portuguese Decree Law nº 91/2018, as of November 12th, 2018.

Keywords: Payment Services; Open Banking; PIX; Payment Schemes.

Summary: 1. The Newborn Brazilian Open Banking. 1.1. Interoperability, Transparency and Cybersecurity. 1.2. Aspects related to Data Privacy. 1.3. Third Party Providers - TPP and cybersecurity policies. 1.4. Brazilian Payment Arrangements Regulation. 2. Brazilian Payment Arrangement and PSD2: a brief comparison. 3. PIX – BACEN Resolution nº 1, of 12 August 2020; 3.1 Schedule; 3.2. PIX Payment Arrangement Regulation; 3.3. PIX Brand Licensing; 4. Final Considerations - Regulatory Value and Interest.

INTRODUCTION

Although in many parts of the world the concept of instant payment and open banking seems to be very a great novelty, the European experience along until the most recent Directive (EU) 2015/2366 of the European Parliament and of the European Council, as of November 25, 2015, i.e., the Revised Payment Services Directive, is a important reminder that such features were being developed in financial markets wat before 2007, namely, the than Payment Services Directives (Directive 2007/64/EC), has already set the basic regulatory structure today repeated, with some differences and different terminology, around the globe.

Our main objective in this paper is to analyze the recent system of payment on the midst of being implemented in Brazil, the so called "PIX", as a what the Central Bank of Brazil Regulation ("BACEN") defines as a "payment arrangement" which rules were defined by the BACEN itself. The main oddity of the PIX is the fact that it is payment arrangement settled and approved by the BACEN, whereas both in the Brazilian regulation and legislation, market practices and traditions, as well as the PSD2, a monetary authority should restrain itself from providing payment systems, whenever such provision conflicts with the regulator inbuilt purpose and activities.

Moreover, we will verify that the Brazilian financial system legislation is, as a matter of fact, even more strict than the PSD2 regulation, and the BACEN actually has no constitutional or legal grounds to deploy the PIX as system payment to be marketed and licensed under contractual private law. For example, in Portugal, the definition of a "payment scheme" under Decree Law nº 91/2018, as of November 12th 2018, article 2 (gg): "*payment scheme means a single set of rules, practices, standards and/or*

implementation guidelines agreed between payment service providers for the execution of payment transactions across the Union and within Member States, and which is separated from any infrastructure or payment system that supports its operation".

Before commenting over the PIX, we will explore the Brazilian *Open Bank* regulation and the payment services regulation, set a brief comparison of its institutes with the PSD2, and then apply the preliminary finding over the PIX itself.

1. THE NEWBORN BRAZILIAN OPEN BANKING

The Open Banking initiative in Brazil started with the Brazilian Central Banking Public Notice nº 73/2019, as of November 28th 2019 and followed the parameters already stablished in the guidelines n° 33.455, April 24th, 2019, in which *Open Banking* was considered as the "in the standardized sharing of data and services by opening and integrating information systems platforms and infrastructures, using a dedicated interface for this purpose, by financial institutions and other institutions authorized to operate by the Central Bank".[1]

Its objectives would be to increase efficiency in the credit and payments market in Brazil, as well as to promote a more inclusive and competitive business environment. These objectives must be compatible with the security of the financial system, the protection of consumers and the protection of personal data.

The draft regulatory act is built on the perspective that Open Banking is based on the sharing of data, products and services by financial institutions and other authorized institutions, at the discretion of its clients, through information systems platforms and infrastructures.

The than proposed regulation established that the largest financial institutions, in the case of those with a size equal to or greater than 1% of GDP or that exercise relevant international activity, are members of prudential conglomerates in Segments 1 (S1) and 2 (S2) (pursuant to Resolution nº 4,553, of January 30, 2017) will be required to participate in Open Banking, with voluntary participation being ensured to other smaller institutions.

Regarding the organization and governance of the institutions, the Public Notice suggests an associative governance model, in which the participating institutions agree on the number and mandate of the members of a given "strategic level", based on criteria such as: (i) the number of members financial institutions or institutions authorized by BACEN, (ii) the existence of two groups of associations with the same degree of participation, the first being composed of institutions from Segment 1 (S1), Segment 2 (S2) and Segment 3 (S3), and the second by institutions in Segment 4 (S4) and Segment 5 (S5).

1 https://www.bcb.gov.br/detalhenoticia/392/noticia

Following the public consultation of Public Notice nº 73/2019, of November 28, 2019, and the parameters and guidelines already set in the Communication nº 33.455, of April 24, 2019, the Central Bank of Brazil (BACEN) and the National Monetary Council (CMN) approved the Joint Resolution nº 01, of May 4, 2020, which regulates the so-called Open Banking in Brazil.[2]

It worth to note that the Brazilian Open Banking is largely inspired in the Revised Payment Services Directive ("PSD2"), i.e., Directive (EU) 2015/2366 of the European Parliament and of the European Council, as of November 25, 2015, as we will further explore in the second part of this paper.

In this sense, the Brazilian Open Banking is a set of rules for organizing the sharing of data and services in the financial system through the opening and integration of information. It will make possible for financial institutions, payment service providers, and other technologies applicable to the banking and financial market, to be able, with the prior consent of their clients, to grant access to their clients' financial information to Third Party Providers - TPP, through dedicated interfaces (Applications Programming Interfaces - API).

