

Uma visão ponderada sobre o 5G e tecnologias relacionadas

por Miguel Vilhena

Versão de 13/10/2025

Nota do Autor

Este documento surgiu de uma investigação de cerca de 3 anos sobre a tecnologia de telecomunicações 5G e outras relacionadas, e está acompanhado de centenas de fontes (694) sobre os temas.

E embora eu não possa oferecer certeza sobre a veracidade de toda a informação contida neste documento – seriam precisos mais uns anos para exaurir todos os temas -, a quantidade e a diversidade da informação e fontes apresentadas, assim como a presença de fontes oficiais e outras com autoridade reconhecida, garantem força à crença que tecnologias mal compreendidas (como o 5G) não deveriam invadir levemente as nossas vidas individuais e coletivas, como lhes é permitido fazer publicamente.

Mas existem infinitamente mais artigos sobre o tema, que podem até oferecer uma visão diferente sobre o assunto. Pelo que apelo ao sentido crítico do leitor na apreciação desta informação, assim como de qualquer outra sobre este ou outro tema disponibilizado, independentemente do meio e da fonte de informação.

Eu permito o uso do conteúdo deste documento desde que seja acompanhado pelo contexto original. A descontextualização da informação ajuda ao engano e será prontamente refutada quando presente em contextos dolosos.

Qualquer sugestão sobre o artigo, ou o tema deste documento, ou correção, por favor usar a página <https://miguelvilhena.eu/pages/contacto.php>.

Síntese

A procura de crescimento económico e de poder governam o mundo social, e na área da tecnologia não é diferente. O bem e a segurança na saúde, no ambiente, na sociedade surge como uma preocupação geral na medida em que não prejudique as expectativas financeiras e políticas, e assegure a estabilidade social a curto e a médio prazo.

O próprio Gabinete das Nações Unidas para a Redução de Riscos de Catástrofes define a perceção de risco das elites mundiais como disfuncional, sofrendo de exagero de otimismo, subestimação dos riscos e de ideias injustificadas de invencibilidade, que, orientando decisões humanas, aumentam significativa e progressivamente os riscos a que as populações, especialmente as mais vulneráveis, estão expostas.

Assim se lançam tecnologias, como o 5G, sem um conhecimento geral bem fundamentado sobre os seus efeitos, ou até se empurram ou se deixa prosperar outras, com certezas científicas sobre os seus malefícios, mas cujos efeitos são largamente ofuscados pelos diretamente responsáveis e ignorados pelas autoridades públicas competentes (como as associadas a plataformas de redes sociais). E assim vão grassando doenças e fatalidades pela população, sem explicação.

E assim chegamos a um estado de coisas em que reina a apatia e a resignação a mudanças sociais que sentimos que não conseguimos combater individualmente, e que não sabemos bem de onde vêm e quem as força a invadir o nosso presente coletivo.

Mas qualquer mudança social para melhor necessita de conhecimento para a orientar, e assim te convido para ler este artigo. Pelo menos as partes que te interessem.

Índice

Título	Página
1 – Introdução	4
2 – Introdução à tecnologia 5G	6
2.1 – A Internet das Coisas	20
3 – Exemplos importantes do uso de radiações micro-ondas	22
4 – Risco de interferência dos serviços de 5G com as leituras meteorológicas	22
5 – Riscos de interferência com sistemas de navegação aeronáuticos	23
6 – Efeitos na biologia humana associados às micro-ondas	23
6.1 – A controvérsia à volta das entidade de avaliação do risco radiológico a nível internacional	37
6.2 – A questão da radiação emitida pelos telemóveis	42
7 – Efeitos na biologia animal e vegetal associados às micro-ondas	43
8 – Verdades e perigos do crescente vício à tecnologia	49
9 – Os problemas da privacidade online e do crime informático	65
9.1 – Os problemas da privacidade online e da videovigilância	65
9.2 – Insegurança informática	84
9.3 – O perigo da propaganda online	93
9.4 – O perigo da automatização de sistemas informáticos	96
10 – Estados Unidos versus China na arena geopolítica mundial: Huawei, ZTE, Xiaomi	103
11 – A questão económica do 5G	107
12 – Automatização de postos de trabalho e anonimização e precarização dos trabalhadores	109
13 – Uma síntese da história da tecnologia 5G	113
13.1 – A implantação da tecnologia 5G em Portugal	117
13.2 – Cronologia do avanço da instalação do 5G em Portugal	120
14 – A questão do lixo tecnológico	132
15 – Conclusões	133
16 – Apelo à consciência	135
17 – Anexos	138
17.1 – Reflexão sobre a adequação do princípio da precaução	138
17.2 – 5G e o Covid	139
17.3 – Boas práticas na navegação na Internet	141
17.4 – Boas práticas no uso de tecnologia	141
17.5 – Recomendação	143
18 - Descrição das adições de conteúdo ao documento	145
19 – Referências	163

1 - Introdução

É apresentada nos meios de comunicação e em publicidade mais frequentemente - com falsidades¹ - a nova tecnologia de comunicação móvel 5G. É a tecnologia que acabou de chegar, que vai trazer Internet móvel com downloads quase instantâneos, poderosas novas *apps*, aparelhos inteligentes (a chamada Internet das Coisas) e vai permitir interagir com as nossas casas e cidades, e informá-las das nossas necessidades e vontades, sem qualquer espécie de demora (latência).

Nas palavras da vice-presidente da Comissão Europeia – Margrethe Vestager: “Nós podemos fazer grandes coisas com o 5G. A tecnologia suporta medicina personalizada, agricultura de precisão e redes de energia que podem integrar todos os tipos de energia renovável. Isto fará uma diferença positiva.”

E se confiarmos nas reportagens dos meios de comunicação convencionais e nos artigos de fontes associadas às empresas de telecomunicações, o 5G é uma tecnologia de sonho, sem problemas dignos de serem mencionados. Só vários, fantásticos, quase inacreditáveis, benefícios.

Com benefícios previstos de hospitais inteligentes, fábricas e quintas inteligentes, casas inteligentes, estádios de futebol inteligentes – cidades inteligentes -, carros auto-dirigidos, de muito maior comodidade associada às novas velocidades de download e multimédia dos aparelhos preparados para a tecnologia 5G, e das novas áreas e oportunidades de negócio que se acredita que irão surgir, mas ainda não se sabem ao certo, a expectativa das empresas de telecomunicações, das grandes multinacionais e dos meios de comunicação é muito ambiciosa sobre as potencialidades do 5G.

O *website* [Portal5G](#) faz uma síntese de informação sobre a tecnologia 5G, e um contraponto interessante a este artigo. Maioritariamente abordando informação positiva sobre a tecnologia 5G, referindo aspetos e objetivos positivos e meritórios associados à tecnologia, mas também sem deixar de referenciar alguns aspetos menos consensuais e, pelo menos potencialmente, problemáticos. A leitura dessa fonte de informação para fazer contraponto deste artigo é recomendada, porque o esclarecimento pessoal sobre um tema surge quando somos capazes de assumir uma posição íntima informada entre os extremos em discussão.

De notar que as aplicações que para já surgem como as maiores e mais ambiciosas apostas concretas na tecnologia 5G até ao momento são o Xbox Cloud Gaming, a Playstation Now e a Amazon Luna. Estes são programas de *streaming* de videojogos para aparelhos conectados à Internet.

Também a indústria da Realidade Aumentada (Augmented Reality – AR), sobrepondo elementos de realidade virtual ao mundo real, que tem vindo a progredir e a fazer uso da tecnologia 5G já em uso. Com jogos, aplicações informativas, etc.

1 - A NOS foi condenada pela Associação da Auto Regulação Publicitária (ARP), de publicidade enganosa em relação ao 5G. Endereço do artigo sobre o facto na secção das Referências abaixo.

Outra evolução tecnológica que concentra grandes expectativas é o chamado **blockchain**, ou Distributed Ledger Technology (DLT). Que é essencialmente um registo digital ubíquo (descentralizado e distribuído) persistente que guarda o histórico sobre bens digitais. Esta invenção acredita-se que venha a afetar os serviços de pagamentos, cibersegurança e saúde.

Uma fantástica oportunidade de negócio criada a partir da tecnologia blockchain é o chamado NFT (Non-fungible token) – uma funcionalidade do blockchain do Ethereum². Um NFT é basicamente um artigo digital (imagem, música, item num jogo, etc) tornado artificialmente único com o propósito de ser cedido temporariamente pela empresa que o comercializa ao consumidor e cujos direitos atribuídos ao consumidor podem ser revendidos (com o aval e o suporte da empresa detentora dos direitos intelectuais associados), contribuindo para uma economia de artigos digitais, que se espera que gere milhares de milhões de euros, dentro de mercados de entretenimento, como música e videojogos. Pode dar azo a lavagem de dinheiro. A isto se associa a procura de criar “escassez digital” com a criação destes bens únicos digitais que podem ser transacionados comercialmente. Esta tecnologia NFT também está a ser implementado em outros blockchains, como o do TRON.

A editora de livros americana Pearson encontra nos NFTs uma solução para tomar partido no mercado da venda de livros digitais usados, ambicionando cobrar uma verba com a revenda.

Também com a tecnologia blockchain surgiram os jogos de criação de flores (CryptoFlowers), gatos (Cryptokitties) e criaturas (Axe Infinity), que permitem a criação de itens únicos com a possibilidade de os negociar, vender e trocar.

À tecnologia blockchain (na qual se inclui os NFTs) existe associado um gasto elétrico elevado na infraestrutura tecnológica necessária.

Mas a tecnologia NFT tem tido pouca aceitação comercial no público, com vários projetos com esta tecnologia falhando, pelo que parece estar a ser na generalidade abandonada.

E se a realidade virtual conquistar novos adeptos, poderemos assistir a avanços no desenvolvimento do chamado “metaverso”, uma espécie de universo paralelo online da empresa Meta.

Também a construtora de automóveis BMW começa a cobrar aos clientes microtransações para desbloquear, por software, funcionalidades já incluídas nos carros da sua marca.

Será que a tecnologia 5G é mesmo assim tão revolucionariamente positiva?

2 - O Ethereum é uma criptomoeda como o Bitcoin.

2 - Introdução à tecnologia 5G

Nós, portugueses, estamos habituados à ideia de que se uma coisa parece ser boa de mais para ser verdade, geralmente é. E a tecnologia 5G, e em especial as radiações eletromagnéticas têm particularidades que pelo menos devem ser conhecidas, porque acarretam consequências e riscos acrescidos para todos nós cidadãos, nas nossas vidas quotidianas e para os ecossistemas, a curto, médio e a longo prazo.

Como declara a FCC no preâmbulo do seu relatório de revisão do regulamento acerca da exposição humana aos campos eletromagnéticos de 2019, "O número e tipos de aparelhos de radiofrequência (RF) proliferaram, e as formas como interagimos com elas estão continuamente a mudar. Como resultado, o nosso ambiente é populado por fontes de RF, por vezes localizados em curta proximidade de seres humanos". Telemóveis, fornos de micro-ondas, aparelhos wireless e bluetooth, comandos de televisão, antenas celulares, televisões, computadores, routers...

E a tecnologia de telecomunicações 5G não irá substituir as tecnologias em uso atualmente na Internet móvel: o 4G e o 3G. Mas funcionará a par delas, mediante a disponibilização e a disponibilidade de recursos.

Só isto já dá que pensar, não dá?

Com a Internet móvel 5G pretende-se usar duas faixas do espectro eletromagnético, conhecidas como FR1 e FR2, para transmitir a informação (imagem, som, texto). A FR1 (*Frequency Range 1*, ou Faixa de Frequência 1) situa-se na mesma zona do espectro de serviços de Internet móvel 3G e 4G, atualmente em uso para a Internet no telemóvel, e em outros aparelhos sem fios ligados à Internet - mas não na conexão por Wireless -, usando frequências entre 700MHz e 6 GHz. E a FR2 (*Frequency Range 2*, ou Faixa de Frequência 2), fazendo uso de ondas eletromagnéticas na dimensão das micro-ondas de extremamente elevada frequência, com uma frequência de 24 GHz a 300 GHz (das quais as ondas com uma frequência maior ou igual a 30 GHz também são conhecidas como ondas milimétricas, pelo facto do seu comprimento de onda se encontrar entre 1 e 10 mm), para transmitir os dados.

Para contextualizar:

Agrupamento de ondas	Designação	Comprimento de onda	Frequência (ondas por segundo)	Alguns dados importantes:
	Luz visível	400 nm–700 nm	790 THz– 430 THz	Espetro do visível.
	Infravermelhos	700 nm – 1 mm	430 THz – 300 GHz	Calor, ondas sub-milimétricas.
Micro-ondas ³	EHF (Extremely High Frequency)	1 mm - 1 cm	30 GHz - 300 GHz	Ondas milimétricas. A atmosfera torna-se opaca às EHF. Pouco usadas para transmissões sem fios.
	SHF (Super High Frequency)	1 cm - 10 cm	3 GHz - 30 GHz	Wifi, UMTS, WiMAX, nova geração de telefones DECT e de variados aparelhos sem fio, radar de aviões, barcos e uso militar.
	UHF (Ultra High Frequency)	10 cm - 1 m	300 MHz - 3 GHz	Telemóveis, wifi, forno de "microondas", televisão digital e analógica, telefones DECT, variados aparelhos sem fios, Bluetooth, uso militar, satélite, radar, e muitos mais.
Ondas de Rádio	VHF (Very High Frequency) até SLF (Super Low Frequency) - ondas curtas, médias e longas	1 m - 100 000 km	30 Hz - 300 MHz	Televisão digital e analógica, rádio amador, rádio.
Sub-rádio	ELF (Extremely Low Frequency)	100 000 km - 10 000 km	3 Hz - 30 Hz	Fenómenos naturais, trovoadas, comunicação sub-aquática e subterrânea.

Tabela 1: Segmento relevante do espectro eletromagnético⁴

As mais altas frequências usadas na tecnologia 5G e um maior número de faixas disponibilizadas permitirão transmitir uma quantidade muito mais elevada de informação (devido em grande parte ao comprimento de onda progressivamente menor) assim como servir um número muito maior de utilizadores.

E a obsessão por velocidades quase instantâneas nas telecomunicações móveis obriga a que a comunicação de dados da torre celular para um telemóvel, e do telemóvel para a torre celular - por exemplo com o streaming de um vídeo (visualização a partir da Internet de um vídeo) de alta definição ou ao jogar um videojogo com uma componente online exigente se faça, quando necessário, por várias ligações em simultâneo entre a torre celular e o telemóvel, de forma a que seja possível fazer downloads de uma maior quantidade de dados (do vídeo, por exemplo), de forma a oferecer fluidez na experiência (de visualização do vídeo em alta [HD] ou ultra-alta definição [UHD]) ao consumidor.

As torres celulares 5G também incluem normalmente 32 ou 64 recetores e transmissores de rede. Sendo os 64 recetores e transmissores para zonas populacionais onde a exigência de

3 - As micro-ondas são consideradas ondas de rádio por diversos autores.

4 - Esquema baseado no diagrama de A. Cudell, 2019.

mais fiabilidade e velocidade na ligação à Internet é maior. Por exemplo, em cidades importantes.

Este facto, e a insistência das empresas de telecomunicações em usar FR2, força a que, para se ter uma instalação funcional de Internet móvel 5G, tenham de haver torres celulares muito mais próximas entre si (para oferecerem ligações móveis em toda uma área, como por exemplo, uma cidade), e mais próximas do solo (com as pequenas células a uma altura mínima de cerca de 3 metros), do que se usassem só o espaço de frequências FR1. Estas instalações deverão estar distanciadas no máximo em centenas de metros entre si para permitir a cobertura móvel, estando em consideração a sua aplicação a tampas de esgoto, de forma a melhorar a penetração da tecnologia em áreas tecnicamente mais difíceis, como áreas urbanas muito populosas, e áreas rurais com dificuldades logísticas. Assim como terão de existir instalações de Internet móvel 5G dentro de casa. Estes aparelhos estarão conectados por fibra ótica com a Internet.

Eu vou falar de seguida dos aparelhos associados à instalação 5G.

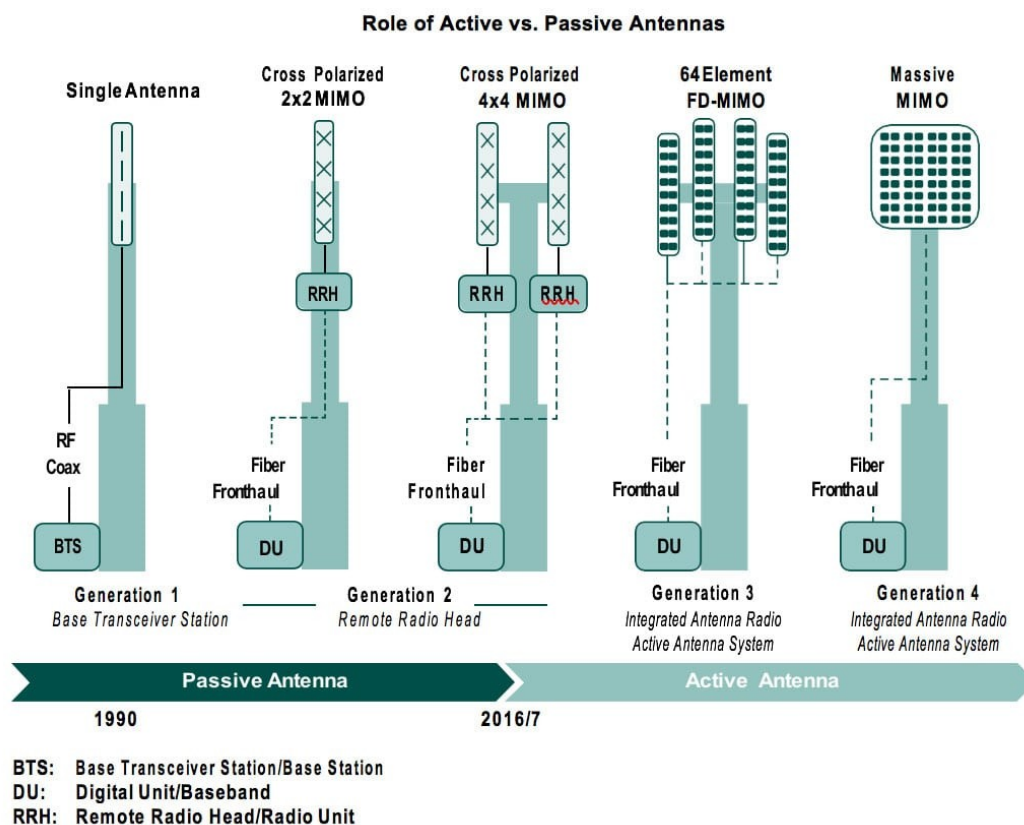


Ilustração 1: Evolução das antenas celulares

A imagem acima retrata a evolução dos tipos de antenas celulares nas últimas décadas. Está em inglês pela dificuldade em traduzir corretamente para português o nome das tecnologias, assim como pelo facto da literatura principal sobre estas tecnologias estar em

inglês. Para entender a tecnologia 5G em profundidade convém ter um conhecimento mínimo de inglês.

Uma grande mudança de paradigma na tecnologia das antenas, recentemente, foi a passagem de Antenas Passivas (Passive Antennas) para Antenas Ativas (Active Antennas). Uma Antena Ativa é uma que tem componentes eletrônicos ativos (por exemplo, transístores), não sendo composto apenas de partes passivas como a haste de metal, capacitadores e condutores. Incluídas nesta categoria estão as antenas inteligentes, antenas de cabeça de rádio remoto e antenas de beamforming. Estas antenas vão ter um papel cada vez mais importante na rede de telecomunicações, e a prevalência das antenas ativas é estimada crescer. Muito deste crescimento será conduzido por configurações de MIMO e de Massive MIMO.

O envio de volumes de informação muito maiores em igual espaço de tempo, assim como as exigências significativamente maiores em termos de latência (intervalo de tempo entre o comando dado e a sua execução através de uma rede) e de estabilidade, conduzem à procura de novas tecnologias que permitam a realização de comunicações com essa exigência. Entre essas tecnologias existem duas que sobressaem, nomeadamente beamforming e MIMO.

Beamforming é a técnica de processamento de sinal utilizada com um conjunto de sensores para transmissão ou receção direcional (emitida ou recebida numa direção particular) de informação.

MIMO (*Multiple Input Multiple Output*) é o nome dado à técnica que permite receber e enviar mais do que uma comunicação de dados simultaneamente, de diferentes utilizadores, na mesmo canal de rádio pela exploração de propagação multi-caminho (baseado na ideia de que diferentes comunicações de diferentes emissores têm de fazer diferentes caminhos, que têm impacto na forma da transmissão, até ao recetor, e vice-versa). A palavra 'massive', de Massive MIMO, refere apenas o número elevado de recetores e transmissores na antena de rádio, que oferece uma muito maior capacidade para fazer comunicações em simultâneo.