The Brazilian Open Banking aims at a means to standardize and share data and services between participating institutions, such as the transmitters, receivers, initiators of payment transactions and account holders. Thus, it is not only applicable to the Brazilian National Financial System ("SFN"), but also to the Brazilian Payment System ("SBP"), that is, payment arrangements will have to be structured in order to include its data and services sharing interface. In fact, we can expect the impact of Open Banking to be very significant among the payment services (payment initiation services, account information services or payment instrument issuance services), with numerous applications, as we have seen since 2015 in the European Union.

Resembling PSD2, the implementation of Open Banking aims at increasing efficiency in the credit and payments market in Brazil, as well as promoting a more inclusive and competitive business environment. However, these objectives must be made compatible with the cyber security premises of the CMN, the protection of consumers and the protection of personal data - topics of great relevance for this new market.

2 The Central Bank of Brazil Public Notice is available at: https://www3.bcb.gov.br/audpub/DetalharAudienciaPage?3.

The sharing of data, products and services by financial institutions and other authorized institutions is also dependent on the client's consent, which deserved special attention regarding its treatment by the participating institutions' systems platforms and infrastructures.

It should be noted that Open Banking will only be mandatory for larger financial institutions, that is, those that have a size equal to or greater than 1% of GDP or that exercise relevant international activity, members of prudential conglomerates in Segments 1 (S1) and 2 (S2) (according to Resolution nº 4,553, of January 30, 2017). The remaining smaller institutions have their voluntary participation ensured.

The BACEN will have total interference and participation in the structuring of the governance model to be adopted by Open Banking participating institutions, which is an alteration in relation to the draft submitted to public consultation: the Article 46 of the Joint Resolution nº 01 establishes the BACEN duty to establish the initial structure responsible for the governance of the implementation process of Open Banking in Brazil, which must be followed, necessarily, by the participating institutions when preparing the sharing convention regulated in art. 44 of the Resolution. This strong regulatory presence, however, must be followed by the promotion of public discussions between the participating institutions, through industry unions and associations.

Among BACEN's concerns in relation to the governance model to be implemented, we could highlight the need for (i) participating institutions and industry segment representation and plurality, (ii) non-discriminatory access, (iii) conflicts of interest mitigation, and (iv) sustainability, which evidently depends on its practical feasibility with the final consumer, as well as the integrity of the system, which must prevent possible security breaches, loss or theft of data, and fraud in general.

It is important to remember that during the public consultation, BACEN made it clear that the organization and governance of the institutions would follow an associative/representative governance model, in which the participating institutions should agree on the number and mandate of the members of a given "strategic level" based on specific criteria, such as: (i) the number of associated financial institutions or authorized institutions by BACEN, (ii) the existence of two groups of associations with the same degree of participation, the first being composed of segment 1 institutions (S1), Segment 2 (S2) and Segment 3 (S3), and the second by institutions in Segment 4 (S4) and Segment 5 (S5).

This governance model would also establish the prohibition of simultaneous participation in the two groups mentioned above and the majority representation by a single association in each of the groups, and would also establish other suggestions for self-regulation like governance and cost sharing provisions. These prescriptions, however, are not contained in the Open Banking Resolution, and will be implemented based on the aforementioned Article 46, through the Convention regulated in Article 44.

1.1. Interoperability, Transparency and Cybersecurity

Among the modifications of the draft submitted to public consultation in November 2019 and the published Resolution, there is a better adequacy to the information security rules, according to both the Brazilian Data Protection General Law (LGPD) and CMN Resolution nº 4,658, of April 26, 2018 - but not only. The Joint Resolution nº 01 requires non-discriminatory treatment and interoperability between systems.

These concerns were already present in the draft submitted to public consultation, however, interoperability lacked additional guarantees, since there is not always reciprocity, that is, an institution with its own network does not always allow access to other networks. Thus, reciprocity was established as a premise for the implementation of Open Banking and will be observed as in the parameters of the Convention of art. 44.

Another additional guarantee is the principle of data quality, inserted as a premise to be observed by the market, which must be seen both from the perspective of information integrity and security, as well as a requirement for updating and consistency of databases - therefore, it is also a concern with data standardization.

Sharing requirements are conditioned by criteria of security, agility and convenience. Article 23 also began to demand greater systemic transparency, as data sharing interfaces must ensure their free access to the public, with the possibility of defining limits for interface calls, under justified and equitable parameters.

Thus, information about the APIs must be made available in a clear manner, appropriate to the nature of the sharing and accessible, including regarding version control and connection support.

The BACEN regulation follows a global trend, and will result in greater vulnerabilities and threats within the market, given the high usage of APIs in public networks with SFN and SBP, that is, more complexity, dynamism and innovation in

these markets means more risk. From the technological point of view, it is important to emphasize that Open Banking Joint Resolution nº 01 is absolutely interconnected with CMN Resolution nº 4,658, of April 26, 2018 ("Brazilian Information Security Regulation"). And more, as Open Banking encompasses not only entities authorized under the SFN and SBP, other companies and entities will eventually have to adopt minimum cybersecurity levels to remain or enter the banking, financial and payment industries.

In particular, this generalizing trend of information security practices can be noted, as Joint Resolution nº 01 ensures the standardization, integrity and availability of data transmitted via API within the scope of Open Banking through the aforementioned Article 44 Convention, regarding the "technological standards and operational procedures" to be adopted by the industry. Participating institutions must agree in this Convention, at a minimum, the implementation of the APIs, including the interface design, the protocol for data transmission, the format for data exchange and the access controls to the interfaces and data, standards and certificates of security measures to be adopted, as well as for the request to share data and services.