Segue-se um diagrama simplificado do funcionamento da rede 5G:

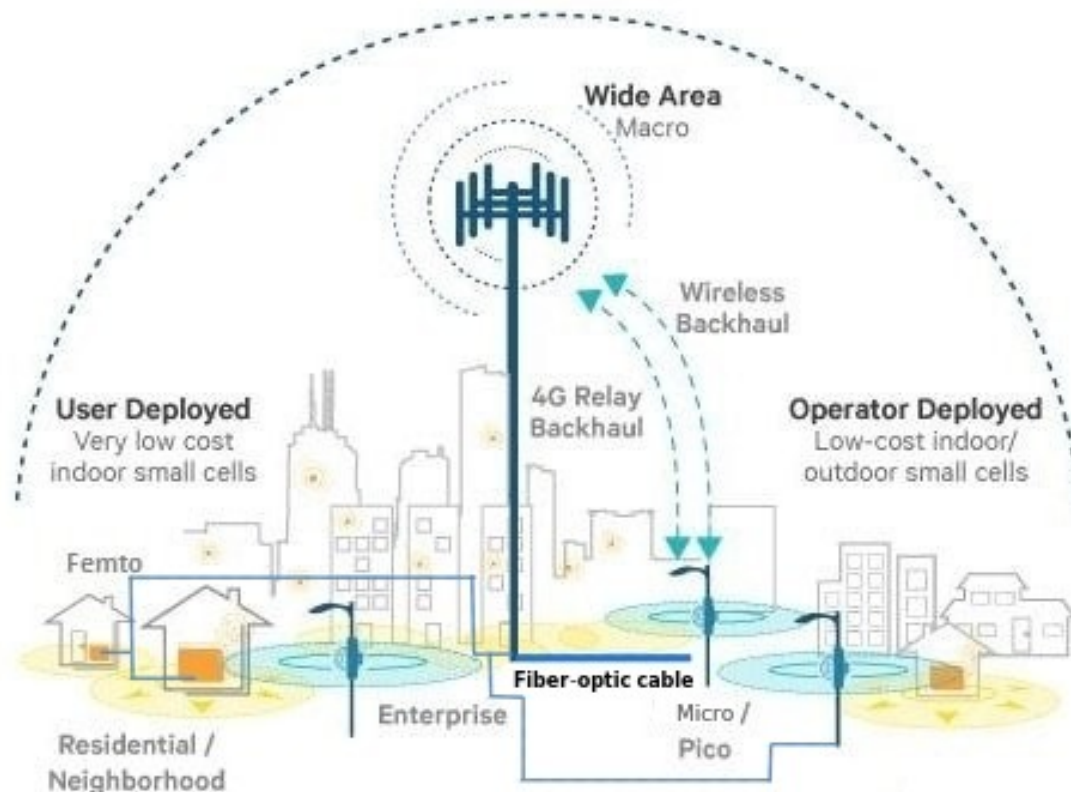


Ilustração 2: Diagrama do funcionamento da Internet Móvel 5G

Femto (*Femtocells*) é a designação associada às instalações pequenas e móveis da tecnologia 5G, que proporcionam serviço a aplicações no domicílio e em empresas. Nas casas com acesso a fibra ótica, o serviço 5G será instalado com facilidade apenas necessitando do recetor/transmissor específico.

Pico e Micro (*Picocells* e *Microcells*) são as designações das pequenas células de maior capacidade que fazem parte da tecnologia 5G. Que podem comunicar através de fibra ótica ou tecnologia sem fios (para já através de tecnologia 4G LTE⁵, posteriormente poderá ser promovida a 5G, mesmo podendo vir a fazer uso de ondas milimétricas) com a macro instalação (torre celular). Em particular as *Microcells*, devido ao maior poder de transmissão (500 - 2500 metros) que as *Picocells* (100 - 250 metros), são capazes de proporcionar cobertura a maiores áreas, e são indicadas para aplicações como cidades inteligentes, metro inteligente, etc. E apesar da designação de “pequenas células”, não são pequenas, e são intrusivas.

A torre celular (macro) estará conectada à rede de telecomunicações, e à Internet, através, quase sempre, de cabo de fibra ótica.

Só com a instalação de fibra ótica será possível oferecer as condições de serviço esperadas da tecnologia 5G.

5 - 4G LTE (Long Term Evolution) é um estado mais avançado de evolução da tecnologia 4G

As Pico e Micro células são versáteis, podendo ser instaladas em vários sítios no espaço público.



Ilustração 3: Exemplos de locais onde operam pequenas células 5G

Agora vou mostrar o aspeto destas antenas:



"Uma visão ponderada sobre o 5G
e tecnologias relacionadas", texto de Miguel Vilhena



"Uma visão ponderada sobre o 5G
e tecnologias relacionadas", texto de Miguel Vilhena



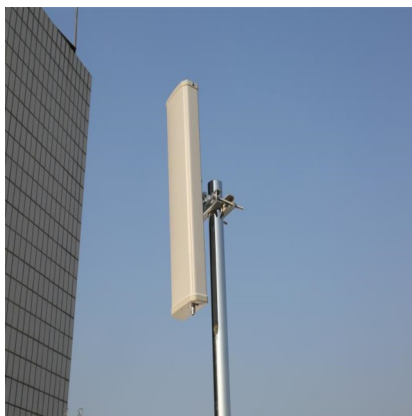
"Uma visão ponderada sobre o 5G
e tecnologias relacionadas", texto de Miguel Vilhena



"Uma visão ponderada sobre o 5G
e tecnologias relacionadas", texto de Miguel Vilhena



"Uma visão ponderada sobre o 5G e tecnologias relacionadas", texto de Miguel Vilhena



Havendo ainda aquelas que se misturam com a paisagem como



A tecnologia celular 5G está também a ser combinada com iluminação LED em postes de luz, preparando as urbes para o desenvolvimento das "cidades inteligentes". Embora inicialmente esta tecnologia comunique por 4G LTE.

"Uma visão ponderada sobre o 5G e tecnologias relacionadas", texto de Miguel Vilhena



Ilustração 4: Esquema de um poste de luz inteligente

Seguem-se dois exemplos desta tecnologia nas imagens a seguir:





Com uma radiação de muito mais alta frequência, com dificuldade em atravessar objetos sólidos, e com uma instalação muito mais massiva de torres celulares, vem o aumento da destruição de árvores na via pública, e parques, pelo mundo fora, com vários relatos e notícias sobre essa devastação progressiva, incluindo aqui em Portugal, na zona de Oeiras, Aveiro, Vila Real, Faro, Porto, Lisboa e Vila Nova de Paiva. Isto porque, para não limitar o rendimento das antenas celulares com a absorção e a difração indesejadas das radiações eletromagnéticas, é necessário que as árvores tenham uma altura inferior à posição das antenas em 3 metros, o que irá impactando necessariamente o ordenamento dos espaços públicos, e também limitará e condicionará a plantação de novas árvores e vegetação na via pública, incluindo em parques.

E acrescido a isto, apesar das afirmações de maior "eficiência energética" da rede celular 5G, as torres de rádio consomem cerca de 2 a 3 vezes mais energia elétrica quando comparadas com as das 4G, de acordo com declarações da *China Mobile* e Matt Walker, analista chefe consultor da MTN. Isto devido à sua maior sofisticação (incluindo o funcionamento com ambas as faixas de frequência FR1 e FR2) e à potência necessária para servir a área a que está aplicada, a que acresce a necessidade de muitas mais torres celulares para fazer a cobertura de Internet móvel em FR2, assim como o consumo elétrico associado a instalações para gerir o processamento local de informação e novos serviços de IoT (Internet of Things [Internet das Coisas]). O consenso da indústria de telecomunicações aponta para que a tecnologia 5G irá duplicar ou triplicar o consumo elétrico para operadoras móveis, quando as redes estiverem implementadas.

Esta necessidade massiva de eletricidade pode levar a problemas a nível de suprimento energético das instalações celulares 5G, e afetar a eficiência destas, assim como afetar a disponibilidade energética para o resto dos serviços sociais. Especialmente nesta altura em que parte significativa das fontes de gás e petróleo é russa, e está sobre sanção americana e europeia e funciona como uma arma no conflito do mundo ocidental e a Rússia.

Este problema em termos de grande consumo elétrico também se traduz em aquecimento elevado dos equipamentos, que pode interferir com o seu funcionamento e encurtar o seu tempo de vida. Segundo os próprios fabricantes das estações base é uma área na qual estão ativamente a trabalhar, com a Nokia em particular a anunciar um tipo de estação base significativamente mais económico e com melhor refrigeração.

Sendo também importante referir a necessidade de quantidades massivas de água para refrigerar os data centers construídos. O que é especialmente preocupante em áreas privadas de água, como terras desérticas.

Tudo isto realça que, apesar estarmos a presenciar o lançamento da tecnologia 5G em termos comerciais a nível mundial, a tecnologia ainda está longe de estar amadurecida e pronta para este empreendimento.

Uma apresentação, de 2017 - que vai na mesma linha de outros estudos anteriores de outras fontes - de Anders Andrae, empregado da Huawei, estima que sem um crescimento dramático em termos de eficiência energética, a indústria da Internet das Coisas poderá usar 20% de toda a eletricidade (em termos mundiais) e emitir até 5,5% das emissões de carbono mundiais em 2025, e até 14% em 2040 (o mesmo nível de emissões dos Estados Unidos em 2017).

Também é de referir que a funcionalidade 5G também gasta mais rapidamente a carga da bateria do telemóvel, ou de outro aparelho móvel, por ser uma tecnologia muito mais exigente.

Para países que recorrem constantemente a combustíveis fósseis para alimentar a rede elétrica, isto só os vai tornar mais dependentes dos combustíveis fósseis, e aumentar a velocidade e a quantidade do consumo destes produtos, aumentando massivamente o preço do consumo da eletricidade, a escassez de água e o ritmo do aquecimento global. Especialmente em tempos de guerras geopolíticas associadas ao serviço energético.

Há que ressaltar, no entanto, que continua o trabalho por parte das empresas ligadas à tecnologia 5G no sentido de melhorar a tecnologia usada, aumentando a sua eficiência e diminuindo o seu consumo, procurando também diminuir o calor libertado e as emissões associadas de CO₂.

Em relação a isto também existem as questões de inspeção e avaliação dos locais de instalação e a monitorização das instalações de antenas de telecomunicações, que como mostrou a instalação de uma antena celular dentro do espaço de um lar de idosos e junto a uma escola em Vila Nova de Famalicão - entre outras instalações semelhantes - serem processos questionáveis em Portugal. Para não falar que o volume de instalações celulares necessárias para garantir um serviço 5G ao nível dos padrões ambiciosos de velocidade, de acessibilidade e fiabilidade estabelecidos, previamente, agravará estes problemas logísticos e de proteção da saúde e do ambiente.

Também há que falar do envolvimento íntimo na elaboração de standards de segurança associados à tecnologia 5G por parte do FBI, do GCHQ⁶ britânico e outras agências de espionagem e organizações policiais, que estão a pressionar no sentido que seja facilitada a coleção da informação dos consumidores, na utilização do 5G, tanto quanto possível

6 - GCHQ é a sigla representativa da agência de inteligência britânica Government Communications Headquarters.

tecnicamente. O que não é de estranhar, visto as notícias sobre os programas de vigilância e coleção de dados de Internet Americanos vindos a público.

A entrega inicial de especificações para 5G NR NSA (Non-Stand-Alone, ou, em português, dependente das tecnologias de telecomunicações prévias [4G e 3G]) ocorreu em fins de 2017 pela 3GPP⁷, evoluindo o trabalho na direção da criação de um conjunto completo de standards para a tecnologia 5G (incluindo 5G NR SA [Stand-Alone]) subsequentemente. Isto permitiu aos vendedores de chips progredir rapidamente com o desenho de componentes e implementações iniciais de redes 5G em 2019.

Em três de julho de 2020 foram oficialmente declaradas como terminadas as especificações para todo um sistema inicial de telecomunicações 5G, pela organização 3GPP (responsável pelo seu desenvolvimento). Sendo que trabalho continua a ser realizado em diversos campos ligados à tecnologia 5G, incluindo gasto e eficiência energéticos, comunicação com veículos, cidades inteligentes, incorporação de Inteligência Artificial e Machine Learning, posicionamento de terminais e localização, segurança, streaming. Também continuam a ser investigadas melhorias e inovações no funcionamento de telecomunicações em FR1 e FR2.

2.1 - A Internet das Coisas

A chamada Internet das Coisas é um conceito fortemente associada à tecnologia 5G.

Criada com base em Inteligência Artificial e Ciência de Dados, a Internet das Coisas (Internet of Things, em inglês) já deixou há muito tempo de ser uma tendência ou moda, se tornando uma realidade em um mundo em constante transformação digital. A consultoria Juniper Research previu, por exemplo, que o número de dispositivos inteligentes conectados globalmente durante 2021 atingiria 46 milhares de milhões.

E a IoT de banda larga já ultrapassou o 2G/3G como o segmento que liga a maior porção de aplicações de IoT, estimando-se que represente 47% de todas as ligações de IoT celulares até ao fim de 2027, comparativamente a 37% para 2G/3G e 16% para tecnologias de IoT em massa (NB-IoT e Cat-M).

"A comunicação móvel teve um impacto incrível na sociedade e nos negócios ao longo da última década. Quando olhamos em perspectiva para 2027, as redes móveis serão mais integrais do que nunca na forma como interagimos, vivemos e trabalhamos. As novas previsões reafirmam a rápida aceleração das implementações de IoT em massa nos próximos anos, abarcando casos de utilização como os wearables de saúde eletrónica, o controlo de recursos logísticos, a monitorização ambiental e os medidores inteligentes, assim como os dispositivos inteligentes de controlo e monitorização da produção. É expectável que as

7 - 3GPP (3rd Generation Partnership Project) é a designação dada a uma colaboração de organizações responsáveis pelo desenvolvimento e manutenção de tecnologias de telecomunicações móveis e standards associados, incluindo 5G.

implementações de IoT em massa constituam 51% de todas as ligações de IoT celulares até 2027", diz em comunicado Fredrik Jejdling, vice-presidente Executivo e Chefe de Redes da Ericsson.

Como afirma António Martins da Costa, presidente da Câmara de Comércio Americana em Portugal, "a maior disrupção surgirá provavelmente do potencial combinatório da tecnologia 5G com outras tecnologias digitais, tais como Inteligência Artificial ou a Realidade Aumentada, potenciando aplicações disruptivas na mobilidade (massificação dos veículos autónomos), na saúde (medicina e cirurgia remota) ou nas cidades inteligentes. É também de esperar uma disrupção significativa no próprio setor tecnológico, uma vez que assistiremos a uma nova vaga de crescimento massivo na geração e comunicação de dados, que terão de ser tratados e armazenados em volumes exponencialmente crescentes, tornando o que hoje chamamos "big data" em algo numa escala ainda maior".

Mas isto é apenas o começo: quanto mais objetos conectados, mais inteligente poderá ser a gestão remota de serviços, o que se converterá em um perigo acrescido se a sua segurança informática for comprometida, ou se por algum motivo funcionar de forma deficiente.

A Internet das Coisas permitirá criar enormes redes de sensores coletando uma imensa quantidade de dados privados e públicos, facilitando um mundo mais intimamente conectado, inteligente, e despojado de privacidade. Praticamente qualquer aparelho, 'aparelhos' grandes e pequenos - carros, casas, sensores médicos, coleiras de animais, robôs autónomos e colaborativos, portos marítimos e controlos aéreos automáticos, estradas inteligentes, câmeras wireless de alta resolução, robôs industriais e sensores ambientais - serão capazes de enviar e receber dados através da Internet.

E acredita-se que será comercializada a capacidade de assumir o controlo de robôs à distância com óculos e luvas em um ambiente realidade virtual. As possibilidades, para o bem e para o mal, parecem ilimitadas.

Analistas do setor estimam que o número de dispositivos ligados à Internet poderá vir a ser de mil milhões até 2035.

E com o advento da Internet das Coisas (Internet of Things), os dados e processos têm de ser transferidos não apenas mais rápidos, mas instantaneamente, e com total fiabilidade. Porque, por exemplo, com os veículos autónomos, a demora na transmissão de informação e processamento pode se revelar fatal.

Esta conjuntura apresenta um desafio titânico e extremamente perigoso para os países e os seus cidadãos, na manutenção da inviolabilidade dos seus aparelhos inteligentes, da sua privacidade e na manutenção da sua própria segurança física, com uma nova Internet 5G extremamente poderosa, massificada e extremamente utilizada, mas também muito longe de estar devidamente testada e segura. Especialmente nos tempos de guerra que vivemos. Onde existirão mais aparelhos ligados, levando a uma maior complexidade da rede, e permitindo muito maiores velocidades e uma capacidade de transmissão de dados sem paralelo tecnologicamente, tornando as redes muito mais vulneráveis a ataques maliciosos.

3 - Exemplos importantes do uso de radiações micro-ondas

O eletrodoméstico microondas usa micro-ondas na faixa dos 2450 MHz, isto é 2.45 GHz. E o aquecimento dos alimentos no forno do microondas ocorre da superfície para o seu interior, por aquecimento que se propaga por migração. E estes aparelhos fazem-se acompanhar com uma detalhada lista de precauções de segurança a tomar no seu uso.

A intensidade das micro-ondas emitidas em um forno micro-ondas é muito superior a de um transmissão de um telemóvel para antena em tecnologia 5G, e de uma antena para um telemóvel na mesma tecnologia. Mas em situações reais, normalmente não haverá só um telemóvel comunicar com uma antena, mas vários, provavelmente comunicando em tecnologias diferentes (3G, 4G, 5G), com a possibilidade da intensidade das radiações eletromagnéticas ser reforçada pelo efeito fotoelétrico, e combinando e interagindo com outros poluentes ambientais.

Também as ondas milimétricas na frequência dos 95 GHz são usadas pelo Ministério da Defesa Americano no sistema para controlo de multidões chamado de Active Denial Systems (ADS), que funciona com curtas exposições a esta radiação. Nas palavras da página oficial do ministério da defesa americano, "o ADS proporciona uma rápida e reversível sensação de aquecimento da pele".

4 - Risco de interferência dos serviços de 5G com as leituras meteorológicas

A faixa das micro-ondas é uma parte do espectro eletromagnético com pouco uso pela maioria da tecnologia atual, embora seja utilizada por radares⁸ e por sensores para medições relacionadas com o clima, incluindo satélites meteorológicos. Por isto teme-se - com vários organismos oficiais a manifestarem preocupação publicamente - que a tecnologia 5G vá interferir com os sensores e as observações do clima, tornando mais difíceis e imprecisas as medições, e significativamente menos úteis os modelos de previsão e sistemas de aviso sobre eventos meteorológicos, pondo em maior risco a segurança das populações.

“Numa altura de vulnerabilidade acrescida a ameaças meteorológicas, é imperativo que observações críticas terrestres sejam protegidas de interferência. O impacto de dados da observação da Terra perdidos pode ser catastrófico para a nação”, atestou William Mahoney, diretor associado do NCAR (National Center for Atmospheric Research), no congresso dos Estados Unidos da América a 20 de julho de 2021.

E isto, em Portugal, vai contra os objetivos estabelecidos pela ANACOM para nortear a sua ação, nomeadamente de “assegurar que certas faixas de frequências sensíveis para a

8 - Há vários estudos associando o uso de radar por polícias a várias espécies de cancro (ver em Referências estudo sobre a incidência de cancro em polícias)

obtenção de dados operem numa base livre de interferências, por forma a garantir a fiabilidade das medições efetuadas pelos sensores dos satélites e as suas transmissões para as estações terrenas de receção, sobretudo no intervalo entre os 400 MHz e os 6 GHz”, como apresentado no seu Plano de Estratégia do Espectro, de agosto de 2016.

5 - Riscos de interferência com sistemas de navegação aeronáuticos

Transportadoras aéreas como a Boeing e a Airbus, assim como várias outras, expressam grande preocupação sobre a presença de tecnologia de internet móvel ultrarrápida 5G junto dos aeroportos e das pistas de aterragem, pela possibilidade de interferência com os instrumentos de voo nos aviões.

“Num dia como o de ontem (domingo), mais de 1.100 voos e cem mil passageiros seriam sujeitos a anulações, desvios ou atrasos”, receram nomeadamente os dirigentes das transportadoras American Airlines, Delta e Southwest e ainda as divisões aéreas dos conglomerados da distribuição FedEx e UPS.

“Considerando o pouco tempo restante e a importância desta calamidade económica, completamente evitável, pedimos respeitosamente que apoie e tome todas as ações necessárias para que o 5G seja desenvolvido, com exceção de quando as torres ficarem demasiado perto das pistas dos aeroportos”, escreveram, na missiva destinada ao governo federal, à agência de segurança na aviação (FAA, na sigla em Inglês) e ao regulador das telecomunicações (FCC).

Estes dirigentes pretendem também uma pausa, “até que a FAA possa determinar como o desenvolvimento pode ser conseguido com toda a segurança, sem perturbação catastrófica”.

Face às inquietações com potenciais problemas de interferências com os aparelhos que medem a altitude dos aviões, a FAA emitiu novas diretivas a limitar a utilização destes aparelhos de bordo em algumas situações.

Mas as transportadoras aéreas norte-americanas insurgiram-se contra os potenciais custos induzidos e apelaram às autoridades para que encontrem rapidamente uma solução.

6 - Efeitos na biologia humana associados às micro-ondas

A mais rigorosa avaliação dos efeitos biológicos das radiações milimétricas foi conduzida na base militar da força aérea norte americana de Brooks, na divisão de Investigação Médica, em San Antonio, e foi publicado em 1998.