This standardization should be detailed in terms of standardizing the layout of the data and services, including the definition of the common data dictionary and similar data clustering processes. Without prejudice to the freedom granted to market agents to establish the standardization parameters, in Circular nº 4,015, of May 4, 2020[3], BACEN already delimits the data and services that will be the object of treatment through Open Banking.

In addition, the Convention must establish industry rules for the other legal aspects of its relationship, such as (i) channels for forwarding customer demands, (ii) procedures and mechanisms for handling and resolving disputes, (iii) reimbursement situations among participants, (iv) repository of participants, (v) rights and obligations of participants, and (vi) among others.

3 Provides for the scope of data and services of the Open Financial System (Open Banking). Its article 2 sets, for example, that the data on the service channels shared under the open banking systems, covers, at a minimum, the mandatory disclosure of certain data and certain electronic channels. It aims at allowing uniformity through the public system, regarding, for example account typology and tariffs to be charged.

The convention will be negotiated and structured by entities representing the participating institutions and segments and may be adhered to directly by the institutions (individually) or by their unions or national associations.[4]

1.2. Aspects related to Data Privacy

Consent

There is a clear concern by the regulator to equalize the requirements of technological innovation and greater market competitiveness with the guarantees of cyber security and data protection, when establishing consent as a prerequisite for data sharing. In this sense, it can be seen that the very definition of consent provided for in Joint Resolution nº 1 is more restrictive than that contained in the LGPD, with 5 articles – articles 10 to 15 – being reserved only to address the rules applicable to consent. According to Joint Resolution nº 1, consent is defined as the free, informed, prior and unequivocal manifestation of will, made by electronic means, by which the customer agrees to share data or services for specific purposes.

The Joint Resolution nº 01 reinforces the role of consent and is in line with international industry practices and with recent international ones regarding the treatment of consent. Thus, Joint Resolution nº 01 establishes that not only is the use of subscription contracts or forms for contracting data sharing prohibited, but the adoption of the opt-out system was also prohibited. Thus, consent must be established actively ("opt-in"), and using authentication systems for security and user identification. However, there is no indication of specific mechanisms or forms of authentication. The strong authentication is one of the innovations brought by the PSD2, it worth commenting the banking and financial markets in Brazil have long adopted quite sophisticated means for authentication.

It should be noted that Joint Resolution nº 01 also sought to establish the time limits for both the exercise of consent and its revocation. Article 15 ensures "the possibility of revoking the respective consent, at any time, upon the client's request, through a safe, agile, precise and convenient procedure, observing the provisions of the legislation and regulations in force".

4 This convention seams as way to mimic the market soft regulation that resulted in the PSD, with the difference that Brazilian financial market is far from reaching the same diversity of the EEA initial effort.

The revocation of consent must take effect within 1 (one) day, counted from the client's request, in the case of sharing the payment transaction initiation service, and immediately, for the other cases.

It is interesting to note that, although the Regulation establishes the revocation of consent, it is silent on the right of rectification, so necessary to ensure that the information transferred is correct and accurate. On the other hand, although it does not refer directly to the right to rectification, the inclusion of the data quality principle, mentioned above, is an indirect form of reference to the right to rectification (which is also regulated in the LGPD).

Finally, consent may be opposed by participating institutions whenever there is a justified suspicion of fraud.

Purposes

The Regulation correctly limit the sharing under specific purposes and allow the customer to control the data clustering. In this sense, it is important to note that participating institutions may or may not choose to cluster data. Evidently, the clustering must necessarily be consented, as part of the transferred data treatment.

Such consent must be requested through clear language, aim at specific purposes, and have a validity period compatible with the purposes, limited, however, to 12 months.

Articles 30 and 31 provide for the institutions' responsibility for data security, however this responsibility is already provided for in specific legislation.

There is also a regulatory obligation to hire a statutory Director, who can accumulate other functions, and who will have the institutional function of supervising the transmission process and ensure its reliability.

1.3. Third Party Providers - TPP and cybersecurity policies

A very important aspect of the Regulation is the recognition of the TPPs (referred to as partner companies) broad role in an Open Banking environment. They will perform numerous services associated with the financial and banking market, notably related to payment services, as has occurred in other jurisdictions. With the entry into force of Joint Resolution nº 01, these entities will be subject to BACEN regulations, in particular CMN Resolution nº 4,658, of April 26, 2018, which already provides for the mandatory implementation of cybersecurity policy, as well as requirements for the contracting of data processing and storage and cloud computing services.

Thus, TPPs should, in the very near future, adopt procedures and controls that include, at a minimum, authentication, encryption, intrusion prevention and detection, of prevention information leakage, periodic testing and scanning for vulnerability detection, protection against malicious software, the establishment of traceability mechanisms, access controls and segmentation of the computer network and the maintenance of backup copies of data and information – practices specified in their respective policies and extendable to their own suppliers (applications and components in particular).

As the Resolution allows the hiring of foreign TPPs directly, and as several jurisdictions already have very complete information security policies, it is extremely important to raise the awareness of the Brazilian national market to its update in view of the new criteria, which will overflow from SFN and SBP to others downstream and upstream industries.

There are limits to the performance of TPPs, insofar as the Resolution provides: (i) the prohibition of contracting between financial institutions, and (ii) the prohibition of total assignment of activities, that is, the transmitting institution must be maintained at all times as direct participant in the sharing process, being able to only subcontract the other authorized activities.

In the same way that privacy and data protection has gained a prominent role in recent years with the advent of the Internet Regulation, the BACEN and CMN Regulation, and finally through the edition of the LGPD, as occurred in other jurisdictions, Joint Resolution nº 1 already indicates that, in addition to SFN and SBP, national markets should already begin to be concerned with their cyber security practices and policies, otherwise they will be excluded from the market.

1.4. Brazilian Payment Arrangements Regulation

The previous topics allowed us to set a clear understanding of the Open Bank regulation in Brazil as, actually, a *payment services* regulation, with considerable similarities to the PSD2, as we will further discuss in the next topic. In any case, before advancing in our argument, it is necessary to set the basic terminology and structure of a payment scheme under Brazilian regulation, as it is not possible to discuss any related PSD2 and Open Banking subject without, of course, touch basis with what is undergoing in the actual market.

The Brazilian payments services framework has its own standardized terms, but they all refer to what is generally known as a "payment scheme". The existing market framework were addressed both in the PSD, evidently, and as well as in the Brazilian regulation, which we will very briefly comment below, as an introduction to the main goal of this paper, i.e., the our concern over the use of the Brazilian Regulation so called "Originator of the Payment Arrangement" (Instituidor de Arranjo de Pagamento), which is neither the PSD2 *payment* system nor the Portuguese *payment scheme*. The PSD2 payment system, is rather a fund transfer system governed by formal and standardized provisions and common rules regarding the processing, not necessarily set under regulation itself, but under the monetary authority supervision. It is related to a private set of rules, in which a "payment brand" is also defined as an essential element hereto. The Portuguese definition does not fall to far from the PSD2, as it is also a ser of rules stablished by payment service providers for the execution of payment transactions – it is also something freely set by the market agents, and further supervised by the Monetary Authority, in this case, the Bank of Portugal.

The Brazilian version does not have a self-regulation origin, on the contrary, the Open Banking in Brazil is set as means to substitute the State owned Brazilian Payment System ("SPB") owned and controlled by the Brazilian Central Bank[5]. This State-owned infrastructure centralizes and controls the procedures for processing and settlement of funds transfer operations (including foreign currency, financial assets, securities). It is formed by operators of the so-called Financial Market Infrastructures (IMF), which, since 2013, also included new players, namely, the "payments arrangements" and "payment institutions" introduced by Federal Law nº 12,865/2013[6].

Payment arrangement: Set of rules and procedures that govern the provision of a specific payment service to the public, accepted by more than one recipient ("Merchant"), (item I of Article 6 of Law 12.865 / 2013)

The "Originator of the Payment Arrangement" is defined as the legal entity responsible for the payment arrangement and, when applicable, for the use of the

5 It is true, though, that one could argue that the a centralized payment system does also exist in Europe and is a fundamental part of the payment and banking basic infrastructure – nevertheless, the Brazilian Open Bank regulation main argument upon public hearing was the replacement of traditional payment methods by instantaneous payment services – i.e., the BACEN would be releasing part of its basic payment infrastructure to create a new market – whereas the EU example seems to be the opposite, as the market set the basic rules for the PSD.

6 The law itself is very confusing statute, as it regulates several unrelated topics, including the new payment arrangements, in a bad practice of Brazilian Congress to disrupt pending political deadlocks. The diploma is available at: http://www.planalto.gov.br/ccivil_03/_Ato2011- 2014/2013/Lei/L12865.htm.

associated trademark[7]. This regulatory payment service provider does not have any equivalent in the European or Portuguese regulation, since the possibility to license a trademark or to set certain rules for a payment scheme or payment system is freely agreed among market entities and individuals, provided it is done within the limits of the applicable laws and regulations.

As per the mentioned Federal Law, a "Payment Institution" is a legal entity that provides services for the purchases and sales and transference of funds, within the scope of a *payment arrangement*, without the possibility of granting loans and financing to its customers.[8]

A Payment Account under the Brazilian legislation is the registration account held in the name of end user, used for the execution of payment transactions[9] while a Payment Instrument is the *device* or set of procedures agreed between the end user and a Payment Institution, to initiate a payment transaction[10].

The Federal Law also set the meaning of Electronic Currency, as resources stored in an electronic device or system that allow the end user to make a payment transaction[11].

Furthermore, under the Brazilian framework a three-part payment scheme is called "closed payment arrangement"[12], the Brazilian regulation defines it as the payment arrangement in which account management, issuance and accreditation are carried out:

(i) by only one payment institution, which is also the originator of the arrangement or

(ii) by a controlling payment institution or controlled by the originator of the arrangement.

As seen above, the Originator of the Payment Arrangement, as well as the need to such entity to formally obtain an authorization to its own "payments arrangement" is very different from the European model. As it describes, the Brazilian Framework seem to consider as possible different kind of payment arrangement, in such extent that it would be possible to require a prior approval from regulator – which is odd since the

7 item II of art. 6 of Law 12.865/2013.
8 item III of art. 6 of Law 12.865/2013.
9 item IV of art. 6 of Law 12.865/2013.
10 item V of art. 6 of Law 12.865/2013.
11 item VI of art. 6 of Law 12.865/2013.
12 Central Bank of Brazil Circular nº 3,682/2013; item I of Article 2 of the Attached Regulation of Circular nº 3,705/2014, and Ciruclar nº 3,886/2018.

regulation itself already set the limits and basic conditions for any payment arrangement eventually agreed among private entities.