O grupo de investigação observou "efeitos profundos das ondas milimétricas... a todos os níveis biológicos, de sistemas sem células, passando por células, órgãos, e tecidos, até organismos animais e humanos". É de notar que foi assinalada que a observação de "muitos dos efeitos reportados era significativamente diferente daqueles causados pelo calor, e a sua dose e frequência sugeriam frequentemente mecanismos não-térmicos". A investigação mostrou efeitos biológicos em frequências de micro-ondas bem menores que os níveis necessários para causar aquecimento.

As autoridades na área das radiações eletromagnéticas apontam para a noção que as ondas milimétricas são menos capazes de penetrar a pele que ondas de mais baixa frequência, sugerindo que então estas são menos perigosas. Ainda assim a variedade de efeitos biológicos descritos pela equipa de investigação do exército foram "muito inesperados de uma radiação que penetra os tecidos biológicos em menos de 1 mm". Os investigadores admitem ter ficado confundidos pelas evidências, afirmando que os efeitos observados "não podiam ser explicados atualmente".

O artigo declara também que "efeitos biológicos de uma exposição prolongada ou crónica de todo o corpo a radiações micro-ondas... nunca foi investigada." Os limites de segurança são "baseados somente em previsões", uma abordagem que a equipa de investigação declara como "não necessariamente adequada".

É de referir o conceito da ressonância simpática ou vibração simpática, que é um fenómeno harmónico em que uma cadeia anteriormente passiva ou corpo vibratório responde às vibrações externas com as quais tem uma semelhança harmónica. Isto significa que um determinado estado psicológico, emocional e físico em uma pessoa pode ser condicionado por agentes, físicos ou abstratos externos (por exemplo radiação eletromagnética) ao qual ela tem sensibilidade.

De notar que os tipos de onda do espectro eletromagnético apresentadas acima (na Tabela1) são chamadas de radiações não-ionizantes, pela sua reconhecida incapacidade de excitar os átomos da matéria expostos a ela de forma suficiente para quebrar ligações dentro deles. Mas este facto não torna estas radiações inofensivas, como demonstrado pelo facto de existir sinalização internacional de segurança para exposição a radiações não-ionizantes, sendo no entanto de notar a sua parca utilização em Portugal.



*Ilustração 5: Sinal de
aviso sobre exposição
a radiações não-
ionizantes*

A ICNIRP (International Commission on Non-Ionizing Radiation Protection), a comissão independente, sem fins lucrativos, sediada em Munique, que emite guias para os parâmetros de segurança na exposição a radiações não-ionizantes a nível internacional, consultada pela União Europeia, assume que os "campos eletromagnéticos com uma intensidade suficiente podem afetar adversamente a saúde". Reconhecendo três efeitos adversos da exposição a radiação eletromagnética: estimulação nervosa (circunscrito a baixas frequências), aumento da temperatura e mudanças na permeabilidade das membranas celulares (que foi visto experimentalmente na frequência de 16 GHz).

Das diretrizes do ICNIRP são excluídos curiosamente participantes voluntários em investigação científica, delegando também em corpos reguladores nacionais a responsabilidade de decisão de outras isenções. O seu parecer está limitado às populações humanas, e é de notar que não discriminam fetos, incluindo-os como parte do público geral, assim como a sua avaliação está limitada exclusivamente à ação de campos eletromagnéticos, escusando-se de avaliar cenários onde os campos eletromagnéticos são apenas um dos fatores.

O parecer de 2020 do ICNIRP (incluído na bibliografia) é baseado no rascunho técnico da World Health Organization sobre a exposição a campos eletromagnéticos e saúde (WHO 2014), em documentos da Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR 2015) and the Swedish Radiation Safety Authority (SSM 2015, 2016, 2018), e na análises de estudos sucedâneos, dentro e fora da área da literatura científica sobre campos eletromagnéticos. De mencionar que este relatório usa literatura disponível, não fazendo esforços para a completar com investigação adicional, em áreas de carência, como na precisão do aumento da temperatura dos corpos ao ponto de causar dano ao ser humano causado pela exposição a campos eletromagnéticos, onde admite falta de evidências conclusivas para determinar valores mínimos.

O investigador indiano Malka N Halgamuge, com base na sua investigação científica, critica as recomendações do ICNIRP dizendo que são direcionadas para efeitos agudos bem conhecidos, porque efeitos da duração da exposição não são considerados, e que são limitadas pela não replicação dos estudos experimentais existentes.

Também a FCC americana está restringida no objeto do seu estudo "aos efeitos das nossas ações na qualidade do ambiente humano, incluindo exposição humana a energia RF [de radiofrequência] emitida por transmissores e construções reguladas pela Comissão."

É um problema quando não há verdadeiramente uma preocupação institucional com os efeitos da radiação eletromagnética no meio ambiente, e nos ecossistemas, dos quais, apesar de toda a arrogância humana, estamos irremediavelmente dependentes.

A FCC até vai mais longe afirmando, no seu documento de 2019 de revisão do regulamento sobre exposições humanas a radiofrequências, que "hoje, tomamos um número de passos em relação a estes limites para garantir a saúde e a segurança dos trabalhadores, e consumidores de tecnologia wireless, enquanto também clarificando e aligeirando as regras para reduzir o peso regulatório nos licenciados."

Sobre a posição da FCC, Theodore Olson, advogado da CTIA (Cellular Telephone Industries Association), afirma que “eles estão a torná-lo tão explícito quanto conseguem – ‘não se metam com o que fizemos aqui’. Qualquer outra coisa arrisca uma política não-uniforme. Se sobreavisas as pessoas, podes assustá-las e fazer que eles não os usem [telemóveis]”.

Já nos anos 60, um neurocientista chamado Allan Frey, na Universidade de Cornell, criou uma experiência na qual sapos eram expostos a certas frequências de micro-ondas. Ele verificou que a radiação podia provocar arritmia, e com uma pequena mudança nas frequências podia fazer o coração dos sapos parar.

Uma característica incómoda das micro-ondas de extremamente alta frequência é a sua dificuldade em atravessar objetos sólidos, como árvores, edifícios, o corpo humano, ou mesmo a água ou o vidro, sendo facilmente absorvida por estes, desde que tenham espessura superior a alguns milímetros. Isto obriga a que os telemóveis de 5G tenham várias antenas espalhadas pelo aparelho (4, 6 antenas, que depende do fabricante e do modelo do telemóvel), em diferentes posições, com o fim de assegurar a melhor ligação à rede móvel possível.

Sendo que, como referido, a estas antenas transmitem em frequências de micro-ondas de extremamente alta frequência quando funcionando em modo 5G. E isto é um problema especialmente quando, como faz a maioria das pessoas, deixa o telemóvel com a Internet móvel permanentemente ligada quando está fora de casa. Há que notar espaços metálicos potenciam a densidade e o efeito das ondas eletromagnéticas no seu interior, pelo efeito fotoelétrico ou efeito Hertz.⁹

Vários estudos reportaram diminuição na fertilidade masculina humana e motilidade do esperma correlacionada com o uso do telemóvel ou o transporte dele no bolso (Kilgallon SJ, Simmons LW. Cell phones, sperm cells don't mix, The price of mobility: Decreased motility. Biol Lett 2005; Agarwal A, Deepinder F, Sharma RK, Ranga G, Li J. Effect of cell phone usage on semen analysis in men attending infertility clinic: An observational study. Fertil Steril 2008; Agarwal A, Desai NR, Makker K, Mouradi R, Sabanegh E, Sharma R. Effects of radio-frequency electromagnetic waves from cellular phone on human semen: An in vitro pilot study. Fertil Steril 2008; Wdowiak A, Wdowiak L, Wiktor H. Evaluation of the effect of using mobile phones on male fertility. Ann Agric Environ Med 2007; 14: 169–172). No entanto, dados precisos sobre a exposição à radiação eletromagnética e reação a ela estão ausentes nestes estudos.

De acordo com a ICNIRP, baseado em resultados experimentais (Sasaki et al. 2017), com o aumento da frequência dos campos eletromagnéticos, a exposição do corpo e o resultante aquecimento torna-se mais superficial, e acima dos 6 GHz este aquecimento ocorre predominantemente na camada da pele. Nomeadamente, 86% das emissões nos 6 e 300 GHz

9 - O efeito fotoelétrico ou efeito Hertz é o fenómeno correspondente à emissão de eletrões por um material, geralmente metálico, quando exposto a uma radiação eletromagnética de frequência suficientemente alta, sendo que este limite depende do material exposto. Os eletrões são desalojados apenas pelo impacto dos fótons quando estes atingem ou excedem uma frequência limite. A intensidade determina também a dimensão do fenómeno. São libertados os eletrões com a radiação absorvida acumulada, aumentando a intensidade da energia electromagnética dispersa no ambiente.

é absorvido entre os 8 e 0.2 mm da pele respetivamente. Embora parte desse calor na derme migre, através do extensa e intrincada rede vascular que a permeia, para o interior do corpo humano. A ICNIRP, no entanto, admite que não tem conhecimento de investigação que tenha determinado o efeito de campos eletromagnéticos de 6 a 300 GHz na temperatura corporal.

Este efeito leva a crer que a temperatura da superfície dos corpos (pele, olhos, testículos) e do meio ambiente sejam afetadas e aumentem em relação direta com a intensidade das radiações eletromagnéticas em ação. Porque toda a radiação carrega energia produzindo um efeito térmico nos objetos com os quais entra em contato. Sendo especialmente preocupante com as radiações micro-ondas pelo aquecimento mais superficial e concentrado que produzem. Sendo este mais um ponto de interrogação sobre o efeito de radiações eletromagnéticas artificiais, e as micro-ondas, no meio ambiente.

Um estudo arménio de 2016 sugere que a exposição a micro-ondas impacta a água, a membrana (celular) plasmática, e a atividade genética, alterando a sensibilidade a diferentes químicos, incluindo antibióticos.

A Oceania Radiofrequency Scientific Advisory Organisation, uma entidade australiana, examinou 2266 estudos, e encontrou "efeitos biológicos ou efeitos na saúde significativos" em 68% dos mesmos. Outra organização, o Bioinitiative Group, referiu-se a 1800 estudos quando concluiu que muitos desses efeitos causam provavelmente danos à saúde se as pessoas forem expostas a radiação durante muito tempo. Isto porque a radiação interfere nos processos normais do organismo, impedindo-os de reparar o ADN danificado e criando um desequilíbrio no sistema imunitário, afirmaram estes cientistas.

Tudo isto levanta questões sobre os efeitos sobre a saúde humana, e de restantes seres vivos, sujeita a tão intensa e tão elevada radiação. Isto especialmente quando visto em relação a uma doença que tem sido vindo a ser reportada pontualmente, embora não reconhecida oficialmente pelos mais altos organismos de saúde, mas com cada vez mais reconhecimento por autoridades de saúde, encarregados da segurança social, políticos e tribunais, chamada de hipersensibilidade eletromagnética. Hipersensibilidade Eletromagnética associa à experiência de radiação eletromagnética - característica, por exemplo, de telemóveis, da redes Wireless e Internet móvel - dores físicas, fraqueza, alergias, dificuldade em estar concentrado e irritabilidade fora do comum, impactos no funcionamento do coração e sistema nervoso, e outros sintomas. E por causa destes sintomas algumas pessoas, de todas as áreas de atividade, sentiram-se forçadas a deixar os seus empregos, ficaram de baixa, ou experimentaram redução significativa da sua produtividade. Isto acontecendo agora enquanto a tecnologia 5G ainda está longe de estar completamente instalada e funcional, com radiações eletromagnéticas de muito mais baixa intensidade. Em Portugal calcula-se haver cerca de 300 mil pessoas a sofrer de Hipersensibilidade Eletromagnética, mal diagnosticadas.

Existe cada vez mais evidências que a exposição a campos eletromagnéticos tem um impacto significativo na capacidade de regulação oxidativa e nitrosativa dos indivíduos afetados por Hipersensibilidade Eletromagnética.

A EUROPAEM recomenda como principal forma de prevenção e tratamento a redução de exposição a campos eletromagnéticos. Afirmando que a redução de exposição deve-se estender a espaços públicos como escolas, hospitais, transportes públicos e bibliotecas, para não afetar negativamente pessoas com Hipersensibilidade Eletromagnética. Isto porque se a exposição a campos eletromagnéticos é reduzida significativamente, o indivíduo tem a hipótese de recuperar, e os sintomas reduzem ou mesmo desaparecem.

A Hipersensibilidade Eletromagnética (EHS [Electromagnetic Hypersensitivity]) está intimamente ligada a outra doença chamada Sensibilidade Química Múltipla (MCS [Multiple Chemical Sensitivity]), um síndrome causado pela exposição a agentes químicos. Estima-se que cerca de 35% das pessoas afetadas pela MCS também desenvolvem EHS. E também a Hipersensibilidade Eletromagnética apresenta efeitos semelhantes ao Síndrome Aguda da Radiação.

A radiação Wireless, campos eletromagnéticos, e a "eletricidade suja"¹⁰ estão associados cientificamente com concentrações elevadas de açúcar no sangue e diabetes. Aumentando em norma a glucose no sangue com a proximidade a torres celulares. Sendo que os diabetes, em média, em 30% dos casos conduzem a doença renal crónica, com evolução para a hemodiálise.

Também ligada cientificamente à exposição a radiação eletromagnética estão problemas do sistema nervoso, incluindo efeitos neurológicos e neuropsiquiátricos, problemas do sistema endócrino, diminuição da fertilidade e mesmo infertilidade, mutações (incluindo nos gametas [espermatozóides e óvulos]), aceleração da morte celular e envelhecimento precoce, leucemia, doenças neurodegenerativas (como a doença de Alzheimer), problemas cardíacos, diminuição da concentração das hormonas sexuais, diminuição do libido e impotência, letargia, tonturas, redução da capacidade cognitiva, visão enevoada, secura dos olhos, depressão, fadiga, redução da pigmentação e aumento da probabilidade de aborto espontâneo.

A radiação eletromagnética afeta a fase fetal e o crescimento humanos. Estudos apontam que a exposição pré-natal e pós-natal a telemóveis está associada a problemas comportamentais e hiperatividade em crianças. Também foi registado que a exposição pré-natal à radiação de telemóvel em ratos causou deficits estruturais e funcionais no cérebro das cobaias. Assim como foi observado que a radiação eletromagnética altera as ondas cerebrais, e contribui para o autismo na exposição pré-natal.

Um estudo de 2012, publicado na revista International Journal of Radiation Biology, encontrou um aumento significativo de danos no ADN das células da raiz dos cabelos à volta da orelha usada junto ao telemóvel, depois de breve exposição (15-30 minutos) a radiação (900 MHz) de um destes aparelhos, conduzindo à perda de cabelo.

E existe um estudo apresentado em 2018 [presente na secção Referências] que aponta para que a exposição, mesmo breve, a micro-ondas poder provocar aquecimento da pele e

10 - É a energia elétrica criada por pequenos transformadores, adaptadores que equipam muitos dos nossos aparelhos atuais, as lâmpadas económicas (CFL, Compact Fluorescent Lamps), reguladores de luz, TVs, etc. Os componentes biologicamente ativos da "eletricidade suja", são as correntes transientes e harmónicas que circulam nas cablagens.

danos permanentes nos tecidos de seres humanos, dentro dos limites de segurança atuais da FCC.

A ICNIRP afirma que danos resultantes da subida da temperatura corporal devido à exposição a radiação eletromagnética são só vistos quando a temperatura corporal sobe acima de 1°C, tirando o corpo humano do estado de normotermia. De notar, no entanto, que importantes mudanças fisiológicas podem ocorrer quando a temperatura corporal sobe 1°C, sendo estas parte da resposta termorregulatória normal do corpo humano, e não efeitos adversos à saúde.

E curiosamente a ICNIRP, na sua guia, trata exposições a campos eletromagnéticos que resultam no aumento da temperatura local no corpo a acima dos 41°C como potencialmente perigosas à saúde, quando a hipertermia acima dos 41°C apresenta risco de causar golpe de calor e morte, assim como pode causar danos significativos aos neurónios, com risco de afetar a meninge. Sendo de notar que a temperatura corporal pode, a partir de uma temperatura típica no funcionamento normal do indivíduo (normotermia), em 10-15 minutos, atingir os 39°C, provocando deficiências no funcionamento cerebral. Também no caso do feto, uma temperatura maternal acima do normal em cerca de 2°C em fetos induzidos pelo calor pode causar anormalidades no desenvolvimento (Edwards et al. 2003). Podem também ocorrer alteração da perfusão placentária, mesmo em aumentos de temperatura aparentemente assintomáticos na mãe, pondo em causa o único mecanismo de termorregulação disponível ao embrião ou feto. Nisto a sua guia não se assume como conservadora, mas de facto arriscada na perspetiva adotada e consequentemente nas normas aconselhadas.

De notar que aborto espontâneo e malformações no feto foram reportadas como resultado de febre da mãe ($\geq 37,8$ °C), ainda que não se saiba se esses efeitos foram devidos à doença que causou a febre ou à temperatura. Infelizmente, os efeitos a longo prazo de stress térmico de baixo nível nos fetos não estão bem documentados.

E existem mais de 500 estudos que encontraram efeitos de saúde negativos na exposição a radiação de ondas de rádio (ondas eletromagnéticas de frequências entre 3 kilohertz [kHz] e 300 gigahertz [GHz]), em intensidades muito baixas para causar aquecimento da pele significativo. Os efeitos incluem acrescido risco de cancro (incluindo cancro da mama), stress celular, aceleração da morte celular programada, aumento de radicais livres, danos a nível genético, transformações estruturais e de funcionamento a nível dos órgãos reprodutores, danos ao sistema endócrino, danos ao sistema metabólico e sistema imunológico, défices de memória e dificuldade da aprendizagem, desordens neurológicas, infertilidade e impactos negativos no bem estar geral dos seres humanos. E os malefícios vão bem para lá dos seres humanos, com evidências cada vez maiores de efeitos negativos na vida vegetal e animal.

Hallberg e Johansson propuseram que as radiofrequências aumentam os efeitos das radiação ultravioleta. Um estudo sobre as causas do melanoma (cancro de pele) em seres humanos concluiu que o aumento de incidência e da mortalidade associada não podem apenas ser explicados pela elevação da exposição a radiação ultravioleta, mas também pela alterações progressivas nos mecanismos de reparação celular, produzidas pelas radiações eletromagnéticas ressoantes com o corpo, que amplificam os efeitos carcinogénicos dos

danos celulares induzidos pela radiação ultravioleta. Os casos de melanoma aumentaram significativamente dos 1960-70 até à atualidade. Também diversos outros tipos de cancro associados com a deterioração do sistema imunitário e a asma têm experimentado um crescimento contínuo. Os dados sugerem que tem havido um aumento progressivo de poluição eletromagnética.

Martin Pall advertiu também que as micro-ondas são muito mais perigosas para o cérebro das crianças, que para o de adultos, pelos crânios menos espessos, permitindo as radiações eletromagnéticas penetrar mais profundamente no cérebro, e pela maior densidade de células estaminais que aparentemente são mais sensíveis a radiação micro-ondas.

O investigador William Ross Adey, da Universidade da Califórnia, também realizou vários estudos sobre os efeitos biológicos e psicológicos de micro-ondas, relatando efeitos como mudanças no funcionamento das células, tecidos, organismos e até de humor, na presença de campos eletromagnéticos. Descrevendo até ocorrências de cancro.

Os campos eletromagnéticos artificiais afetam imediatamente os indivíduos quando expostos a eles, e levam os glóbulos vermelhos a mudarem para uma forma irregular com pontas (equinócitos), e mesmo a aglutinarem-se, perdendo gradualmente a sua funcionalidade e dificultando a circulação sanguínea. Tal acontece porque as células sofrem trauma e degradam-se. Isto interfere com a libertação de oxigénio e a remoção de dejetos celulares, como o dióxido de carbono, e dificulta a circulação e a oxigenação das células. São sintomas de ocorrências deste tipo, fadiga, dores de cabeça, dificuldade na concentração da atenção, sensação de insensibilidade, sensação de adormecimento, sensação de formigueiro, e de frio nas extremidades.

Um estudo de 2020 (de Jiajun Luo, Hang Li, Nicole C. Deziel, Huang Huang, Nan Zhao, Shuangge Ma, Xin Ni, Robert Udelsman e Yawei Zhang) aponta que a suscetibilidade genética pode ser um fator na associação entre o uso do telemóvel e cancro da tiroide. Com algumas variantes genéticas foi notada uma associação significativa com tumores na tiroide. A associação aumentava com a duração e a frequência do uso do telemóvel.

O doutor Joel Moskowitz, da Escola de Saúde Pública da Universidade da Califórnia, em Berkeley, asseverou na *Scientific American* que, de acordo com a sua revisão da parca literatura científica recente sobre o tema, as ondas milimétricas podem afetar negativamente o sistema nervoso periférico, o sistema imunitário, e o sistema cardiovascular. "A investigação aponta", escreveu ele, "que a exposição a longo prazo pode levar a riscos de saúde na pele (e.g., melanoma), nos olhos (e.g., melanoma ocular) e nos testículos (e.g., esterilidade)".

Também associada à poluição eletromagnética existe a exposição aos chamados radicais livres. Estes são átomos instáveis que causam danos ao ADN das células e membrana celular, que tornam as células suscetíveis a doenças e patógenos, assim fragilizando a saúde dos seres humanos. Os radicais livres estão associados com doenças como cancro, doença de Alzheimer, arteriosclerose, doença de Parkinson, e muitas outras. Os campos eletromagnéticos têm vários efeitos químicos, incluindo causar deterioração em moléculas de células e provocar desequilíbrios iónicos no organismo. Aparelhos inteligentes e Wifi

ininterrupta necessitam de ondas eletromagnéticas indutoras de radicais livres nos ambientes em que operam, causando continuamente ligeira inflamação associada com destruição celular e do ADN.

Apesar disto os radicais livres também têm funções importantes aos seres vivos, nomeadamente participam na transformação de alimentos em energia química durante a digestão, e são uma parte crucial do sistema imunitário, flutuando pelo sistema circulatório atacando invasores.

Os radicais livres são formados constantemente no metabolismo celular normal e em vários eventos patológicos e, quando em excesso no meio intracelular, causam a oxidação dos componentes da molécula biológica, em um evento chamado stress oxidativo, provocando degeneração celular. O stress oxidativo está associado com danos nas proteínas e lípidos, e ácidos nucleicos, e estudos relacionam-no com denegação macular, doença cardiovascular, certos cancros, enfisema, alcoolismo, doença de Alzheimer, doença de Parkinson, úlceras e todo o tipo de doenças inflamatórias, como artrite e lúpus. Assim como é apontado, cientificamente, como fator decisivo no envelhecimento, pelo dano causado pelos radicais livres no DNA das células, que afeta o seu desenvolvimento.

O investigador indiano Malka N. Halgamuge afirma em dois artigos científicos seus que a forma como os campos eletromagnéticos artificiais podem afetar a glândula pineal é ainda desconhecida, embora reconheça que os resultados mostram que o significado de disrupção da melatonina devido à exposição a campos eletromagnéticos fracos que pode possivelmente levar a efeitos na saúde a longo termo em seres humanos.

Este investigador declara que campos eletromagnéticos podem aumentar a quantidade de radicais livres, acionar respostas biológicas ao stress e alterar reações enzimáticas, incluindo ao nível da glândula pineal e da produção de melatonina. Aumentando o potencial dos radicais livres causarem mais danos no organismo, e apoiando a hipótese de que a exposição a campos eletromagnéticos fracos, pela disrupção da produção de melatonina, pode afetar adversamente a saúde humana.

A isto acresce o facto de vários destes efeitos biológicos serem cumulativos e, eventualmente, irreversíveis, se agravando com a frequência, a intensidade e o tempo de exposição a campos eletromagnéticos artificiais. Cujos efeitos se vão propagando e agudizando, afetando progressivamente as populações, espalhando e acumulando danos genéticos, tornando-se uma herança hereditária coletiva de uma geração para a seguinte, gerando problemas físicos e psicológicos crescentes, com expressão cada vez mais tangível e elusiva.

E todos os seres humanos são afetados pela energia eletromagnética, e tudo isto deverá gerar aumentos generalizados em termos de custos de saúde a médio e longo prazo, cujas doenças apesar de afetar de forma aproximadamente igual todos os estratos sociais da população, evidenciam e aprofundam as desigualdades entre as classes mais ricas e mais pobres. Uns tendo que se remediar com os hospitais públicos, e os tratamentos comparticipados pelo Estado, com o resto dos custos recaindo sobre os seus rendimentos

limitados, e outros com a liberdade financeira de escolher os melhores serviços de saúde disponíveis.

Sendo especialmente preocupante o efeito da poluição eletromagnética em bebés, crianças, doentes, idosos e inválidos, pela sua vulnerabilidade.

Especificamente as ondas milimétricas são em regra geral absorvidas dentro de uns milímetros de pele humana e pelas camadas mais superficiais da córnea (nos olhos). A exposição breve pode ter efeitos físicos adversos no sistema nervoso periférico, no sistema imunológico, e no sistema cardiovascular.

E há estudos (um de 2008 e outro de 2018, presentes na bibliografia) que mostram que as micro-ondas podem penetrar a pele pelos canais que conduzem o suor, agindo como antenas para as radiações da faixa das micro-ondas. O estudo de 2018 vai mais longe e afirma que o grau de refletividade de radiações eletromagnéticas depende da intensidade da transpiração, isto é, da condutividade dos canais de suor, e está correlacionado com os níveis de stress (físico, mental, emocional). E terminando, este último estudo deixa o aviso que a totalidade das ramificações destas conclusões ainda é uma incógnita. E alerta que se devem considerar as implicações da imersão humana na poluição eletromagnética, especialmente nas frequências superiores a 24 GHz e inferiores a 1 THz, “para as quais os canais de suor (como antenas helicoidais) estão mais recetivos. Nós estamos a levantar uma bandeira vermelha contra o uso indiscriminado de tecnologias sub-THz para telecomunicações, antes das possíveis consequências para a saúde pública serem exploradas.”

As micro-ondas, em baixas intensidades, mostram forte correlação à depressão, à fadiga e insónias em humanos.

A Agência Internacional de Pesquisa do Cancro, da Organização Mundial de Saúde das Nações Unidas, classificou em 2011 as ondas de rádio como possivelmente cancerígenas para os seres humanos. E em face destes novos estudos, e da confiança gerada em muitos investigadores de radiações eletromagnéticas, o IARC estabeleceu como prioridade rever nos próximos cinco anos o estatuto das ondas de rádio na área do cancro.

E também existem evidências significativas dos malefícios do 2G e o 3G, mas pouco é conhecido dos efeitos da exposição à tecnologia 4G - uma tecnologia já com mais de 10 anos - pela falta de financiamento para este tipo de investigação. Entretanto está-se a ver um aumento da frequência de tumores na zona da cabeça e do pescoço, que podem ser atribuídos à proliferação da radiação dos telemóveis e outros aparelhos sem fios. Estes aumentos são consistentes com resultados de estudos de casos e controlos sobre o risco de tumor em indivíduos com uso intensivo de telemóvel.

Desconhece-se também se existem efeitos decorrentes da exposição simultânea a vários tipos de ondas de rádio, na qual se pode incluir a exposição, num mesmo espaço de tempo, a duas ou mais das tecnologias 3G, 4G e o 5G. Se existirem efeitos, o risco geral de malefícios

pode aumentar significativamente. Com riscos, para lá do cancro, de doenças neurológicas e danos na reprodução, devido ao stress oxidativo¹¹ causado.

Com isto não estamos a dizer que a radiação eletromagnética e as tecnologias de Internet móvel são a causa única destas doenças, mas sim possivelmente um dos fatores contributivos para elas, que justificaria em parte o seu crescimento nos países desenvolvidos.

A organização EUROPAEM na sua guia de 2016 para a prevenção, diagnóstico e tratamento de problemas de saúde e doenças relacionadas com a radiação eletromagnética, declara que nos países da OCDE (Organização para a Cooperação e Desenvolvimento Económico) – dos quais Portugal faz parte – ocorre uma grande variação ao nível da prescrição de antidepressivos, e que uma tendência geral de aumento tem sido observada. Questões de estatuto socioeconómico e standards terapêuticos não conseguem explicar completamente estas observações. Com problemas funcionais como inflamação crónica e mudanças no funcionamento de neurotransmissores causadas por influências ambientais muito pouco investigados.

Um aumento estável na prevalência de doenças alérgicas/asmáticas está a ocorrer, com 30-40% da população mundial em 2016 a ser afetada por uma ou mais doenças alérgicas/asmáticas. Suspeita-se que condições ambientais como a exposição cada vez maior das populações a campos eletromagnéticos tenham um papel causal em problemas de saúde, incluindo a exposição à radiação que emana de telefones sem fios (DECT), antenas celulares e telemóveis (GSM, GPRS, UMTS, LTE), especialmente smartphones, afirma a EUROPAEM.

Apesar dos mecanismos biofísicos e bioquímicos dos efeitos biológicos associados aos campos eletromagnéticos de baixa intensidade não serem conhecidos com exatidão, há numerosos dados indicando que estes mecanismos podem se conjugar para efeitos associados a ELF e RF (Binhi VN. Magnetobiology: Underlying Physical Problems. San Diego: Academic Press, 2002:1–473; Binhi VN. Principles of electromagnetic biophysics (em Russo). Moscow (RU): Fizmatlit, 2011:1–571; Georgiou CD. Oxidative stress-induced biological damage by low-level EMFs: mechanism of free radical pair electron spin-polarization and biochemical amplification. Em: Giuliani L, Soffritti M, editors. Non-thermal effects and mechanisms of interaction between electromagnetic fields and living matter. Bologna (IT): Ramazzini institute, 2010. European Journal of Oncology – Library Vol. 5. pp 63–113.

Disponível em:
<http://www.icems.eu/papers.htm?f=/c/a/2009/12/15/MNHJ1B49KH.DTL>; Pall ML. Electromagnetic fields act via activation of voltage-gated calcium channels to produce beneficial or adverse effects. J Cell Mol Med 2013;17(8):958–65; Blank M, Goodman R. Electromagnetic fields stress living cells. Pathophysiology 2009 16(2–3):71–8; Blank M, Goodman R. Electromagnetic fields stress living cells. Pathophysiology 2009 16(2–3):71–8).

Sendo de notar que condições de exposição específicas causam respostas diferenciadas em diferentes indivíduos. No entanto, relatos pessoais indicam que essa responsividade ou

11 - O stress oxidativo é uma condição biológica em que ocorre desequilíbrio entre a produção de espécies reactivas de oxigénio (EROs) e a sua remoção através de sistemas (enzimáticos ou não enzimáticos) que as removam ou reparem os danos por elas causados.

suscetibilidade individuais expandem ao longo do tempo, e essa intolerância então se estende sobre uma gama vasta de condições de exposição.

Problemas e doenças crónicas associadas com sintomas não-específicos estão a subir. Em adição a stress crónico, em ambientes sociais e profissionais, exposições em casa, no trabalho, e durante atividades de lazer, existem stressores ambientais contributivos ou causais que merecem a atenção da comunidade de saúde. Parece necessário estudar as exposições a campos eletromagnéticos, ou como declarado por Hedendahl et al. (Hedendahl L, Carlberg M, Hardell L. Electromagnetic hypersensitivity – an increasing challenge to the medical profession. *Rev Environ Health* 2015;30(4):209–15): “É tempo de considerar campos eletromagnéticos ELF e RF como poluentes ambientais que precisam de ser controlados”.

É uma gigante irresponsabilidade e um risco impossível de calcular o desenvolvimento da tecnologia de comunicações móveis 5G apostando em uma abordagem meramente técnica, comercial e policial, sem compreender os níveis de exposição às radiações eletromagnéticas a serem experimentadas pelas populações e os efeitos das mesmas nos indivíduos, pelo menos.

As próprias seguradoras normalmente excluem dos seguros de saúde problemas decorrentes da exposição a radiações eletromagnéticas. A Swiss Re, a maior companhia de seguros e resseguros do mundo (operando em mais de 30 países), emitiu em março de 2019 um relatório onde classificou o 5G como um risco emergente elevado, avisando que “potenciais atribuições de problemas de saúde podem surgir com uma latência longa”.

Ao que se associa o aumento do tecnostresse (stress associado à dificuldade de adaptação à tecnologia e mau uso dela) que tem vindo a aumentar com o teletrabalho em tempos de pandemia, tanto em termos de tecno-sobrecarga (a sensação de estar obrigado a trabalhar mais e mais horas, excedendo limites e comprometendo o bem estar pessoal) como de sensação da invasão do ambiente de trabalho, através da tecnologia, da vida pessoal, com a ideia da cultura de trabalho do sempre conectado.

Que conduziu à nova lei que protege o direito a desligar do trabalho, no tempo fora do expediente, a não ser por motivos de "força maior", mas que também ainda assim não proíbe o envio de e-mails, sem resposta exigida, fora do horário laboral, abrindo-se ao abuso. [E isto ajuda a refutar o mito afirmado constantemente, ao longo das décadas, de que o avanço tecnológico ajudará a uma redução do trabalho e horário de expediente, e criará mais tempo livre para o trabalhador.]

A isto é adicionado o facto da recomendação¹² da União Europeia para a exposição do corpo humano a radiações eletromagnéticas - de 2018, de acordo com as diretrizes de 1998 da Comissão Internacional de Proteção Contra Radiação Não Ionizante (ICNIRP), e baseada no aquecimento significativo da pele a curto prazo – usar uma métrica chamada a Taxa de Absorção Específica (Specific Absorption Rate [SAR]), contestada por ignorar a particular

12 - Recomendação na qual assentam os limites para exposição eletromagnética da maioria dos países membros da UE, incluindo Portugal

sensibilidade do corpo humano à radiação eletromagnética, evidenciada pelo Efeito de Frey¹³, que acontece com exposições a radiações abaixo dos limites assumidos pela lei Portuguesa, e por se limitar a considerar exposições em períodos curtos (6 minutos, 30 minutos) e singulares, e não exposições regulares, e a várias fontes de emissão. Esta forma de medição da exposição a ondas eletromagnéticas ignora também as propriedades do sinal. O padrão e a duração da exposição ajudam a determinar os efeitos de certas características do sinal (pulsação, polarização) ao nível biológico e de saúde. Não contabilizando também a recente informação avançada pela investigação científica que as micro-ondas podem penetrar a pele pelos canais de suor.

E existe uma alarmante ausência de testes científicos válidos sobre os efeitos (não-técnicos) do 5G. E esta situação acaba tornando a implementação comercial da tecnologia 5G uma experiência a nível global sobre os cidadãos (portugueses e estrangeiros), de uma tecnologia nunca testada em ambiente real, que viola o Código de Nuremberga¹⁴.

E qual é o efeito acumulado da exposição em profissões expostas frequentemente e a grandes densidades de radiações eletromagnéticas, como hospedeiras de bordo de aviões de grande porte de transporte de passageiros e empregos obrigados a viajar constantemente (em estrutura metálicas pequenas e fechadas que amplificam e aumentam a exposição), empregados de aeroporto, empregados de grandes eventos e de grandes estruturas logísticas direcionadas para esses eventos, onde a quase totalidade de pessoas leva e usa o seu telemóvel? E os empregados de lojas de telemóveis?

E como será com a Internet das Coisas, com a ligação massiva de aparelhos elétricos do quotidiano à Internet 5G?

Um artigo científico de maio de 2020, intitulado de Adverse health effects of 5G mobile networking technology under real-life conditions, enfatiza que a maioria das experiências de laboratório conduzidas até ao momento do estudo não foram elaboradas para identificar os mais severos efeitos adversos em reflexo dos ambientes reais nos quais sistemas de radiação wireless operam. Muitas experiências não incluem pulsação e modulação da onda portadora. A larga maioria não tem em conta efeitos adversos sinérgicos com outros estímulos tóxicos (tais como químicos e biológicos) que atuam na presença da radiação wireless. Este artigo também apresenta evidências que a tecnologia emergente das redes móveis 5G afetará não só a pele e os olhos, como comumente se acredita, mas também irá ter efeitos sistémicos adversos.

O estudo de 2019 com o título de Validation of Potential Effects on Human Health of in Vivo Experimental Models Studied in Rats Exposed to Sub-Thermal Radiofrequency. Possible Health Risks Due to the Interaction of Electromagnetic Pollution and Environmental Particles (de Aaron A. Salas-Sánchez, Alberto López-Furelos, J. Antonio Rodríguez-González, Francisco J. Ares-Pena e M. Elena López-Martín) conjectura sobre a poluição eletromagnética, lançando a possibilidade de, em ambientes urbanos que combinam a 13 - Efeito de Frey, também conhecido como Efeito Auditivo de Micro-ondas, descreve a percepção de estalidos e sons induzidos pela emissão de frequências rádio ao indivíduo, sem recurso a qualquer aparelho eletrónico.

14 - O Código de Nuremberga é um conjunto de princípios éticos sobre a pesquisa com seres humanos.

poluição eletromagnética e química de partículas ambientais, a excitabilidade cortical, resposta inflamatória e o stress celular poderem ser alterados em seres humanos, usando por base evidências que a poluição eletromagnética pode aumentar os efeitos de alguns outros poluentes, como o stress celular induzido por exposição a metais.

Tudo isto leva a comunidade científica a urgir a realização de experiências independentes e a elaboração de novos limites para a exposição a radiações eletromagnéticas que tenham em conta estas realidades.

Além de que nenhum aparelho nas telecomunicações é testado em termos de segurança de uso, apenas controlado ao nível da emissão de radiações.

De referir que a quase totalidade dos testes referidos em curso na União Europeia se focam no seu funcionamento técnico, e também nos media, no entretenimento, nos transportes e nos veículos autónomos.

E depois há a dúvida principal: a radiação proveniente da tecnologia móvel é perigosa? Como o mundo está prestes a entrar na era 5G, engenheiros, físicos, biólogos e médicos podem olhar para milhares de estudos e cálculos sobre os efeitos dos campos electromagnéticos de radiofrequência na saúde nas anteriores tecnologias 2G e 3G. Mas há um forte desacordo quanto à forma de interpretar os resultados - e as implicações para a rede 5G, para as quais há uma particular falta de estudos científicos.

Na sua guia de 2020, a ICNIRP (International Commission on Non-Ionizing Radiation Protection), assume a limitação da literatura científica atual para avaliar com precisão os riscos da radiação não-ionizante, e em especial na faixa das micro-ondas. A comissão declara então fazer uso de modelação teórica, generalizações, deduções e palpites educados conservadores para colmatar a falta de segurança nas suas conclusões ou incapacidade de chegar a elas, de forma a procurar assegurar a prevenção de efeitos nocivos da exposição a campos eletromagnéticos.

A seguradora Swiss Re adverte para o perigo da testagem dos produtos não ser representativa das utilizações reais, especialmente em casos de novos produtos que são comercializados rapidamente para muitos utilizadores, na possibilidade de levar a eventos danosos.

Tudo isto contribui para uma sociedade onde surgem e proliferam doenças e mortes sem explicação. Pela falta de investigação sobre os efeitos das alterações introduzidas - incluindo as tecnológicas como o 5G - nos ambientes humanos, e naturais.

6.1 - A controvérsia à volta das entidades de avaliação do risco radiológico a nível internacional

Um grupo de cientistas domina as entidades que devem fornecer aconselhamento sobre o risco de radiação. Isto significa que a investigação "certificada", que chega ao radar dos políticos que têm de utilizar a ciência para fazer leis e regulamentos, é limitada.

Isto constitui um monopólio de opinião, diz Einar Flydal. O antigo cientista da Telenor na Noruega é autor do livro "Smart meters, the law and health". Flydal critica a base científica que está na base das decisões políticas sobre os limites de segurança radiológica que se aplicam na maioria dos países.

"A maioria dos investigadores são definidos como dissidentes e são simplesmente excluídos através de um processo que não se entende do ponto de vista ético. Isto não pode ser compreendido a partir de resultados científicos. Deve ser entendido politicamente, como o resultado de uma batalha de interesses em que as autoridades de proteção contra as radiações se tornam frequentemente peões com falta de recursos", afirma Flydal.

Existe muita discussão sobre o tema dos efeitos das radiações eletromagnéticas na saúde e nos ecossistemas, levando a um espectro de opiniões sobre o assunto.

As autoridades de segurança radiológica na Europa recebem aconselhamento de algumas ou de todas estas organizações científicas:

- A Comissão Internacional para a Protecção contra as Radiações Não Ionizantes, ICNIRP;
- O Comité Científico da Saúde, Ambiente e Riscos Emergentes da UE, SCENIHR / SCHEER;
- O Grupo CEM da Organização Mundial de Saúde da OMS;
- Unidade sobre o Cancro da OMS, IARC, Agência Internacional de Investigação sobre o Cancro;
- O Conselho Científico sobre Campos Electromagnéticos da Autoridade Sueca para a Segurança das Radiações;
- O Grupo de Especialistas em Radiação Não-Ionizante, AGNIR, (um comité científico britânico que existiu até 2017).

Estes grupos deviam garantir uma vasta gama de pareceres científicos. No entanto, não é esse o caso.

A ICNIRP é particularmente influente, pois não só avalia a investigação sobre as radiações e os riscos para a saúde, como também fornece orientações para os limites de segurança que a maioria dos países utiliza. Trata-se de uma organização privada, registada na Alemanha, nos arredores de Munique, e que funciona atrás de uma porta amarela nas instalações do gabinete federal alemão para a proteção contra as radiações. As decisões sobre quem são os cientistas que fazem parte da organização são tomadas pela própria ICNIRP.

"A ICNIRP não tem um processo aberto para a eleição dos seus novos membros. É um grupo que se auto-perpetua, não sendo permitida a discordância. Porque é que isto não é problemático", pergunta Louis Slesin, editor da publicação Microwave News, em Nova Iorque. Ele tem acompanhado o debate científico sobre radiação e saúde durante décadas.

"Não há cientistas altamente qualificados em número suficiente", explica Mike Repacholi, um pioneiro da investigação sobre radiação que fundou a ICNIRP em 1992. A investigação excluída muitas vezes não satisfaz normas elevadas, acrescenta Eric van Rongen, director da ICNIRP. "Não somos contra a inclusão de cientistas que pensam de forma diferente. Mas eles têm de preencher o perfil numa posição específica e não podem ser aceites apenas pelas suas opiniões dissidentes", diz van Rongen.