To simplify the Brazilian framework, we can consider a three-party scheme and a four party-scheme depicted below in figures one and two:

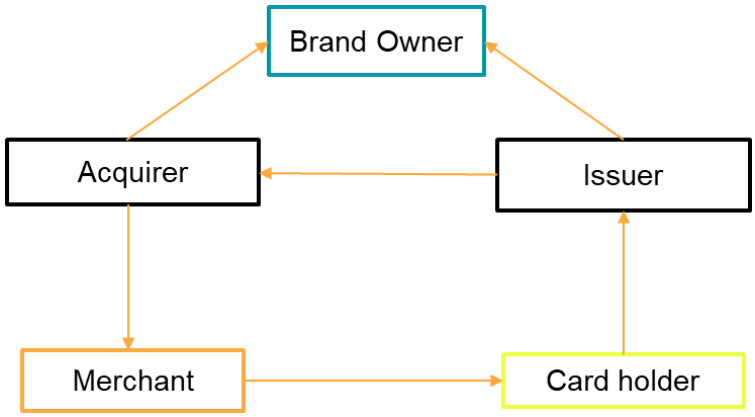


Figure one: Four party-scheme (Brazilian opened payment arrangement)

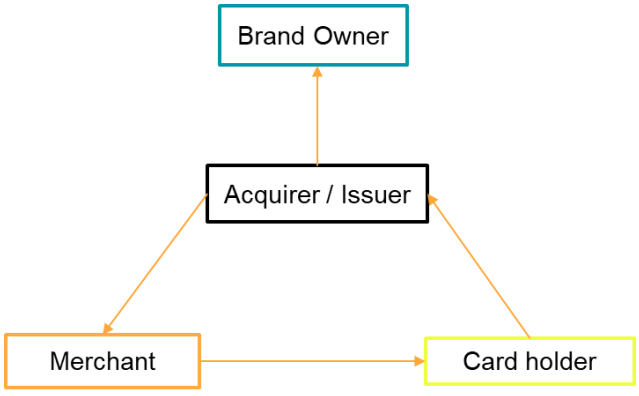


Figure two: Three party-scheme (Brazilian closed payment arrangement)

The payment institutions are the acquirer and the issuer, which can provide payment services. The Originator of the Payment Arrangement would be the Brand Owner, which licenses its brand to certain payment institutions, upon a payment of a fee.

2. BRAZILIAN PAYMENT ARRANGEMENT AND PSD2: A BRIEF COMPARISON

The Report from the Commission to the European Parliament and the Council on the application of the PSD2 on payment services, dated as of July 24th, 2013 offer us an excellent summary of the PSD and PSD2 history and implementations, most of the following remarks are direct references or transcriptions of it.[13]

The PSD entered into force on December 25th, 2007 with, with some Member States failing to achieve the then regulated deadline for its implementation, due to the need of each State Member to introduce a new compatible legal framework. Full harmonization and functionality across Europe took time, also in view of the twenty-five (25) optional provisions, meant to address each domestic market particularities.

PSD initially set four kind of entities allowed to develop payment services, which are: (i) credit institutions; (b) electronic money institutions; (c) post office giro institutions; (d) payment institutions and (e) the ECB and national central banks, when not acting in their capacity as monetary authority or other public authorities.

It is clear that PSD2 allows Central Banks and National Banks to develop payment services – provided, of course, that such practice does not conflict with its capacity of monetary authority.

PSD2 Annex I cover seven (7) different categories of payment services namely: (i) Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account; (ii) Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account. (iii) Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider: (a) execution of direct debits, including one-off direct debits; (b) execution of payment transactions through a payment card or a similar device; (c) execution of credit transfers, including standing orders.

13 REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the application of Directive 2007/64/EC on payment services in the internal market and on Regulation (EC) No 924/2009 on cross-border payments in the Community (Text with EEA relevance). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0549&from=EN

Execution of payment transactions where the funds are covered by a credit line for a payment service user: (d) execution of direct debits, including one-off direct debits; (e) execution of payment transactions through a payment card or a similar device; (f) execution of credit transfers, including standing orders; (iv) Issuing of payment instruments and/or acquiring of payment transactions; (v) Money remittance; (vi) Payment initiation services; (v) Account information services.

As viewed above, the Brazilian framework, including the very recent payment initiation service on a specific regulation called "PIX" (as will be decried bellow), refers to five (5) entities, on a much more restrict set of services, each associates with the respective entity: (i) the Originator of the Payment Arrangement is the entity responsible for setting the payments arrangement governing rules and the licensing of any trademarks associated thereto – we can relate this entity to the definition set in the PSD2 for Payment System and Payment Trademark, and correctly associated in the market to the owners of brands such as VISA, MasterCard and Diners; (ii) The Electronic Money Issuer are equivalent to PSD2 *electronic money institutions*; (iii) Issuer of postpaid payment instrument re equivalent to PSD2 *credit institutions;* (iv) Acquirer is the same as in PSD2, and (v) Payment transaction initiator is the same as in PSD2.

The Brazilian "Originator of the Payment Arrangement", which is associated to the brand or trademark used for the payment services has not equivalent in the PSD2, as already mentioned above. The Portuguese regulation also does not require a prior approval of the payment scheme, provided it does not breach the applicable laws, regulations and business rules.[14]

Also, the PSD2 has no equivalent for the term "Payment Arrangement", as something specifically created by a kind of service provider – rather the "Payment System" definition set in PSD2 as "a fund transfer system governed by formal and standardized provisions and common rules regarding the processing, clearing and/or settlement of payment transactions, along with the definition of "Payment brand" as the

14 Whereas in the Portuguese regulation, for example, as per article 151, it is clear that the payment scheme is supervised, not preapproved, as it is considered as a major offence *"the establishment of rules or provisions with equivalent effect in licensing agreements, rules on card payment schemes or agreements entered into between card acquirers and payees in breach of business rules laid down in Articles 6 and 8 (except second paragraph of paragraph 6), 10 (except paragraph 4) and 11 in Chapter III of Regulation (EU) No 2015/751 of the European Parliament and of the Council of 29 April 2015"* – although to operate as a service provider is necessary to obtain a prior licensing from Portugal Bank. There is no such a thing as the previous authorization of a payment scheme, nor in the PSD2. The Bank of Portugal has clear prudential and supervisory powers ser in articles 6 to 8 of Decree Law nº 91/2018, as of November 12th 2018.