A ICNIRP é, de facto, a organização que estabelece os limites de segurança radiológica em grande parte da Europa. Ainda assim, é apenas um de entre vários grupos científicos. No entanto, os grupos são, em grau notável, compostos pelos mesmos peritos.

Dos 13 cientistas da ICNIRP, seis são membros de, pelo menos, um outro comité. No grupo da OMS, isto aplica-se a seis em cada sete. Um em cada três investigadores da comissão da UE que emitiu pareceres sobre radiações em 2015 esteve representado noutros grupos.

Isto não é assim tão estranho, de acordo com Gunnhild Oftedal. Ela é membro tanto da comissão ICNIRP como do grupo de investigação da OMS. "Pede-se às pessoas que demonstrem ter competências. Vejam quem tem assento em conselhos de administração e conselhos em geral, é assim em toda a sociedade", diz.

Os conflitos na investigação sobre os campos electro-magnéticos (CEM) têm raízes longas. Historicamente, a ciência neste domínio tem estado associada ao sector das telecomunicações e ao sector militar. Os limites de segurança da ICNIRP têm sobretudo em conta as necessidades da indústria das telecomunicações, afirma Dariusz Leszczynski, antigo investigador de longa data da agência finlandesa de proteção contra as radiações.

Leszczynski não está representado no ICNIRP, nem noutros grupos de peritos de renome. "O objectivo da ICNIRP é estabelecer limites de segurança que não matem as pessoas, enquanto a tecnologia funciona", ironiza.

Este cientista repete a crítica feita por Louis Slesin, o editor do Microwave News. "Há muita política para decidir o que entra num estudo e o que fica de fora". Por exemplo, excluir pessoas com mais de 60 anos de um estudo sobre tumores cerebrais na Austrália, publicado

recentemente, não faz qualquer sentido", diz Slesin, salientando que a maioria dos tumores cerebrais aparece em grupos etários mais velhos.

Este estudo específico, feito por dois cientistas também representados na ICNIRP, concluiu que não pode haver ligação entre os telemóveis e os tumores cerebrais, porque a incidência de cancro cerebral na população em geral tem sido estável há anos. Mas essa conclusão contrasta fortemente com um trabalho publicado em Inglaterra em 2018 que revelou um crescimento, para mais do dobro, do glioblastoma, o tipo mais agressivo de tumor cerebral, entre 1995 e 2015.

Também em 2018 foi lançada uma revisão sobre a epidemiologia do cancro (de Anthony B. Miller, Lloyd Morgan, Iris Udasin e Devra Lee Davis) que afirma risco acrescido de tumores no cérebro, nervo vestibular e glândulas salivares associado com o uso do telemóvel. Referindo 9 estudos (2011–2017) reportando um risco acrescido de tumores cerebrais associados ao uso do telemóvel. Também abordava 4 estudos (3 em 2013, 1 em 2014) afirmando um risco acrescido de tumores no nervo vestibular. Afirma também uma ligação com tumores benignos como o meningioma e o Schwannoma Vestibular. Declara também preocupação com outros tipos de cancro, nomeadamente de mama (em homens e mulheres), leucemia, da tiróide e testículos. A revisão apoia a passagem da classificação corrente do risco de radiação de radiofrequência, pela Agência Internacional para a Investigação do Cancro, de possível carcinogénico (Grupo 2B) para carcinogénico para seres humanos (Grupo 1).

Existe frequentemente uma ligação entre as conclusões dos estudos e a fonte do dinheiro que pagou a investigação. A ciência financiada pela indústria é menos suscetível de encontrar riscos para a saúde do que os estudos pagos pelas instituições ou autoridades.

O dinheiro da investigação vai frequentemente para as universidades e tem "biombos" entre o cientista individual e o dinheiro, diz Lennart Hardell, médico e cientista do hospital universitário de Örebro, na Suécia. "O problema é, no entanto, que se fica dependente desse dinheiro. A maioria das pessoas não morde a mão que as alimenta", acredita o investigador sueco.

Hardell estuda as ligações entre a utilização de tecnologias móveis a longo prazo e o cancro do cérebro, e concluiu que uma pode causar a outra. Ele fez parte do comité do IARC em 2011, mas não está representado em outros comités. Segundo Hardell, a sua investigação é financiada pelo seu salário do hospital, bem como por fundos angariados por fundações locais de combate ao cancro e por organizações nacionais. "Claro que também trabalhei muito nos meus tempos livres", afirma.

Martin Röösli é professor associado do Instituto Suíço de Saúde Pública e é membro da ICNIRP e de outros órgãos consultivos. "Os estudos financiados exclusivamente pela indústria são suscetíveis de ser tendenciosos", confirma Röösli ao Investigate Europe. Mas, no seu estudo, os modelos financeiros mistos, com mecanismos de salvaguarda adequados, não resultaram em resultados de investigação tendenciosos - e tinham uma qualidade mais

elevada. Pode também haver resultados preferidos em qualquer campo, afirma Röösl: "Os investigadores podem criar incertezas para angariar fundos para a sua investigação".

Alguns estudos podem prolongar-se por 15 a 20 anos. Tais projetos são pão e manteiga para os investigadores, argumenta Louis Slesin. Alguns estudos são financiados pela indústria. "Será que isto constitui um conflito de interesses para os cientistas envolvidos?", pergunta Slesin - e responde: "Claro que sim".

Gunnhild Oftedal não descarta que a fonte de financiamento pode afetar as conclusões - tal como "uma forte convicção de que se vai encontrar alguma coisa" pode.

Nem todos querem denunciar o dinheiro dos negócios. A indústria deveria, sem dúvida, pagar pela investigação dos potenciais perigos dos seus produtos; mas esta só deveria ser realizada independentemente dos financiadores, pensa Zenon Sienkiewicz, um fisiologista britânico, que faz parte da comissão da ICNIRP e que já fez parte de outros organismos consultivos.

A investigação está criticamente dependente de financiamento externo, acrescenta o antigo cientista da ICNIRP Norbert Leitgeb, professor no Instituto de Engenharia dos Cuidados de Saúde da Universidade de Tecnologia de Graz, na Áustria. "A questão não é saber se a indústria forneceu dinheiro, o que deveria fazer se os seus produtos são motivo de preocupação. A questão importante é saber se existem barreiras eficientes que garantam que as partes interessadas não podem interferir com os investigadores e influenciar os resultados ou conclusões científicas", afirma.

O debate sobre um potencial enviesamento da indústria ignora um potencial enviesamento contrário, de ONG e grupos de pressão privados, afirma Leitgeb. "Grupos como o das pessoas que dizem ter hipersensibilidade eletromagnética deveriam merecer a mesma atenção".

Mike Repacholi fundou a ICNIRP, bem como o projecto CEM da OMS. No início, o projecto da OMS recebeu um financiamento substancial da indústria. Ao deixar a OMS, Repacholi tornou-se um consultor da indústria.

"Tem havido tantas críticas à investigação financiada pela indústria que a indústria não financia agora a investigação. No entanto, são eles que estão na origem das preocupações com a saúde. Quem perdeu com esta situação?", pergunta Repacholi.

No entanto, tanto a ICNIRP como a OMS excluem agora os investigadores que receberam apoio da indústria ao longo dos últimos três anos.

O "núcleo" de cientistas da OMS tem vindo a trabalhar desde 2012, e esperava-se que a sua investigação estivesse concluída há muito tempo. Mas as alegações de unilateralidade também assolaram este comité. Agora, a OMS vai criar um grupo de investigação mais alargado que avaliará o trabalho do "núcleo" inicial e o expandirá. Os participantes ainda não foram nomeados, mas incluirão "um amplo espectro de opiniões e conhecimentos

especializados", garante um porta-voz da OMS ao Investigate Europe. Esta avaliação abrangerá áreas como a relação entre campos eletromagnéticos e o cancro, efeitos reprodutivos adversos e efeitos da exposição ao calor de qualquer fonte na dor, queimadura, cataratas e doenças relacionadas com o calor.

Muitos críticos dos organismos dominantes de investigação dos CEM, e dos seus laços históricos com a indústria, comparam a situação com a forma como os fabricantes de tabaco conseguiram manter a dúvida sobre se fumar era perigoso. "Não gosto dessa comparação, porque aí os efeitos nocivos são claros, ao passo que com os CEM ainda estamos a adivinhar quão grande ou pequeno é o problema", diz Louis Slesin.

A lição a tirar da questão do tabaco, pensa ele, é ter cuidado para não dar demasiado acesso e influência à indústria. "Em 2000, a OMS publicou um importante relatório em que fez mea culpa sobre a forma como permitiu à indústria tabaqueira influenciar o seu pensamento", lembra Slesin.

A FCC afirma que "não encontra base apropriada para e assim declina propor emendas aos seus limites em existência nesta altura [2019]". Os limites de segurança sobre a exposição humana à radiofrequência da FCC estão quase inalterados deste 1998.

O mundo da tecnologia, e das telecomunicações, sofreu uma revolução desde 1998, mas, mesmo com novos e melhorados instrumentos de medição e mais experimentos, os limites permaneceram aproximadamente os mesmos, até para exposições superiores 6 GHz (que estão na ordem do dia por causa da tecnologia 5G pretender utilizar essa faixa).

E é de notar que a FCC sustenta a sua decisão sobre o 5G na posição oficial de alguns organismos de saúde pública (nomeadamente a Food & Drug Administration [FDA], Organização Mundial de Saúde, a American Cancer Society e o National Institutes of Health) de não afirmação da tecnologia de micro-ondas como responsável por problemas de saúde humana, ou outros biológicos. O que por si só não assegura que não cause problemas de saúde ou ambientais.

A maior parte da investigação sobre as radiações da tecnologia móvel e a saúde foi feita sobre as tecnologias 2G e 3G. Sobre a tecnologia 5G não há praticamente estudos sobre os seus efeitos biológicos. E os estudos sobre micro-ondas que existem são secretos. Mas também não se sabe qual será a modulação do sinal utilizada na nova tecnologia.

E assim, nos próximos anos, a super-rápida 5G será implantada e utilizará, em parte, frequências muito mais elevadas do que as que foram utilizadas anteriormente. Os conhecimentos científicos sobre o que isto pode significar para a saúde pública são mínimos.

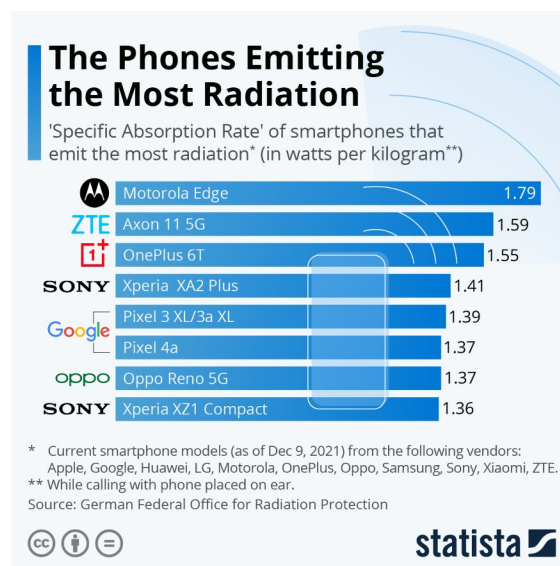
O responsável da ICNIRP, Eric van Rongen, concorda, porém, com os críticos numa questão: é necessária mais investigação.

"Absolutamente. Há ainda muita incerteza. Por exemplo, sabemos muito pouco sobre os efeitos a longo prazo da utilização móvel no cancro do cérebro, para tirar conclusões. Precisamos absolutamente de mais informação", garante Rongen.

Sendo relevante que, como denunciado na investigação jornalística pan-europeia "The 5G Mass Experiment", dos 14 cientistas, no ICNIRP, responsáveis pela elaboração da guia de segurança sobre campos eletromagnéticos associados aos telemóveis, 10 tinham recebido fundos da indústria de telecomunicações. A conclusão foi que estes membros do ICNIRP faziam parte de um pequeno círculo de insiders que rejeita investigação alarmamente, servindo efetivamente os seus empregadores das telecomunicações ao estabelecer limites de exposição pouco exigentes.

6.2 - A questão da radiação emitida pelos telemóveis

Em 2022, o instituto de pesquisa Statistica elaborou um infográfico que apresenta os smartphones, de marcas de maior renome internacional, que emitem mais radiações eletromagnéticas quando o telemóvel está encostado ao ouvido, de acordo com a taxa de absorção específica (SAR) em modelos disponíveis no mercado:



O gráfico acima foi feito com base em análises do Ministério da Proteção contra a Radiação alemão (Bundesamt für Strahlenschutz [BfS]), que compilou uma base de dados sobre telemóveis vendidos oficialmente no país e a radiação por eles emitida, em valores SAR (medidos a nível da orelha e do corpo), que atualiza regularmente. Ela está disponível em:

http://www.bfs.de/SiteGlobals/Forms/Suche/BfS/DE/SARsuche_Formular.html?gts=6048912_list%253DSAREar_double%252Bdesc&csstring_SARAdditional=aktuell

Na legislação Europeia é exigida uma inspeção aos aparelhos móveis dos fabricantes ao nível das emissões de radiações eletromagnéticas, a fim de verificar se estão a cumprir com os regulamentos estipulados. Mas este exame técnico é feito por entidades terceiras acreditadas pela União Europeia e os estados-membros, podendo em circunstâncias específicas (nomeadamente se o produto for fabricado na União Europeia), ser assegurado o cumprimento dos regulamentos europeus pelas empresas que fabricam os produtos.

Mas já foi observado experimentalmente que os níveis de radiação, ao contacto com o corpo, que os telemóveis emitem excedem em 1.6 a 3.7 vezes os limites de radiação recomendados pela União Europeia em termos de valores de SAR, nas distâncias que se podem considerar mais comuns no uso (0 a 5 mm do corpo).

E já houve um escândalo nos Estados Unidos, quando um meio de comunicação social inspecionou a radiação eletromagnética emitida por telemóveis da Apple, Samsung e Motorola, e verificou que poucos aparelhos cumpriam com os regulamentos de segurança sobre a emissão de radiações eletromagnéticas, o que deveria ter sido assegurado por testes aprovados pela entidade supervisora FCC (Comissão Federal de Comunicações).

A Apple esteve mesmo a mãos com uma ação em tribunal por emissões de radiações eletromagnéticas por alguns dos seus modelos acima dos valores estipulados pela FCC (Federal Communications Commission) nos Estados Unidos. Mas foi arquivada, num processo algo turbulento.

7 - Efeitos na biologia animal e vegetal associados às micro-ondas

O Comité Científico da Saúde, Ambiente e Riscos Emergentes (Scientific Committee on Health, Environmental and Emerging Risks - SCHEER), em substituição do antigo Comité Científico dos Riscos para a Saúde Emergentes e Recentemente Identificados (Scientific Committee on Emerging and Newly Identified Health Risks - SCENIHR), avaliou a escala e o nível de interação na futura relação entre a tecnologia 5G e ecossistemas e espécies em termos de possíveis perigos, assim como a urgência em estudar estes itens, como elevada, em 2018. Sugeriu que poderia haver consequências biológicas de um ambiente 5G, devido ao facto de não existirem "provas claras para informar o desenvolvimento de guias de exposição à tecnologia 5G".

Com relação a isto, existe um estudo (Everaert J, Bauwens D., A possible effect of electromagnetic radiation from mobile phone base stations on the number of breeding house sparrows [*Passer domesticus*]. *Electromagn Biol Med* 2007; 26: 63–72) que reportou que as populações reprodutoras de pardais decresciam de forma muito significativa, durante a época

de acasalamento, com a proximidade de transmissores de telecomunicações móveis GSM, associados a campos eletromagnéticos operando nas frequências de 900 MHz ou 1800 MHz, e de ambas estas bandas. Os dados mostram que menos pardais machos foram vistos em locais com campos eletromagnéticos de intensidade relativamente alta associados a estações base GSM, apoiando a hipótese de que exposição a longo prazo a altos níveis de radiação afeta negativamente a abundância ou o comportamento de pardais na natureza.

O doutor Ron Melnick supervisionou o estudo mais caro de toxicidade financiado pelo estado norte americano (30 milhões de dólares), com o intuito de estudar o efeito das radiações eletromagnéticas utilizadas nos telemóveis em ratos. Com o protocolo avaliado rigorosamente por oficiais das instituições EPA (United States Environmental Protection Agency), FDA (United States Food and Drug Administration), NIOSH (National Institute for Occupational Safety and Health), e a BEMS (Bioelectromagnetics Society), entre outras. Deste escrutínio a conclusão unânime foi que este seria o mais autoritário estudo animal conduzido nos Estados Unidos para avaliar o risco na saúde humana. O estudo, publicado em 2018, encontrou cancro e outros efeitos nos ratos expostos a radiações eletromagnéticas associadas a telemóveis. A FDA rejeitou então o estudo, e reiterou que "as evidências científicas disponíveis até à data [2018] não apoiam efeitos negativos na saúde [humana]".

Pouco depois da publicação do estudo anterior, em Bolonha (Itália) um grupo de investigadores do Instituto Ramazzini - um laboratório de investigação sobre o cancro sem fins lucrativos - divulgou os resultados do seu estudo sobre os efeitos na saúde da radiação eletromagnética. Esta equipa analisou os efeitos de fontes distantes de radiação, como torres de telecomunicações. Os resultados apontavam para um aumento de tumores nas células gliais e tumores de Schwann em células do coração, em ratos. Este estudo, também, foi ignorado pela FDA.

Em 2003, um neurocirurgião, de nome Leif Salford, verificou experimentalmente que frequências de micro-ondas moduladas matavam células nos cérebros de ratos. Segundo Salford, o cérebro de um rato é muito semelhante ao de um ser humano, fazendo acreditar que aquilo que se passou com os ratos se possa passar em seres humanos. E isto muito abaixo das restrições impostas pela FCC (Federal Communications Commission) nos Estados Unidos (que são significativamente mais exigentes que os aplicados na União Europeia).

As micro-ondas emitidas por torres de telecomunicação afetam organismos que vivem na vizinhança, como vertebrados, insetos, vegetais, e seres humanos. Pequenos organismos são especialmente vulneráveis, pelo seu tamanho reduzido que facilita a penetração das radiações eletromagnéticas nos tecidos internos, incluindo o sistema nervoso central, quando existente.

Há estudos que apontam para o efeito negativo no meio ambiente e nos ecossistemas das ondas eletromagnéticas, tendo sido observadas a redução da produção de trigo (Soya et al., 2003), alteração na concentração de cálcio em raízes de ervilhas (Belyavskaya, 2001), alterações na distribuição de cromatina nas células do meristema expostas a campos magnéticos fracos (Belyavskaya, 2001), o crescimento atrofiado em pinheiros (Balodis et al, 1996), a aceleração na produção de resina, a aceleração do envelhecimento e a diminuição da germinação das sementes (Selga & Selga, 1996), isto também em pinheiros.

As micro-ondas foram relacionadas com o declínio da saúde das plantas (Tanner & Romero-Sierra, 1974), o declínio da concentração de cálcio e enxofre nas folhas de árvores da espécie faia-europeia (na relação direta da intensidade da exposição) (Schmutz et al., 1996), mudanças citogenéticas no trigo (Pavel et al., 1998), e nas células animais foram observados efeitos na comunicação intercelular e nos canais de cálcio (Dutta et al, 1989).

Mas o efeito das micro-ondas pulsadas (muito semelhantes à moderna telefonia sem fios) na vegetação não é todo igual. Cada espécie se comporta de forma diferente com a exposição. Não parece afetar os carvalhos-americanos (*Quercus rubra*) nem as bétulas-do-papel (*Betula papyrifera*). Os pinheiros-vermelhos (*Pinus resinosa*) tiveram o seu crescimento acentuado. O álamo tremedor (*Populus tremuloides*) e o bordo vermelho (*Acer rubrum*) viram aumentar a sua espessura (Kiernan, 1995).

Foi corroborado que campos eletromagnéticos estáticos têm um efeito estimulante no crescimento e desenvolvimento de plantas, mas um efeito inibidor no caso da exposição a campos eletromagnéticos variáveis (Martinez et al., 2003).

Foram feitos estudos sobre a exposição de anfíbios a radiação eletromagnética, pela sua importância nos ecossistemas e fiabilidade como bio-indicadores; os ovos de anfíbio estão diretamente expostos à radiação eletromagnética.

A poluição eletromagnética é considerada como uma causa possível de deformações (falta ou excesso de membros), de mudanças no ritmo cardíaco (Levitina, 1966), de arteríolas dilatadas e de declínio de algumas populações anfíbias.

Um estudo de 2 meses, em Valladolid, Espanha, sobre a exposição de óvulos e girinos do sapo (*Rana temporaria*) a radiação eletromagnética de várias antenas de rádio localizadas a uma distância de 140 metros, verificou uma proporção anormal de baixa coordenação de movimentos, crescimento assíncrono, resultando em grandes e pequenos girinos, e uma taxa de mortalidade na ordem dos 90%. Em comparação, o grupo de controlo, dentro de uma gaiola de Faraday, desenvolveu uma coordenação de movimentos normal e crescimento síncrono, e apresentou uma taxa de mortalidade de 4.2% (Balmori, 2010).