"a term, a sign, a symbol or a combination thereof, in physical or digital form, capable of showing the card payment system under which card-based payment transactions are carried out" and, finally, Payment Multibrand, as the "the inclusion of two or more payment brands, or payment applications of the same payment brand, in the same payment instrument" reflects the fact that the SEPA and the PSD have origins in the financial markets self-regulation[15].

Not be free of criticism, the PSD2 and the Portuguese payment services regulation has a list of negative scope, on Article 3, which is a set a list of payment transactions or services to which the PSD does not apply. The EU 2019 Report consider such negative scope as would makes it difficult for consumers to figure out which activity falls under which regulatory framework.[16]

The list of negative scope comprises, for example, payment transactions made exclusively in cash directly from the payer to the payee, without any intermediary intervention; (b) payment transactions from the payer to the payee through a commercial agent authorized via an agreement to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee; (c) professional physical transport of banknotes and coins, including their collection, processing and delivery; (d) payment transactions consisting of the non-professional cash collection and delivery within the framework of a nonprofit or charitable activity; (e) services where cash is provided by the payee to the payer as part of a payment transaction following an explicit request by the payment service user just before the execution of the payment transaction through a payment for the purchase of goods or services; (f) cash-to-cash currency exchange operations where the funds are not held on a payment account, along a total of twenty four (24) exclusions.[17]

The Brazilian Payment arrangement, in this sense, is extremely more simple, as the exclusion applies only to the "the set of rules" governing the use of a payment instrument issued by a company, intended for the purchase of goods or services offered by it, is not characterized as a payment arrangement, or issued by an agency or governmental body for State purposes.

15 Report from the Commission to the European Parliament and the Council, *idem*.
16 Idem, ibdem. p.p. 3-4.
17 Article 4 of the Directive (EU) 2015/2366 of the European Parliament and of the Council, of 25 November 2015.

Low-value payments and e-money are regulated in Articles 34 and 53, setting principles for derogations over regulatory requirements and conduct of business rules for simple payment products for to low-value transactions.

The PSD provides for flexibility, as Member States can choose to reduce or double the amounts laid down in the provisions for national transactions as well as increase those amounts for prepaid instruments. Although PSD2 is concerned about prudential risk and ensure the passporting[18] rule for State Members[19].

18 These concerns are jointly referred in paragraphs 47 and 48 of the PSD2 preamble, Directive (EU) 2015/2366 of the European Parliament and of the Council, of 25 November 2015: *"(47) It is important to ensure that all persons providing payment services be brought within the ambit of certain minimum legal and regulatory requirements. Thus, it is desirable to require the registration of the identity and whereabouts of all persons providing payment services, including of persons which are unable to meet the full range of conditions for authorisation as payment institutions. Such an approach is in line with the rationale of Special Recommendation VI of the Financial Action Task Force on Money Laundering which provides for a mechanism whereby payment service providers who are unable to meet all of the conditions set out in that Recommendation may nevertheless be treated as payment institutions. For those purposes, even where persons are exempt from all or part of the conditions for authorisation Member States should enter them in the register of payment institutions. However, it is essential to make the possibility of an exemption subject to strict requirements relating to the value of payment transactions. Payment institutions benefiting from an exemption should not benefit from the right of establishment or freedom to provide services and should not indirectly exercise those rights while being a member of a payment system. (48) In view of the specific nature of the activity performed and the risks connected to the provision of account information services, it is appropriate to provide for a specific prudential regime for account information service providers. Account information service providers should be allowed to provide services on a cross-border basis, benefiting from the 'passporting' rules."*

19 The *passporting rules*, nevertheless, were not entirely accommodated and even today the PSD2 is solely in force in the EEA, as explained in the Report From the Commission to the European Parliament and the Council: "*The number of "passported" payment institutions in Member States varies greatly across the EEA. In some countries, a significant number of payment institutions applied for passports; in others, no payment institutions have sought to obtain a passport to operate abroad21. For stakeholders, "passporting" is an important feature. Competent authorities tend to apply divergent approaches. Nevertheless, the introduction of the passporting regime is a significant change and although the effects of this provision on the market have not yet been witnessed, the PSD set a stable framework for a pan-European development of payment institutions*".

3. PIX – BACEN RESOLUTION Nº 1, OF 12 AUGUST 2020

The Central Bank of Brazil Resolution nº 1, as of August 12th, 2020 ("Resolution") introduced the *PIX payment arrangement*, which, as the name indicates, is a Payment Arrangement as defined by Brazilian Federal Law nº 12.865, as of October 9th, 2013, and is not a State Owned platform or infrastructure. The confusion, however, is understandable, after all, how could the Monetary Authority act in as private market payment service provider – in particular, how could it be a Originator of a Payment Arrangement, authorized and supervised by itself?

The Article 1 of the Resolution states that: "the PIX payment arrangement is instituted", and who is its originator? Now, item I of § 2 of Article 90 of the Resolution leaves no doubt: the "Central Bank of Brazil, as the originator of the PIX".

Additionally, it is important to note that Article 3 of the Regulation attached to Circular nº 3,682, as of November 4th, 2013, issued by the Central Bank of Brazil (PIX Originator), establishes that:

"Art. 3 The Originator of the Payment Arrangement must be constituted in the country as a legal entity with a corporate purpose compatible with the institution of payment arrangements." (emphasis added)

BACEN is a federal agency, created by Law nº 4,595, as of December 31st, 1964 and bound to the Brazilian Ministry of Finance. Its internal regulations are clear in stating: "the Central Bank has the purpose of formulating, executing, monitoring and controlling monetary, exchange rate, credit and financial relations policies abroad; the organization, discipline and supervision of the National Financial System (SFN) and the Consortium System; the management of the Brazilian Payment System (SPB) and the money supply services". Still, there is no provision in Law nº 4,595,as of December 31st, 1964, that BACEN has the competence to institute a payment arrangement or act directly in the private market as a payment service provider – such as, for example, entering into a licensing agreement under a payment scheme brand.

The Resolution seems to have justified BACEN's competence to act as monopolist of a market that it regulates in the Article 10, item IV, of Law nº 4,595, as of December 31st, 1964 – It happens that such provision governs BACEN's private attribution in "receiving the compulsory deposits mentioned in the previous item and, also, voluntary deposits in sight of financial institutions", that is, it does not authorize BACEN to act as an Originator of Payment Arrangement, nor as a payment service

provider or a brand licensor in the private payment markets: it does regulate the one of the most important prudential regulatory attributions under the Basel principles.

The other legal provisions cited by the Regulation as their preamble also do not help to resolve the the conundrum: (i) Article 10 of 10.214, of March 27, 2001 establishes that BACEN (jointly with Monetary Committee and Brazilian Securities Authority - CVM) will have the competence to lower the rules and instructions necessary to comply with the regulation of clearing houses and providers of clearing and settlement services, within the scope of the Brazilian payment system, and (ii) nothing in Arts. 6th, 7th, 9th, 10th, 14th and 15th of Law nº 12,865, as of October 9th, 2013 authorizes the regulator itself to act as a Originator of a Payment Arrangement, a payment service provider, or a licensor of a service provision market brand. On the contrary, its attributions are restricted to the regulation, standardization, supervision and monitoring of the Brazilian Payment System.

Evidently, as we reviewed above, would we be able to apply the PSD2 there would be no space for discussion, as Central Banks and National Banks could only develop payment services whenever in conflict with its capacity of being a monetary authority, and of course, when authorized by law.

It is true that PIX was widely reported, since December 2018, when BACEN informed that, through Communication nº 34.085, August 28th, 2019 that it would be responsible for defining the rules for the arrangement of instant payments that came to be called PIX, "for the implementation and operation of its unique and centralized settlement infrastructure and for the set and operation of the unique and centralized database of addressing data of the arrangement". Now, the entire public debate focused on the uniform rules of a payment arrangements, and even the Public Consultation Notice nº 76/2020 raised many doubts about the mandatory nature of the PIX brand, in particular, we highlight the questions presented by the Brazilian Institute of Studies Competition, Consumption and International Trade - IBRAC.[20]

Now, one could easily accept that the Brazilian Central Bank has authority to set the governing rules for the payment service market, as, for example under Circular nº 4,027, as of June 12nd, 2020, which is perfectly compatible and adequate with the purpose or a Monetary Authority. It is, though, difficult to make it compatible with the

20 Available at BACEN website: https://www3.bcb.gov.br/audpub/DetalharSugestaoPage?10.

BACEN setting its own private brand for the private payment service market, notably as it is contrary to its own institutional interests and purposes.

The Brazilian Central Bank is not a State-Owned company, and could not, under any circumstances, develop a private activity in competition with private market agents, which are subject to the BACEN regulation. It is even worse to consider that, if PIX is to be offered as free brand, it will undoubtedly be an unbeatable *payment arrangement*: there will be no room for any new market entrant in Brazilian payment services: it seems that PIX might be a true State monopoly of dubious legality.

It is of notice to highlight that the Brazilian Financial System, unlike other Brazilian industries, has little or no interference from Brazilian Antitrust Authority Agency (CADE), in a sad chapter of Brazilian antitrust history[21]. The Central Bank is the all-powerful entity that regulates both the ex post and ex ante markets - and now, it seems, it is also a monopolist of instant payment methods.

Even though we can consider the PIX to be perfectly legal and constitutional, the singular role that BACEN intends to develop among the countries that currently have Open Banking systems is curious. It is not too much to remember that the payment arrangement most widely used in Portugal, for example, is owned by a private entity, and instituted by the SIBS Group, owner of the Multibanco brand.

Adherence to PIX is mandatory for all financial and payment institutions authorized to operate by BACEN with more than 500 thousand active customer accounts (demand deposit, savings, and prepaid accounts). From the date of publication, these institutions will have 90 days to adhere to the PIX, that is, until 11/10/2020.

Only a small portion of the market will have the freedom to join other Open Banking arrangements (if any), as this is a faculty granted to institutions below the limit.

Many payment institutions have already applied for membership in the PIX, but may reconsider this membership within 15 days of the publication of the Resolution: after this period, they must either require authorization, or they must adhere to the set of minimum regulatory standards established for the sector. This means that adherence to PIX result in regulatory cost, in any case.

21 In the judgment of merger act no. 8012.006762 / 2000-09 the authority of the competent authority responsible for analyzing and authorizing mergers in the Brazilian Financial system was questioned, being submitted to General Attorney Opinion AGU/LA-01/2001 (attached to opinion GM-020), through which it was BACEN's private competence to assess the authorization of mergers, acquisitions, merger or any merger, including transfer of share control. Left Therefore, CADE's competence to assess mergers in the Financial System is excluded.