O declínio em espécies anfíbias está associado com cursos de água a altitudes elevadas nos trópicos, e negativamente associado com águas paradas e baixas elevações. Em lugares elevados, a contaminação eletromagnética é geralmente maior.

Há evidências de efeitos atérmicos em aves.

Várias experiências com ovos de aves mostraram uma mortalidade elevada de embriões expostos a radiação eletromagnética de telemóveis.

As radiações eletromagnéticas alteram os sistemas imunitário, nervoso e endócrino e operam independentemente ou em conjunto com outros fatores tóxicos como radiação ultravioleta e poluentes químicos. Este tipo de exposição causa stress no sistema imunitário, que impede a reparação do ADN.

Também nos animais existe diferentes graus de suscetibilidade a radiação eletromagnética entre as espécies, e mesmo entre populações.

Estudos também encontram efeitos sobre os insetos, com consequências previsíveis nos ecossistemas, pela importância da função dos insetos na natureza.

Panagopoulos et al. (2004) expuseram moscas-da-fruta (*Drosophila melanogaster*) à radiação de um telemóvel móvel (900 MHz) durante os primeiros 2 a 5 dias de vida adulta. A capacidade reprodutiva da espécie decresceu de 50% a 60% em condições de radiação modulada (emissão que se produz enquanto se fala ao telemóvel) e 15% a 20% na exposição a radiação não modulada (com o telemóvel em repouso). A descida da capacidade reprodutiva aconteceu em ambos os sexos, ainda que tenha afetado mais as fêmeas que os machos. Os resultados deste trabalho indicam que esta radiação afeta o desenvolvimento sexual dos insetos de uma forma atérmica (sem aumento da temperatura).

Panagopoulos e a sua equipa, em 2002, também investigaram os efeitos de campos eletromagnéticos na descendência da mosca-da-fruta, observando:

- a) um decrescimento significativo na ordem dos 6% da capacidade reprodutiva quando exposta a campos eletromagnéticos alternados;
- b) um incremento da capacidade reprodutiva na ordem dos 40% com a exposição a campos eletromagnéticos pulsados;
- c) um decrescimento dramático da capacidade reprodutiva, de 60%, com a exposição a radiações da tecnologia GSM (da 2ª geração de telecomunicações móveis).

Os autores concluíram que as radiofrequências, especificamente de GSM, são altamente bioativas e provocam alterações significativas nas funções biológicas dos organismos vivos, pelo que recomendam evitá-las. Notam que, em especial, a oogénese e a espermatogénese são etapas muito sensíveis a factores externos.

Em outro estudo sobre as moscas-da-fruta, no qual foram expostas à radiação de um telemóvel, se observou um aumento da concentração da proteína do stress (hsp70), que normalmente é sintetizada quando as células são expostas a condições ambientais adversas, assim como um aumento da fosforilação na transcrição nuclear, e, surpreendentemente, um aumento da fecundidade (Weisbrot et al., 2003).

Um investigador da Universidade de Doz (Austria) e apicultor aficionado, Ferdinand Ruzicka, descreveu como os problemas com as suas abelhas (*Apis cerana*) começaram com a instalação de várias antenas celulares perto das suas 40 colmeias (a 50 metros de uma estação base e a 150 metros de outras três) em 2003. Ele observou sintomas de stress e o colapso das colónias de abelhas quando as antenas começaram a emitir. O mesmo foi observado por outros apicultores (F. Ruzicka, com. pers.). A princípio se produziu uma grande desordem e uma tendência pronunciada à formação de enxames. No verão teve lugar um invulgar decréscimo nas populações das colmeias. No inverno, apesar do frio e da neve, e do facto de

terem pólen armazenado do outono, as abelhas saíram das colmeias, com a morte de exemplares. Ele associou estes problemas à exposição a radiação eletromagnética das antenas de rádio, e, com esta ideia, realizou um levantamento junto dos apicultores austríacos. Dos 25 apicultores que tinham antenas de telecomunicações perto das suas colmeias, 37,5% observaram um aumento de agressividade, 25% observaram uma tendência significativa à formação de enxames, e 62,5% observaram o desaparecimento de colônias.

Em um estudo realizado na Alemanha sobre abelhas, poucas abelhas irradiadas voltaram para as colmeias e demoraram mais tempo a fazê-lo, e o peso das colmeias destas abelhas diminuiu com a exposição.

Um crescente volume de testemunhos de pessoas e observações indicam que as moscas e as aranhas, entre outros insetos, desapareceram das áreas afetadas pelos campos eletromagnéticos das antenas de telecomunicações, onde se experimenta os níveis mais elevados de radiação (A. Soria, com. pers. e observações próprias). Desconhece-se se ocorre um abandono das áreas ou a morte das espécies que vivem nestas zonas, mas há uma tendência a evitar as micro-ondas pulsadas por parte dos animais.

As radiofrequências induzem efeitos biológicos em biomoléculas, que incluem mudanças na concentração iônica intracelular, proliferação celular, interferências com o sistema imunitário, interferência com a capacidade reprodutiva de animais, efeitos na concentração das hormonas do stress, efeitos em desenvolvimento no útero, efeitos sobre os genes, efeitos no sistema nervoso, efeitos no sistema circulatório, e um decrescimento no número de nascimentos.

A variação da intensidade e frequência do campo eletromagnético na proximidade de uma antena de rádio, devido ao número de ligações ativas e ao tipo de comunicações, torna-o mais bioativo que os campos eletromagnéticos constantes, possivelmente porque é muito difícil para os organismos vivos adaptarem-se a ele, o que pode tornar a vida na sua proximidade complicada (Panagopoulos et al, 2004).

A própria SCHEER (Scientific Committee on Health, Environmental, and Emerging Risks) europeia declarou o 5G como risco emergente de alto impacto em 2018. O comité europeu declarou que “no horizonte, uma nova geração de ainda mais curtos comprimentos de onda de alta frequência 5G está sendo proposta para alimentar a Internet das Coisas (Internet of Things, IoT). A IoT promete-nos estilos de vida fáceis e convenientes com uma rede de telecomunicações interconectada massiva de 5G. No entanto, a expansão da banda larga com radiação de radiofrequência de mais curto comprimento de onda realça a preocupação que problemas de saúde e a segurança permanecem ignorados. A controvérsia continua em relação a danos das tecnologias wireless de 2G, 3G e 4G atuais. As tecnologias 5G estão bem menos estudadas para efeitos ambientais e humanos”, e conclui que “redes de 5G serão em breve lançadas para utilizadores de telemóveis e aparelhos inteligentes. Como a exposição a campos eletromagnéticos pode afetar seres humanos mantém-se um tema controverso, e estudos ainda não apresentaram prova conclusiva do impacto em mamíferos, aves, ou insetos. Esta falta de evidências claras para informar o desenvolvimento de guias

sobre a exposição à tecnologia 5G deixa em aberto a possibilidade de consequências biológicas não intencionais.”

Sendo alarmante notar que não há uma séria preocupação e regulamentação que proteja a vida não-humana de exposições a radiações eletromagnéticas, na Europa ou nos Estados Unidos da América, apresentando uma visão muito redutora e insensível aos efeitos dos campos eletromagnéticos no meio e nos seres vivos em geral.

De acordo com um relatório recente, em 2022 a rede 5G vai conseguir atingir mais de mil milhões de ligações. O relatório aponta ainda que em 2025 a rede ultra rápida poderá alcançar um total de 25% de todas as ligações a nível mundial. A China deverá ser o país onde o 5G será mais fortemente impulsionado. A consultora previa que ainda em 2020 o número de equipamentos 5G na China ultrapassasse os 100 milhões. E ainda que este país ultrapasse sozinho a marca de mil milhões de conexões em 2024.

E segundo os dados partilhados pelo Ericsson Mobility Report, e citados por comunicado pela Altice Portugal, estima-se que, nos próximos cinco anos (até inclusivé 2027), o número de subscrições 5G atinja os 4,4 mil milhões em todo o mundo, metade de todas as subscrições móveis.

No mesmo relatório da Ericsson de 2021, é afirmado que no final de 2021 haveriam 660 milhões de subscrições de redes 5G em todo o mundo. A procura acima do esperado nos mercados da China e América do Norte explicariam este crescimento, assim como a redução dos preços dos smartphones com aquela tecnologia. O que comprovava, tal como previsto, que a nova geração móvel será a de mais rápida implementação até agora.

E a nova geração móvel 5G está bem posicionada para se tornar na tecnologia de acesso móvel dominante por subscrições a nível global até 2027. Por essa altura, perspetiva-se que o 5G represente cerca de 50 por cento de todas as subscrições móveis mundiais - abrangendo 75% da população mundial e representando 62% do tráfego global de smartphones.

Mas isto não leva curiosamente à pressão internacional ao financiamento de estudos para uma determinação precisa das condições para a segura exposição a campos eletromagnéticos e suas consequências biológicas, perante todos os interesses e *lobbies* (alguns deles muito pouco claros) que compõem e pressionam a uma adoção extremamente rápida de novas tecnologias, sem devido e prudente escrutínio.

E se este otimismo despreocupado é de facto válido, porque não fazer estudos independentes sobre o impacto da tecnologia 5G a nível ambiental, incluindo na saúde humana, antes de avançar para a sua adoção massiva e rápida a nível global?

8 - Verdades e perigos do crescente vício à tecnologia

Estima-se que pelo mundo fora aproximadamente 4 milhares de milhões de pessoas estejam conectadas online, com mais de 90% usando aparelhos móveis e gastando várias horas por dia no mundo virtual. A que acresce a dificuldade de fazer um uso saudável dos smartphones, tablets e portáteis, e da Internet wireless e móvel, que geralmente resvala, pelo menos durante períodos para um uso desregrado e compulsivo - vicioso -, que tendencialmente aumentará significativamente com a multiplicação de serviços online, contribuindo para a continuada deterioração das relações humanas e sociais.

Isto é corroborado pelo relatório Mobility Report da Ericsson de 2021, que declara que se registou um aumento de quase 300 vezes no tráfego de dados móveis desde 2011, e que o ritmo de mudança está a acelerar.

Os aparelhos e aplicações móveis são centrais para o que tem sido uma transformação fundamental no comportamento das pessoas. As *apps* passaram a orquestrar as nossas vidas, para o bem e para o mal.

Com o CoV-Sars-2, a confusão e o pânico gerados, confinamento, os períodos de isolamento decretados e as regras de distanciamento obrigatório, houve um aumento massivo de consumo de Internet nos primeiros quatro meses de 2020, quer por entidades quer por particulares, e também um aumento significativo no consumo de apps, e em especial jogos. Aumentou o nosso uso, e a nossa dependência, dos telemóveis, tablets, computadores e plataformas informáticas como mensageiros, redes sociais, aplicações de entretenimento e para trabalho.

A tecnologia informática tem criado coisas maravilhosas no mundo, com as muitas mudanças significativas sistémicas que têm ocorrido pelas possibilidades que elas criaram. Como a facilitação da comunicação em tempo real à volta do globo. Mas também têm permitido o exacerbamento de traços negativos humanos e da nossa civilização, que nos ajudaram a chegar a este estado tumultuoso e precário civilizacional em que vivemos.

Atualmente nós podemos nos isolar totalmente numa bolha com tecnologia.

Desde o surgimento comercial do motor de busca Google tem se popularizado um novo tipo de economia, muitas vezes erradamente catalogada, que assenta sobre a coleção massiva de dados e a monopolização da atenção do consumidor tanto quanto o possível, vendendo a clientes a capacidade de mudar gradual, ligeira e impercetivelmente a nossa percepção e comportamento através de aplicações informáticas e de lucrar com isso. Isto tem levado ao aperfeiçoamento de designs persuasivos e viciantes para captar e manter a atenção do utilizador, e condicioná-lo, fazendo do consumidor (a sua atenção, os seus dados e as suas preferências) o produto à venda, e das relações estimuladas e permitidas pelo serviço comercial, ocorrências financiados por interesses terceiros escondidos.

E como a tecnologia tem conduzido a experiências cada vez mais virtuais e abstratas (como as redes sociais), semelhantes no seu estilo a videojogos, naturalmente produz desumanização nos indivíduos, conduzindo a pessoas menos compassivas, empáticas, e mais frias e calculistas, mais sádicas e masoquistas.

Também nos videojogos se tem popularizado o paradigma “live service” que, empregando técnicas da psicologia, procura monopolizar a atenção dos jogadores de forma contínua, tentando que esses produtos de entretenimento se transformem em espaços digitais onde os consumidores joguem, vivam, se relacionem, trabalhem e gastem frequentemente o seu dinheiro sobre a forma de microtransações.

E o modo incognito do Google Chrome é reportado como enganador em e-mails da Google, não oferecendo verdadeira privacidade ao utilizador.

Assim como testes feitos no iPhone apontam que, contrariamente ao que a Apple afirma publicamente, são recolhidas informações identificativas do aparelho e do utilizador, que violam a privacidade deste.

Como afirmou Satya Nadella, presidente da Microsoft: “Nós estamos a sair de um mundo onde o poder de computação era escasso para um lugar onde é agora quase ilimitado, e onde o recurso verdadeiramente escasso é cada vez mais a atenção humana.”

A própria Microsoft reconheceu num relatório, em 2015, que o vício à tecnologia era evidente, particularmente nos jovens.

E o componente viciante nos telemóveis e tablets poderá não ser o aparelho em si e nem tanto a nossa falta de força de vontade de nos desligarmos dele, mas a forma de funcionamento das suas aplicações. As apps nos aparelhos móveis (telemóveis e tablets) foram desenhados para monopolizar a nossa atenção e nos manter ligados tanto quanto possível, com a informação que constante e metodicamente oferecem, e detrás da qual escondem toda a sua operação.

Aproveitam-se do nosso vício em obter recompensas, e da dose química de dopamina e de oxitocina que nos condicionam, e causa bem estar. Como as *slot machines* e o jogo antes delas, as apps destes aparelhos capitalizam num fenómeno chamado de “reforço intermitente”.

Considerado por psicólogos como o mais poderoso motivador, o reforço intermitente assenta na aleatoriedade na receção de recompensas. O investigador B. F. Skinner verificou experimentalmente, com pombos, que a antecipação da recompensa motivava mais a cobaia a procurar a recompensa. Cria-se a expectativa da recompensa, mas não se sabe quando ocorrerá ou mesmo se seremos recompensados de todo, o que cria excitação (do jogo).

E este conhecimento científico e as equipas de profissionais com formação na área da psicologia humana que vendem as suas capacidades às empresas de software as ajudam a

tornar as suas aplicações viciantes para os seus utilizadores e a manipulá-los, ignorando questões éticas, sem leis eficazes que as supervisionem.

A ex-diretora de Política Pública Global da Meta e denunciante Sarah Wynn-Williams afirmou perante os senadores dos EUA numa audiência nesta quarta-feira, dia 10, que a Meta direcionou anúncios publicitários a adolescentes com base no seu estado emocional.

“[A Meta] conseguia identificar quando [os adolescentes] se sentiam inúteis, desamparados ou fracassados e pegavam nessas informações e partilhavam-nas com os anunciantes”, afirmou Wynn-Williams de acordo com o site TechCrunch. “Os anunciantes entendem que, quando as pessoas não se sentem bem consigo próprias, é a altura certa para apresentar um produto porque é mais provável que as pessoas o comprem”.

A ex-diretora da Meta explicou que, por exemplo, se uma adolescente apagasse uma selfie numa das redes sociais da empresa, essa informação seria usada pelos anunciantes como um sinal de que era uma boa altura para exibir um produto de beleza - uma vez que a ação apontava que não se sentia bem com a sua aparência.

O fenómeno do reforço intermitente pode ser observado no jogo tradicional, nos videojogos, nas redes sociais (Facebook, Twitter, TikTok, Instagram, etc.), mensageiros (Whatsapp, Facebook Messenger, etc.) e outras aplicações informáticas, incluindo apps.

Por exemplo, nos jogos populares classificados como “free-to-play” ou “freemium”, populares em especial nos dispositivos móveis, que não cobram dinheiro inicialmente pela sua utilização, mas que pressionam a gastar dinheiro com microtransações apresentadas dentro do jogo, usando para isso mecânicas predatórias, incluindo sorteios de recompensas com uso a sistemas de rifas (Gatcha) e recurso a técnicas de pressão social (de colegas, amigos, familiares, conhecidos, pessoas na mesma faixa etária, outros jogadores). Técnicas que visam fazer os jogadores gastar dinheiro, principalmente aqueles que mais costumam gastar – chamados “baleias”. Isto desenvolvido custosamente, com premeditação, recorrendo à psicologia, de forma a manipular os seus utilizadores. Um exemplo de um jogo assim é Diablo Immortal.

Mas também há jogos pagos que fazem uso destas técnicas de psicologia para manipulação ao gasto em microtransações, chamados normalmente de “Live Service”, como o Gran Turismo 7, para as consolas Playstation 4 e 5. E jogos igualmente pagos que têm modos que pressionam ao gasto em microtransações, como o Call of Duty e o FIFA, ambos disponíveis para várias plataformas incluindo consolas e computadores.

E estas microtransações, podem pelo nome parecer muito “baratas” [que podem não necessariamente ser, podendo chegar dezenas ou mesmo centenas de euros, dependendo do jogo] ou sem grande importância, mas, por exemplo, Diablo Immortal anunciou ganhos na ordem de 100 milhões de dólares em dois meses de atividade, somente com microtransações.

O governo chinês reconhecendo estes males na indústria dos videojogos tem nos últimos anos criado legislação devido ao problema do vício dos videojogos. Em 2021, a China

estabeleceu tempos de jogos rígidos para os menores de 18 anos e suspendeu a aprovação de novos jogos no mercado chinês por cerca de 8 meses.

E agora no dia 22 de dezembro de 2023 anunciou novas propostas de legislação que limitariam o valor monetário gasto em jogos online. A reação dos investidores a isto foi de pânico, causando uma perda de cerca de 80 milhões de euros em valor de mercado das duas maiores empresas de videojogos chinesas, Tencent e NetEase. Também empresas estrangeiras viram a sua cotação em bolsa diminuir no seguimento deste anúncio, como a Roblox, Electronic Arts, Unity Software e a Ubisoft.

Os jogos online na China ficariam proibidos de dar aos jogadores prémios de assiduidade, e por gastarem dinheiro nos serviços, assim como proibia a disponibilização de mecânicas Gacha a menores e a especulação e o leilão de itens virtuais, procurando com isto proibir estratégias comuns de incentivo ao investimento pessoal e de maximização da faturação nos jogos online. Os jogos também passariam a incluir um limite máximo de depósito de dinheiro na conta para gastos nestes serviços.

A remoção destes incentivos provavelmente reduziria o número de utilizadores diários e a faturação das aplicações, poderia forçar as editoras a mudar fundamentalmente o seu design dos seus produtos e estratégias de monetização, e afetar o mercado de videojogos a nível global a longo prazo.

Mas poucas horas depois as autoridades chinesas vieram anunciar que as novas propostas de legislação para os videojogos online podem ser revistas tendo em conta as opiniões e os receios das partes envolvidas.

Doutora Hilarie Cash afirma que há evidências muito fortes de que, no início da infância, os ecrãs interativos são hipnotizantes para as crianças. E que os ecrãs interativos são aqueles com o maior potencial para serem viciantes.

Atualmente há também uma hipermediatização do jogo online em Portugal, ao qual o primeiro ministro português, Luís Montenegro, se viu associado ao ter a empresa familiar a que estava ligado a receber 4.500€ mensais do grupo Solverde durante algum tempo. Esta hipermediatização condiciona fortemente a população em Portugal a jogar, e em especial os já viciados ao jogo, criando mais miséria.

Estas aplicações sobrecarregam e excedem as nossas fraquezas biológicas e humanas, e estão na raiz do vício à tecnologia, da polarização social, radicalização, idolatria, enraivecimento cultural.

A controvérsia, o medo, a raiva e a polarização prendem a atenção dos utilizadores às aplicações (como no caso do Youtube) e criam oportunidade para as empresas tecnológicas lucrarem.

E as notícias falsas propagam-se mais rapidamente e dão dinheiro a ganhar. A verdade é normalmente séria, aborrecida e neutra.

Existe um famoso episódio de manipulação furtiva nas redes sociais - uma experiência de contágio de escala massiva - na qual a empresa Facebook (agora chamada Meta), em 2010, procurou influenciar subliminarmente os utilizadores americanos na sua navegação das suas páginas para que votassem nas eleições, com sucesso. O investigador que liderou a experiência afirmou que “se queremos tornar o mundo num lugar melhor numa escala massiva, nós devemos nos focar não apenas em mudar o comportamento de uma pessoa, mas também em utilizar a rede para influenciar os amigos da pessoa”. Ou seja, manipulação subtil.

Posteriormente foram feitas outras experiências de contágio de escala massiva usando o Facebook, como em 2014, a chamada “Evidência experimental de contágio emocional de escala massiva através de redes sociais”, com o objetivo de entender se emoções podem ser transferidas na ausência de interações físicas e de linguagem não verbal. Na altura desconhecia-se se era possível, tendo este estudo verificado experimentalmente possíveis efeitos no comportamento em proporção, individualmente, reduzida. Lançando-se a hipótese de que em redes sociais massivas, estes efeitos subtis se acumulariam - com os utilizadores e as interações - tornando-se mais significativos, como viria a ser demonstrado em 2016, pelos escândalos da influência da consultora Cambridge Analytica na consulta pública sobre o Brexit no Reino Unido e da interferência russa nas eleições presidenciais americanas.

Também disto são exemplos os desafios virais nas redes sociais, nomeadamente do TikTok, alguns deles extremamente perigosos, que podem conduzir a problemas de saúde e até mesmo à morte, como o desafio do blackout da que já levou à morte de várias crianças.

Se virmos alguma moda online (como por exemplo um desafio do TikTok) e se outras pessoas a catalogarem como um desafio ou divertido ou interessante, acabam por estar a retratar isso como um jogo social, condicionando a nossa percepção do tema, e a diminuir a nossa consciência para os seus perigos e a diminuir a nossa prudência. **A isto é preciso atenção.**

O Facebook e outras plataformas digitais funcionam como ferramentas de persuasão.

Com isto estas empresas tecnológicas tornam um conjunto de ações mais prováveis e outro menos provável nos seus utilizadores através do condicionamento do comportamento destes. Em milhares, milhões ou até milhares de milhões de pessoas.

Cada vez que pegamos no telemóvel e o ligamos antecipamos uma recompensa. Normalmente nos satisfazemos e procuramos criar a possibilidade de receber mais recompensas. A partir de determinada altura já nos sentimos condicionados a procurar as aplicações por “gatilhos internos”, que tendencialmente são estados emocionais negativos, que nos conduzem a usar as aplicações sem qualquer notificação da app. Aborrecimento, solidão, ... Criamos nós próprios os gatilhos que nos impelem a usar as apps e funcionalidades destes aparelhos.

Estas aplicações informáticas procuram fazer gestão do equilíbrio de prazer-dor e de estados de défice de dopamina na psicologia do utilizador, com o seu processo de estimulação, procurando prender a atenção dos utilizadores ao serviço.

Estes programas usam os nossos amigos, as notificações, Inteligência Artificial para descobrir, prever e fazer uso daquilo que se prevê nos irá viciar, ou prender ao ecrã, ou manipular, ou permitir que os publicitados testem em nós o seu marketing digital para descobrir a forma de nos seduzir. E uma vez descoberta uma fórmula mais eficiente para nos seduzir, repetem-na e procuram melhorá-la. Este fenómeno constitui uma nova forma de poder e influência enormes, obtida por estas empresas tecnológicas, na qual nós participamos ativa e passivamente.

E recentemente, impulsionado pelo feminismo e a procura de igualdade de direitos e aceitação social das minorias nos países ocidentais, incluindo na legislação, e pela tendência social e corporativa a abraçar um movimento geral progressista cultural, na Internet tem-se vindo a experimentar um fenómeno de censura e de repressão de expressões consideradas como hostis ou politicamente incorretas nas redes sociais e em fóruns, o que tem conduzido a uma autocensura interna e mudança do comportamento individual de forma a não se sofrer sanções e ser silenciado nestes espaços. Tem conduzido a aquilo que já foi chamado de uma espiral de silêncio.

Esta é uma forma de manipulação – distinta da televisão ou da imprensa – mais subtil, mais insidiosa, difícil de controlar e perigosa. Que evolui rápida e continuamente. E mesmo sabendo como esta tecnologia funciona não nos torna imunes à sua sedução e ao vício.

A Microsoft revelou, em 2015, que os Canadianos tinham dificuldade em manter a atenção. E que isto tinha um impacto significativo no equilíbrio da vida de trabalho, particularmente para entusiastas da tecnologia e de media. Com 44% dos Canadianos tendo que se esforçar muito para se concentrar nas tarefas, 45% perdendo o foco com pensamentos e imaginações não-relacionadas e com 37% das pessoas não fazendo bom uso do seu tempo e tendo que trabalhar mais tarde ou aos fins-de-semana para compensar.

Esta tecnologia usa a evolução humana e o associado imperativo biológico de nos relacionarmos socialmente com outras pessoas – viver em comunidades, encontrar parceiro sexual, propagar a espécie -, que diretamente afeta a libertação de dopamina no cérebro e a sensação de prazer, para manipular o utilizador.

A tecnologia e o seu modelo económico de retenção da atenção transformaram as interações sociais humanas. Interromperam o fluxo normal das conversas de uma forma que tem sido incrivelmente prejudicial para as nossas relações sociais, prejudicial para a nossa empatia, e para a forma como aprendemos a comunicar ao longo de milhares de anos de evolução. E conduzindo ao isolamento físico social, à dificuldade de comunicar em pessoa de uma forma autêntica, fazer contacto visual, ler expressões faciais e comunicar eficazmente de forma não verbal, e à diminuição de relações sociais tradicionais (no mundo real).

Este modelo de retenção da atenção, nas redes sociais e outras plataformas com uma componente social, afeta também a perceção de valor pessoal e a auto-confiança, e a identidade, pondo-nos perante problemáticas para os quais não fomos preparados. A nossa evolução tornou-nos sensíveis para o que as pessoas à nossa volta pensam de nós. E estamos preparados para lidar com o que milhares ou milhões de pessoas opinam sobre nós???

E esta pressão social dá espaço ao bullying, à fraude e ao assédio online.

Tudo isto alimentado por algoritmos opacos de disponibilização de conteúdo das redes sociais e outros serviços online, que procuram prender a atenção do utilizador. Estes algoritmos estão associados a experiência de conteúdo extremo, a problemas de imagem do corpo, insatisfação, dismorfia corporal e distúrbios alimentares, segundo o artigo “The dangers of the rabbit hole: Reflections on social media as a portal into a distorted world of edited bodies and eating disorder risk and the role of algorithms”, produzido por Jennifer A. Harriger, Joshua A. Evans, J. Kevin Thompson, e Tracy L. Tylka.

E isto é tão mais acentuado pelo facto de consciente e inconscientemente, com a evolução da tecnologia e do capitalismo, chegamos a uma época de “personal branding”, onde as pessoas são estimuladas a fundir a vida profissional e pessoal, fazendo de si próprias marcas, com o objetivo de se tornarem produtos e vender a sua imagem. Disto são exemplo os influencers das páginas de Internet, redes sociais e serviços de streaming (como o Youtube), que procuram influenciar o seu público e as modas, com objetivo social e, frequentemente, financeiro. [Não é por acaso que ser famoso se tornou um objetivo social tão popular contemporaneamente.]

Mas começa também já a haver uma reação ao “personal branding”, com pessoas a procurarem o anonimato online e offline, quer através do uso da tecnologia, de presença online mascarada e até procurando não se deixar identificar publicamente nas suas interações ou comportamentos, porque não vêm na identificação pública com as suas próprias ações um bem, com medo de ver a sua presença online, ou até opiniões captadas, invadir e afetar negativamente a sua vida real.

A relação difícil com a tecnologia está também associada ao fenómeno que se chama de Fear Of Missing Out (FOMO), ou o medo de isolamento social e de perda pessoal por não ter uma determinada experiência. Assim como ao medo do tempo de silêncio, de vazio e das coisas que o podem popular, quando desligamos o ecrã. Isto condiciona-nos a normalmente procurar o ligar outra vez. E isto é associado a um aumento da ansiedade, perturbação mental e depressão.

Um estudo recente do Pew Research Center revelou que cerca de 46% dos americanos dizia não poder viver sem o seu telemóvel. Embora o sentimento seja hiperbólico, cada vez mais pessoas estão a ficar mais dependentes dos telemóveis e outros dispositivos eletrónicos portáteis.

Segundo um artigo científico de 2017, da Universidade Korea de Seul, Coreia do Sul, Hyung Suk Seo, médico, professor de neuroradiologia e seus colegas, identificaram um

desequilíbrio químico encontrado em viciados, adolescentes, ao telemóvel e à Internet. Um excesso de ácido gama-aminobutírico (GABA) no córtex cingulado anterior. Este é um neurotransmissor que inibe ou desacelera a transmissão de sinais no cérebro, associado com a visão, o controlo motor e a regulação de várias funções cerebrais, incluindo a ansiedade. O excesso de GABA pode resultar em efeitos secundários, incluindo sonolência e ansiedade. Uma boa notícia do estudo é que este desequilíbrio foi observado decrescer de forma significativa ou mesmo normalizar após terapia cognitivo-comportamental (TCC).

Os investigadores também encontraram uma ligação entre estes vícios - à tecnologia e ao telemóvel - e depressão, ansiedade, insónia severa e impulsividade nos testados.

Estamos a ser educados de que - quando estamos desconfortáveis, sós ou medrosos - temos um pacificador digital que nos distrai. Isto nos atrofia a habilidade de, autonomamente, lidarmos com estes estados de espírito, condicionando o desenvolvimento de uma dependência à tecnologia. Sendo isto exacerbado pela visão contemporânea do desconforto e do sofrimento como somente indesejáveis.

E esta fixação aos dispositivos móveis contribui para dificuldades relacionais - e até fenómenos de retaliação – devido à dificuldade de desligar e dar atenção aos interlocutores ao vivo.

E, inclusive, a dificuldade nas comunicações digitais e no acesso às redes sociais geram desconforto e ansiedade, pela incapacidade de usar a tecnologia como esperado, num fenómeno conhecido mundialmente como nomofobia (no mobile). Sentimos isto, por exemplo, quando nos esquecemos do telemóvel em casa, sentimos pânico (aumento da frequência cardíaca, inquietação) pela falta dele e voltamos atrás para o buscar.

Existe também uma moda conhecida informalmente como Dismorfia do Snapchat, na qual jovens procuram cirurgia cosmética para se assemelharem ao seu look em selfies usando filtros visuais que apresentam resultados irreais, e favorecem o surgimento de problemas de imagem, e, em casos extremos, distúrbios alimentares.

Este ambiente tecnológico que existe contribui para uma sociedade que procura apresentar e manter permanentemente uma imagem de beleza, sucesso e perfeição pessoal, recompensada com estes estímulos a curto-prazo (gostos, polegares para cima, corações, *smileys*) e comentários positivos, que nós confundimos com valores reais e com verdade. Mas na realidade é popularidade momentânea, frágil, a curto-prazo, que nos deixa ainda mais vazios e sôfregos de atenção do que antes de a experimentarmos. Ajudando a nos tornar mais ansiosos, frágeis e deprimidos. Sendo associado a depressão, automutilação e suicídio.

E as mudanças de padrões de comportamento, por condicionamento digital, refletem-se em alterações neurológicas, criando predisposição ao comportamento aditivo, e em especial à experiência da dopamina. Estimula o sistema límbico, a amígdala e a reação de lutar ou fugir. Afetando o desenvolvimento mental das crianças, a sua criatividade, atenção, e as suas capacidades cognitivas.

O estudo intitulado “Windows of developmental sensitivity to social media” publicado na revista Nature Communications, de investigadores das universidades de Cambridge e Oxford, e do Donders Institute for Brain, estabeleceu a ligação, a nível populacional, entre uso de redes sociais e a experiência de menos bem-estar pessoal. Apontando as idades de 11-13 para raparigas, 14-15 para rapazes e 19 anos para ambos os sexos como os períodos, em geral, onde ocorre uma relação mais negativa entre uso de redes sociais e satisfação com a vida. Embora a relação entre uso de redes sociais e satisfação com a vida seja caracterizada como bastante negativa no princípio da adolescência. E um uso maior das redes sociais também prediz uma menor satisfação com a vida passado 1 ano (e o contrário: menor uso de redes sociais e mais satisfação de vida também é verificado) na faixa etária dos 10 aos 21 anos.

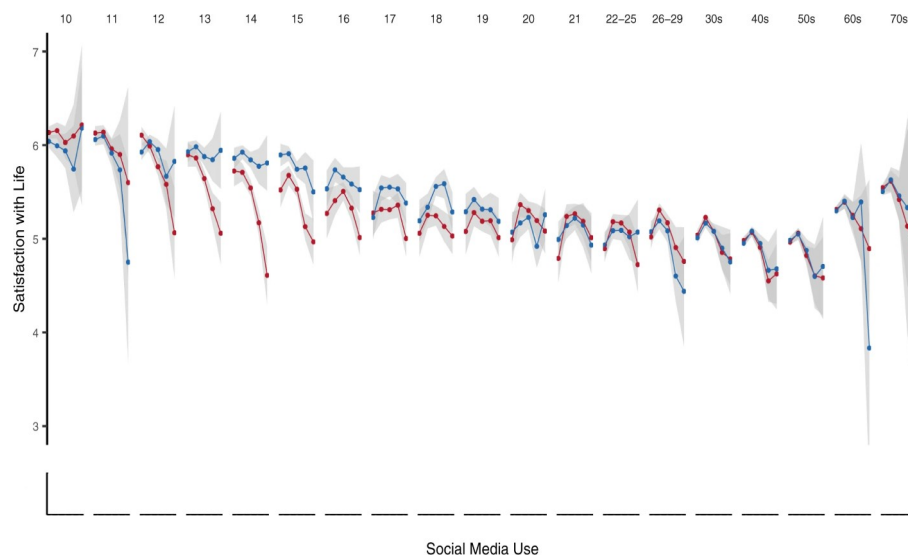


Ilustração 6: Gráfico apresentando a relação entre o uso estimado de redes sociais e reportado nível de satisfação com a vida em diferentes faixas etárias verificado dentro do estudo Windows of developmental sensitivity to social media.

Estes resultados sugerem que mudanças associadas ao crescimento, tais como no desenvolvimento da estrutura do cérebro e na puberdade, e também mudanças nas nossas circunstâncias de vida - como mudança de meio escolar – parecem nos tornar mais vulneráveis aos efeitos negativos das redes sociais em alturas particulares da nossa vida. Como o fazem na adolescência. Com o impacto do uso das redes sociais a variar de acordo com a idade e o sexo.

E tão mais é importante a atenção à tecnologia e aos seus efeitos pela capacidade dela, nomeadamente das redes sociais, de servir, em especial para os jovens, para ajudar a realizar os seus impulsos de socializar, de se afirmar socialmente, exprimir a sua criatividade, até por pressão dos pares.

E isto é especialmente preocupante pelo facto do cérebro dos pré-adolescentes e adolescentes não estar totalmente desenvolvido, nomeadamente o córtex pré-frontal, que lhes dá menor capacidade para auto-regulação e auto-disciplina, favorecendo o comportamento impulsivo. Que se alia à natural imaturidade e entusiasmo próprios destas idades.

O político republicano americano Jordan Cunningham declarou publicamente que “sabemos que certas empresas gigantes das redes sociais desenham os seus produtos para viciar crianças, e um número significativo dessas crianças sofre danos sérios como resultado... como depressão, ideação suicida, ansiedade, desordens alimentares. Proteger crianças online não é só senso comum, salvará vidas”.

E a tecnologia pelo seu imediatismo, que nos entretém, condiciona por si própria já um comportamento impulsivo no seu utilizador.

E estatisticamente a capacidade de prestar atenção em seres humanos tem vindo progressivamente a diminuir – determinada em 2013, em média, nos 8 segundos. Um segundo menos que um peixinho dourado. Convertendo-se isto num problema cada vez mais premente.

A atenção a longo prazo diminui com a utilização de sistemas informáticos, uso de redes sociais e literacia digital.

Um relatório da Microsoft, sobre atenção, de 2015, dirigido a vendedores, afirma que o impacto social que a utilização de redes sociais tem na sustentação da atenção está dependente do tipo de utilização de tecnologia e do ambiente. Utilizadores frequentes de redes sociais prestam mais atenção em ambientes interativos (digitais), e são piores comparativamente em experiências mais passivas. E também processam informação e memorizam-na mais eficientemente.

Também utilizadores mais antigos de tecnologias de informação têm menor atenção a longo prazo, mas mais períodos de elevada atenção a curto prazo. Assim como utilizadores mais antigos prestam mais atenção aos ecrãs e processam informação melhor que os utilizadores menos experientes. Prestando também menor atenção a fontes de informação passivas, como televisões.

O documento lança a questão:

“Com notícias reduzidas a 140 caracteres e conversas condensadas em emojis, como está isto a afetar a forma como Canadianos vêm e interagem com o mundo?”

E responde:

“Atenção é obviamente um ingrediente necessário para publicidade efetiva, mas os estilos de vida digitais dos canadianos estão a mudar o cérebro, decrescendo a capacidade de foco prolongado e aumentando o seu apetite por mais estímulos.”

E isto expandido, revelando que:

■ “de uma forma geral, estilos de vida digitais diminuem a capacidade de estar focado numa só tarefa, em especial em ambientes não digitais. (...) Consumidores conectados estão-se a tornar melhores a fazerem mais com menos, através de períodos mais curtos de maior atenção e codificação mais eficiente para memória”;

■ “exposição a vários ecrãs treina consumidores a serem piores a ignorar distrações – eles estão cada vez mais desejosos de algo novo. Isto significa mais oportunidades para roubar a atenção, mas também que as marcas precisam de trabalhar mais para mantê-la”.

O neurotransmissor do bem-estar dopamina é fundamental a estes resultados, sendo libertada quando os utilizadores fazem algo que consideram recompensador. Neste caso, a excitação do novo. Os consumidores de tecnologia são especialmente recetivos à novidade, encontrando maior excitação em saltar de experiência em experiência, do que em se concentrar numa só coisa num dado momento.

Fatores fundamentais que impactam a atenção são, segundo o estudo:

- consumo de media;
- uso de redes sociais;
- ritmo da adoção da tecnologia;
- comportamento com a exposição a vários ecrãs.

A quantidade e diversidade de opções e estímulos proporcionados pelas aplicações informáticas ajudam a diminuir a capacidade de atenção.

“[O que a informação consome é] a atenção dos seus recipientes. Então uma riqueza de informação cria uma pobreza de atenção”, segundo o galardoado pelo prémio Nobel Herbert Simon.

A habilidade de filtrar distrações não é afetada quando o utilizador usa só um ecrã. E a performance do indivíduo diminui com o multi-tasking com diferentes fontes de informação (redes sociais, televisão, internet, e-mails, telemóvel, tablet, etc.).

Pessoas com maior capacidade de atenção escolhem experienciar menos distrações e tem menos experiências com vários ecrãs em simultâneo.

Utilizadores frequentes de vários ecrãs, por outro lado, têm dificuldade em filtrar estímulos irrelevantes, vendo-se distraídos mais facilmente por várias fontes de media. E são levados a um estado de excitação que os torna recetivos a experiências mais imersivas de conteúdos digitais, e possivelmente ao vício à tecnologia.

Utilizadores moderados de redes sociais também apresentam, segundo o relatório da Microsoft, maior capacidade de multi-tasking do que utilizadores pouco frequentes. No entanto essa capacidade perde-se com o uso elevado de redes sociais.

As redes sociais têm a capacidade de esgotar as capacidades de um utilizador, reduzir a capacidade de alocar atenção, de conectar com o conteúdo a nível emocional e de processar informação.

E o mais impressionante sobre o documento da Microsoft, para vendedores, é a sua manifesta ausência de espanto ou preocupação sobre a alteração evidente provocada pela tecnologia no comportamento humano. A Microsoft e outras empresas tecnológicas estão conscientes que as suas técnicas e produtos estão a afetar o comportamento humano, com transformações profundas, e em alguns casos claramente negativas, e não manifestam qualquer preocupação ética, não se importam:

“Cérebros estão a ser religados – qualquer mudança em estímulos resulta em uma religação... as técnicas e mecanismos para ativar a rápida transferência de atenção serão extremamente úteis”, segundo Danah Boyd, uma investigadora da Microsoft citada.

“A tecnologia não é uma ameaça ou problema para vendedores, em si”, pode-se ler na apresentação.

E nem os governos, nem os governantes, que elegemos para proteger o povo, ou as agências públicas criadas para salvaguardar o interesse das populações, se interessam o suficiente para se debruçar sobre o tema. **Ninguém defende o interesse público neste assunto.**

“Com o aumento da prevalência da experiência de vários ecrãs, social torna-se integrado em diferentes formas, e consumidores continuam a adotar novas tecnologias, a capacidade de atenção está em geral a diminuir. Esta é uma verdade universal, NÃO é só ‘crianças hoje’”, esclarece a Microsoft no artigo.

Também é causa normal do uso destes aparelhos eletrónicos, pelas longas horas a utilizá-los, a Síndrome de Visual do Computador. Nas palavras da empresa da área do tratamento médico Trofa Saúde, Síndrome de Visual do Computador “caracteriza a responsabilidade por um conjunto de sintomas oculares associados ao uso de computadores ou outros dispositivos eletrónicos, durante um longo período, habitualmente superior a 2 horas”. Nomeadamente sensação de peso/cansaço ocular, cefaleias, sensação de corpo estranho (do olho), irritação/ardor ocular, olho vermelho, lacrimejo, intolerância às lentes de contacto, visão turva para perto ao final do dia, visão turva para longe após estar muito tempo a ver ao perto, lentidão de focagem, dor ao nível da região cervical, ombros e coluna associados à postura utilizada, fadiga, irritabilidade, diminuição da concentração, problemas de sono.