PIX, as a payment arrangement, presupposes governance rules that are apparently democratic, and supposedly compatible with market competition, among them (art. 4) the “representativeness and plurality of institutions and participating segments”, “non-discriminatory access” and the “mitigation of conflicts of interest”. This apparent openness is contradictory to the mandatory adherence, and to the fact that the arrangement's creator is the regulator who supervises it.

Also in this sense, to the extent that PIX has a permanent advisory committee (which subsidizes BACEN in defining the rules and operating procedures), the governance structure of PIX has the following members: (i) associations representing nationwide, which are already formed by large financial conglomerates, (ii) the providers and potential providers of information technology services (Circular nº 3,970, of November 28th, 2019, provides for the requirements and prohibitions applicable to the Service Provider Information Technology – “PSTI”), (iii) clearing and settlement clearinghouses and service providers that offer liquidity provision mechanisms within the scope of PIX, and finally, (iv) paying and receiving users, through representative associations nationwide.

It is evident that the first three member groups of the committee above represent large conglomerates and economic groups, while the representative national associations of “users and payers”, because they are so dispersed, will certainly have no influence on the design of the PIX rules.

3.1 Schedule

The implementation phases of the PIX are as follows: the processes for identifying accounts subject to regulation will be carried out by a body called the “Transactional Account Identifiers Directory” or “DICT”, whose operation will start on October 5, 2020, in restricted operation, and November 16, 2020, in full operation. The PIX will start operating on November 3, 2020, in restricted operation and on November 16, 2020, in full operation.

In spite of the governance rules of the Forum carried out by the aforementioned Advisory Committee, it will be up to the Central Bank itself to detail the complementary guidelines and determinations regarding the PIX sending and receiving transaction, but that is only within a restricted transition phase – after that, the Advisory Committee will have a broader role.

3.2. PIX Payment Arrangement Regulation

PIX, as a payment arrangement, has a set of manuals and specific rules detailed in different documents to be made available by BACEN, in particular: (i) PIX Brand Use Manual; (ii) PIX Initiation Standards Manual; (iii) Cash Flow Process Manual; (iv) Minimum Requirements for User Experience; (v) SFN Networking Manual; (vi) SFN Security Manual; SFN Service Catalog; (vii) Communication Interfaces Manual; (viii) PIX Times Manual; (ix) Operational Manual; (x) Dispute Resolution Manual; and (xii) Penalties Manual.

The centralization of the PIX as an official payment arrangement of the Brazilian Central Bank will also have repercussions on the downstream and upstream markets. For example, Article 3 of the Regulation establishes that the "PIX key" and "QR Codes" will be used by DICT[22] to authenticate all transactions – this means that the provider of the PIX authentication solutions will have, in practical terms, the monopoly of this market in Brazil .

On the other hand, if there is an intention to promote competition, this resolution has not yet been made clear.

If the whole concept of Open Banking lies precisely in the opening of new markets, where the payment infrastructure centralized by the State is transferred to individuals, it is somewhat confusing that PIX is mandatory, and that the majority of its rules are set by the few existing conglomerates.

It could not even be estimated that the PIX has a limited scope to certain more sensitive transfers in the market, since it covers all possible payment transfer forms, namely: (i) purchase, based on deposit and domestic account, (ii) purchase, based on prepaid and domestic payment account, (iv) transfer, based on deposit and domestic account, and (v) transfer, based on prepaid and domestic payment account.

Regarding the procedures for executing the instant payment, the PIX admits the manual insertion of data by the paying user or the use of information sent or previously made available (reference code). Each operation will be linked to an individual or corporate taxpayer register number.

In addition, several "Identifier Code in the Brazilian Payment System" or "ISPB" will be created for each PIX participant.

22 The Central Bank of Brazil ICT Department.

PIX participants, similarly to the Portuguese SIBS Group, Multibanco brand, will be able to offer initiation of payments through a participant's main application, in terms of the number of users, which can be used by natural persons and which is accessible by cell phone.

There is also the functionality of scheduling operations, “Scheduled PIX”, for operations on future dates.

3.3. PIX Brand Licensing

Another issue present in the new Regulation is the possibility for the Central Bank to establish, through regulation, a contract for the right to use of the PIX brand, which is exclusively owned by the Central Bank of Brazil. Participants authorized for the arrangement will have a temporary, non-exclusive and non-transferable license to use the brand, in its nominative and figurative forms.

The licensing shall be regulated under Article 139 of the Brazilian Industrial Property Code (“CPI”), which means that BACEN will retain the title of a commercial brand, a trademark, for use in the payment services private markets: it is not a collective brad nor a certification mark (which would be regulated by Articles 147 to 154 of the CPI): thus, there is no doubt that the PIX brand is set to directly compete with any payment arrangement brands in the Brazilian market.

It is evident that the consolidation of the PIX brand, both due to the huge reputation that BACEN, as Monetary Authority, attributes to it, and the fact that the platform will probably be free, will prevent the creation of any competitor to PIX.

4. Final Considerations - Regulatory Value and Interest

It is true that the Resolution contains important rules for the Brazilian Open Banking market, as it is obviously adherent to the BACEN regulation: such Resolution should rather establish the minimum standards for payment service systems and schemes, rather than compete with them: the possibility of several institutions of payment services in the Brazilian market would certainly bring great benefits to the final consumers and to the economy as whole – but such effect may be considerably hindered by the PIX effect.

***