A autora do livro iGen e professora de psicologia Jean Twenge estudou as gerações a partir de 1995, que são as primeiras gerações humanas a passar toda a sua adolescência com smartphones. Afirmo que este facto teve efeitos em cascata através de muitas áreas da vida destas pessoas. Descrevendo pela positiva, a criação de uma ética de trabalho muito forte, grande pragmatismo e grande capacidade de se manterem em segurança. Mas também podem estar demasiado seguras, podendo não estar a ter as experiências autónomas que as ajudam a entrar na fase adulta.

E esta situação é tão mais agravada pelo facto de as redes sociais - mas também outras aplicações como motores de busca ou serviços de streaming de vídeos - usarem algoritmos para editarem os resultados que nos apresentam, de acordo com a informação que adquirem sobre as nossas preferências, nos encerrando em nichos de circulação de informação que espelham em determinada medida as nossas preferências: câmaras de eco. Estas tendem a ser confortáveis e a contribuir para a polarização dos pensamentos e discursos dos utilizadores. Com cada utilizador com a sua experiência online particular, com a sua realidade e os seus factos.

O ser humano tende a aceitar a realidade que lhe é apresentada. E com o tempo adquire a falsa certeza que todos os outros concordam consigo, porque aqueles com que lida frequentemente, dentro da sua câmara de eco, partilham ou toleram, de forma geral, das suas opiniões. Isto o torna mais sugestionável, e diminui a sua capacidade de lidar com informação que contraria a sua perspetiva. Afetando a sua habilidade para a ser um indivíduo objetivo e construtivo. Especialmente em alturas de guerra de informação, como nesta altura de guerra na Ucrânia. Sendo crianças, jovens e idosos, os sectores da população mais vulneráveis à propaganda e às câmaras de eco.

Tudo isto resulta numa prisão comportamental em que ficamos encarcerados. A exploração de vulnerabilidades na psicologia humana por ferramentas que, alterando o comportamento (gostos, preferências e hábitos), nos encham de compulsões e de ansiedades, nos afetam a nossa psicologia – gerando a possibilidade da necessidade de psicoterapia e fármacos - e estão a destruir o tecido social como ainda o conhecemos, influenciando um ambiente tecnológico e social orientado à manipulação, ao vício e à indiferença – à desumanidade.

De acordo com diversos estudos e depoimentos de professores de diversas universidades coletados pelo jornal turco Türkiye Today, os jovens atualmente ficaram tão acostumados a usar teclados que acabam “entrando em choque” ao saltar da escrita digital para a tradicional. Como qualquer habilidade que é lentamente perdida pelo não uso, os alunos agora demonstram uma maior dificuldade em escrever no papel, uma perda considerável na caligrafia, muitas vezes torta na página, e apresentam uma letra ilegível.

Motivados pelo uso das redes sociais como meio de comunicação, os alunos muitas vezes evitam frases longas ou não conseguem construir parágrafos significativos. A Gen Z não só tem mais dificuldade em escrever e se comunicar de forma eficaz, mas, independentemente de fazê-lo manualmente ou com teclado, não consegue criar parágrafos com frases independentes, o que torna mais caótico e difícil a tentativa de compreensão dos seus textos.

No entanto a capacidade de síntese melhorou significativamente, mas a longo prazo torna o aprofundamento em tópicos mais complexos especialmente difícil.

Além de que os serviços que estas empresas tecnológicas fornecem distorcem o sentido da comunicação, e da cultura, associando-as a manipulação e dissimulação, oferecendo um

péssimo exemplo à sociedade, em especial às gerações que crescem com a *social media* e a resignificação subtil que operam as plataformas digitais.

E guiados e manipulados pelos algoritmos [a forma de funcionamento] destas *apps* (por exemplo das redes sociais) a comunicação entre os seres humanos tem sofrido, e com ela a democracia. Estas aplicações prosperam com os sentimentos fortes que garantem a atenção dos utilizadores (como o ódio), alimentando a divisão.

Estas empresas tecnológicas conquistaram o espaço público, mas não tomam responsabilidade nem são responsabilizadas pelo seu efeito nas populações, na sociedade, nos próprios seres humanos.

Juízes do United States Court of Appeals for the Fifth Circuit pretendem dar ao governo do estado americano do Texas poder para controlar a área da moderação de conteúdo das grandes redes sociais. Isto acontece porque, alegam os políticos conservadores, as redes sociais descriminam o discurso conservador. Procurando assim favorecer a política conservadora na Internet.

A própria seguradora Swiss Re afirma que este tipo de práticas antiéticas quando descobertas e tornadas públicas podem manchar a reputação da empresa, salientando que o acréscimo de atenção a estas práticas de design de programas pode levar a intervenção regulatória (política).

A FTC (Federal Trade Commission) americana está a começar a se debruçar sobre os chamados “padrões negros” decetivos utilizados por empresas online, dividindo-os em 4 tipos:

- 1) induzindo falsas crenças;
- 2) escondendo informação;
- 3) impondo custos não-autorizados;
- 4) subvertendo escolhas de privacidade.

O que todas estas categorias partilham são práticas de design enganosas, com a intenção de publicitar, transmitir informação, transmitir urgência, obstruir ação do cliente, esconder informação, adição furtiva de produtos e custos, interferência não-solicitada a nível do interface do cliente, coação ou condicionar a escolha de forma indevida.

E corroborando as expetativas da Swiss Re, o presidente Biden pediu ao congresso americano para implementar novas leis para aumentar a segurança infantil nas redes sociais. “É altura de fortalecer as proteções de privacidade, banir publicidade orientada a crianças, exigir que as empresas tecnológicas parem de recolher informação pessoal sobre as nossas crianças”, declarou o presidente americano. Concluindo ainda que “nós devemos responsabilizar as plataformas das redes sociais pela experiência nacional que eles conduzem nas nossas crianças por lucro”.

O governo americano também planeia alocar, no próximo ano, 5 milhões de dólares no orçamento para investigar o impacto na saúde mental das redes sociais.

E, entretanto, foi submetido ao senado americano o projeto-lei Kids Online Safety Act (KOSA), que assenta na censura e vigilância do conteúdo apresentado a menores (com 16 anos ou menos), na partilha de dados do funcionamento da plataforma respeitante ao serviço a menores com inspetores e investigadores, e no estabelecimento de estipulações para pesquisa de mercado em plataformas online sobre menores (16 anos ou menos).

Também os legisladores do estado da Califórnia avançaram com propostas de lei para proteger o bem estar das crianças nas redes sociais. Tendo sido assinada pelo governador Gavin Newsom a legislação conhecida como California Age-Appropriate Design Code Act, passando-a efetivamente a lei no estado da Califórnia, nos Estados Unidos da América.

Estes desenvolvimentos nos Estados Unidos aconteceram depois da denunciante, e ex-empregada do Facebook, Frances Haugen ter acusado a empresa mãe do Facebook (Meta) de ignorar a segurança das crianças na plataforma numa audiência no congresso. "... o que precisamos de fazer é tornar a plataforma mais segura através de escolhas de design", aconselhou Frances ao comité, sugerindo a ideia de adicionar "fricção" na partilha de conteúdo que poderá reduzir a propagação de desinformação.

Sendo que, apesar das demonstrações públicas de preocupação ao mais alto nível político americano, passar legislação no congresso dos Estados Unidos será previsivelmente uma batalha consideravelmente difícil, em função do lobbying que as maiores empresas tecnológicas - Google, Apple, Meta e Amazon - fazem. No ano de 2021 gastaram mais de 55 milhões de dólares em lobbying ao governo federal americano. Em 2020 gastaram 34 milhões de dólares.

E também outras empresas tecnológicas, em particular a Oracle, Microsoft, Epic e Fox Corp também fazem lobbying ao sistema político.

No entanto mais de uma dúzia de outras empresas tecnológicas, entre elas a Proton e a DuckDuckGo, urge os congressistas americanos a passarem legislação anti-monopólio para o mercado tecnológico. Na perspetivas destas empresas, isto permitiria lidar com conduta anti-competitiva e com as falhas na privacidade online.

Dentro da União Europeia as multinacionais da área da tecnologia também fazem lobby, mas apesar disto a Comissão Europeia está-se a preparar para aplicar, a partir de outubro de 2022, leis anti-monopólio para os mercados digitais sob a designação de Digital Markets Act (DMA), com a Apple a se lamentar, afirmando que podem criar vulnerabilidades à privacidade e segurança dos utilizadores.

De referir que do escândalo sobre a espionagem da empresa Oracle sobre a Microsoft veio-se a saber que ambas as empresas financiam supostas organizações independentes da área das tecnologias, como forma de procurar influenciar a opinião pública sobre estas empresas.

A doutora Amy Orben, da Universidade de Cambridge, aconselha a toda a gente a refletir sobre o seu uso de redes sociais e a encorajar essas conversas.

E segundo o professor Andrew Przybylski, Director de Investigação no Oxford Internet Institute, precisamos de iniciar a conversa sobre o que os jovens fazem, a razão porque usam as redes sociais, o que eles sentem acerca delas e a forma como isto se integra na vida familiar.

É recomendável controlar o tempo que dedicamos ao telemóvel e outros meios informáticos, que nos permite controlar a dependência que sentimos em relação à incapacidade e ao desconforto e ansiedade de não podermos aceder a eles, as suas aplicações e a comunicar com eles.

Precisamos de pedagogia no uso destes aparelhos ubíquos no nosso dia-a-dia, no nosso trabalho, tempos livres, atividades, que em determinados contextos se assume como essencial. É recomendável aprendermos a nos controlar no seu uso, saindo de contextos de dependência. [Há uma secção com alguns conselhos importantes sobre o uso responsável da tecnologia nos anexos deste documento.]

Nas palavras de Richard Branson: “Não te tornes em um escravo à tecnologia – gere o teu telemóvel, não deixes que ele te gira a ti.”

A natureza predatória da tecnologia é muito bem capturada pela música Reaktion da banda RezoDrone:

“(Agora!) Eu te mostro tudo
(Agora mesmo!) A verdade por detrás do véu
(Agora!) Eu te dou tudo
(Agora mesmo!) Então te tiro tudo, [tudo] para longe!

O amor é uma reação
Apenas uma distração
Um jogo que eu sempre jogarei
Tu podes ser o único
Não apenas o solitário
Mas tu continuas a fugir

O tempo é uma ilusão
Não faças confusão
Há apenas o aqui e o agora
Porque és tu a razão
Que eu estou a acreditar
Que nós podemos ter liberdade de alguma forma?

(...)

Sufocando na tua ilusão
Fatalmente ferido
Eu sou só um invólucro desesperado
Levantando-se das cinzas
Quebrado e trágico
Seco num poço desolado

Não precisas de mais um segundo
Apenas toma a pílula e engole
Os teus pensamentos me pertencem agora
O único que tu seguirás

Eu não consigo sentir nada de todo
Como pude eu te deixar
Abrir-me e me ver cair?
Nunca me elevar! (Me elevar! Me elevar!)

(...)"

9 - Os problemas da privacidade online e do crime informático

Para lá disto, o sonho das telecomunicações vertiginosamente mais rápidas do 5G também aumenta o potencial da pirataria informática, e da recolha de dados privados de cidadãos, ao oferecer ligações de Internet muito mais rápidas e de maior capacidade, e também ao servir para concretizar o anseio empresarial de ligar aparelhos eletrónicos do quotidiano e das atividades laborais à Internet (na Internet das Coisas) através da infraestrutura do 5G, avançando na automatização da vida privada e as áreas profissionais.

9.1 - Os problemas da privacidade online e da videovigilância

A empresa Oracle, detentora dos direitos e desenvolvedora da linguagem de programação Java, e do ambiente de desenvolvimento Netbeans, possuidora dos direitos de autor do termo 'Javascript' e desenvolvedora de recursos para esta linguagem de programação, que distribui com o seu software programas antiéticos como a toolbar da Ask e o McAfee Security Scanner, já foi apanhada a espiar a empresa Microsoft, e também a fornecer o software de vigilância online e análise de grandes quantidades de dados Endeca, posteriormente incorporado no software Big Data Discovery, a organizações policiais nos Estados Unidos, na China e em outros países repressivos. Já estabeleceu parcerias com as forças policiais chinesas. E atualmente é alvo de um processo judicial nos Estados Unidos acusada de invasão

da privacidade dos consumidores, sem consentimento, ao usar software de rastreamento para criar dossiês digitais de utilizadores individuais da Internet para efeitos de marketing, de uma forma furtiva, com o serviço “ID Graph”. É alegado que este serviço coleciona informação sobre utilizadores de Internet e infere sobre as suas vidas, incluindo o histórico de compras e eventos de vida (como casamento ou um novo emprego). Também é alegado que a Oracle usa cookies, pixels de rastreamento¹⁵, e até bibliotecas da linguagem Javascript desenvolvidas por si para coletar dados pessoais de forma dissimulada e sem consentimento, incluindo através do uso destas por terceiros sem o seu conhecimento.

A organização dos direitos humanos irlandesa Irish Council for Civil Liberties afirmou, numa declaração, que a “Oracle se gaba de ter dossiês detalhados de 5 milhares de milhões de pessoas e de gerar 42.4 milhares de milhões de euros em ganhos anuais.”

“Os dossiês da Oracle sobre pessoas incluem nomes, moradas, e-mails, compras online e no mundo real, movimentos físicos no mundo real, salário, interesses e orientação política, e um histórico detalhado de atividade online. A Oracle também coordena um mercado global de dossiês sobre pessoas através do Oracle Data Marketplace”, é descrito também na declaração.

TikTok também faz uso de pixéis de rastreamento, e tem vindo a crescer significativamente o seu ramo de publicidade, pelo que se espera que a recolha de dados de utilizadores aumente também de forma expressiva.

O comissário da FCC (Federal Communications Commission) Brendan Carr urgiu à Apple e Google para remover das lojas digitais a aplicação TikTok, afirmando que esta rede social apresenta um risco à segurança nacional americana, devido à sua extensa coleção de dados privados dos utilizadores e ao acesso do estado chinês a esses dados sensíveis.

ByteDance, a empresa mãe do TikTok, realizou uma investigação interna sobre alegadas violações de privacidade, e revelou que quatro funcionários chineses tinham acedido a dados privados de duas contas de jornalistas americanos. Estes funcionários alegadamente foram despedidos.

As plataformas digitais, como o Facebook e o Instagram, estabelecem parcerias comerciais com redes de anunciantes, como a MoPub, vendendo-lhes dados pessoais em tempo real dos seus utilizadores, que são leiloados aos clientes destes serviços, que podem chegar a ser milhares. Um caso polémico disto foi o de um padre americano, cuja informação que partilhava com a plataforma Grindr¹⁶, de 2018 a 2020, permitiu que este fosse exposto como gay e que a sua rotina (incluindo detalhes da sua vida íntima) fosse tornada pública.

Empresas de venda de dados pessoais também comercializam identificadores de pessoas marcadas como “grávidas” ou “a comprar produtos associados com a maternidade”, ou até

15 - Pixel de rastreamento é uma técnica de rastreamento que faz uso de código HTML para sinalizar o comportamento do utilizador

16 - A plataforma Grindr declara que, desde o princípio de 2020, partilha menos dados pessoais com parceiros comerciais que a concorrência, limitando a partilha ao endereço IP, advertising id (identificação do utilizador para publicidade) e a informação necessária para suportar o serviço de publicidade.

reportam a compra de contraceptivos, incluindo alguns dos quais políticos conservadores americanos querem banir ou restringir o acesso.

A empresa Meta (detentora do Facebook, Instagram e Whatsapp) foi condenado a pagar 5 milhares de milhões de dólares à FTC (Federal Trade Commission) por não respeitar a privacidade dos seus utilizadores e oferecer falsas garantias de privacidade e de segurança dos dados pessoais, incluindo partilha de informação de segurança com agentes publicitários, em violação de um acordo prévio com a FTC sobre a privacidade associada às suas plataformas de 2012.

E recentemente foi descoberto que a empresa Meta fazia coleção em websites de hospitais de dados médicos, nomeadamente de consultas, medicações e diagnósticos, em outra violação flagrante da privacidade dos utilizadores de Internet.

O Twitter também foi obrigado a pagar 150 milhões de dólares à FTC, por vender os dados de segurança dos seus utilizadores a agentes publicitários, pelo menos até 2019, quando garantia que estes dados eram só usados para a garantir a segurança dos utilizadores e das suas contas.

Várias apps de saúde mental e ligadas à religião, por sua vez, têm pobre segurança e oferecem pouca ou nenhuma privacidade, e algumas ainda partilham os dados sensíveis dos utilizadores com terceiros, incluindo seguradoras.

A Amazon, empresa conhecida do retalho online, tem construído o seu império de vigilância, com a assistente virtual Alexa, aparelhos inteligentes domésticos, a aquisição da empresa Ring, e do produto Ring Video Doorbell (campainha com transmissão e gravação de vídeo e áudio e ligação à internet), e agora com o processo de compra da empresa iRobot, uma competidora no mercado dos aparelhos inteligentes para a casa. Segundo a Fight for the Future, Electronic Frontier Foundation, International Brotherhood of Teamsters, and Public Citizen, que escreveram uma carta conjunta à FTC sobre o negócio de 1.7 milhares de milhões de dólares, “o acordo proposto apresenta um conjunto importante de preocupações relacionadas com a privacidade dos consumidores e competição no mercado. Deixando a Amazon absorver uma empresa competidora de aparelhos domésticos inteligentes com acesso a dados dos consumidores incrivelmente detalhados poria em perigo a competição justa e os mercados livres enquanto poria em perigo a privacidade dos consumidores.”

A carta também adianta que “não há espaço mais privado que a casa. No entanto com esta aquisição, a Amazon prepara-se para ganhar acesso a dados extremamente íntimos acerca dos nossos espaços mais privados que não estão disponíveis através de outros meios, ou a outros competidores”, incluindo plantas dos espaços, rotinas diárias e escolhas de vida.

“A Amazon usa dados não só para avançar nos seus objetivos anti-competitivos (...), mas também para alimentar algoritmos esfomeados que procuram prever e moldar o comportamento de consumidores individuais. Estes algoritmos, quando associados com o impacto mundial da Amazon, exacerbam racismo e sistemas de opressão preconceituosos sobre o género”, é isto declarado na carta conjunta.

Tudo isto alimenta um Capitalismo da Vigilância digital, que assenta na vigilância tão permanente quanto possível do comportamento individual por empresas tecnológicas, que vendendo visibilidade e publicidade, lucram ao garantir que os publicitados têm tanto sucesso quanto possível, com base nas coleções de dados por elas recolhidos. Assim como alimentam e dão acesso a ferramentas de predição de comportamento aos seus clientes. E também estabelecem parcerias com governos. Com estas atividades, as empresas da Internet (por exemplo das redes sociais) ganham biliões de euros e estatuto, tornando-se nas empresas mais ricas na história da humanidade.

No passado a vigilância era uma prerrogativa do estado político, mas agora é uma espécie de parceria público-privada.

Tudo o que fazemos online é observado, seguido e medido. Cada nossa ação é cuidadosamente monitorizada, gravada e colecionada. E isto alimenta modelos preditivos, em permanente atualização, sobre o nosso comportamento: sobre quem somos, o que fazemos e o que faremos.

A Vodafone e a Deutsche Telekom recentemente começaram ensaios com Trustpid para reintroduzir a localização persistente dos utilizadores, como forma de lucrar com a venda dos dados de utilização dos aparelhos, procurando criar perfis personalizados dos utilizadores.

A que acresce as áreas tecnológicas de serviços assentes na vigilância de pessoas, nomeadamente de alunos e trabalhadores. Serviços como o Gagggle, que devassam totalmente a privacidade online de alunos, com o uso de Inteligência Artificial e supervisores, que muitas vezes não têm qualificação e quase nenhuma formação na empresa para o fazer. Ou como as empresas Crossover e Awareness Technologies, que vendem serviços de vigilância digital de trabalhadores no seu local de trabalho, que monitoram o computador, mas também observam a pessoa, e até as interações com colegas, e combinam estas informações com programas de Inteligência Artificial.

Especialistas temem que o uso deste tipo de software resulte em comportamentos punitivos, em vez de pedagógicos.

E nos Países Baixos uma empresa americana foi condenada por despedir um trabalhador remoto que se recusou a deixar ser observado através da webcam 9 horas por dia, em contradição com o direito ao respeito da vida privada, consagrado pelo Artigo 8 da Convenção Europeia dos Direitos do Homem.

No emprego de software de videovigilância estudantil o propósito predominante parece ser a disciplina do aluno. De acordo com um relatório do Center for Democracy and Technology, 78% dos professores em escolas que usam este tipo de spyware nos Estados Unidos reportaram que alunos, na respetiva escola, já foram sinalizados por este software para punição disciplinar, e 44% dos professores revelaram que a monitorização da atividade dos estudantes já levou a estes serem contactados pela polícia.

Os direitos e a privacidade de estudantes LGBTQ+ também sido afetados pelo emprego desta tecnologia nos Estados Unidos, ao terem conteúdo LGBTQ+ sinalizado erradamente como pornográfico e a serem reportados pelos softwares instâncias do uso de termos relacionados com a orientação sexual, como “gay” e “lésbica”. E, de acordo com o Center for Democracy and Technology, este tipo de software já revelou em vários casos a sexualidade de estudantes aos seus pais sem o seu conhecimento ou autorização, citando 13% dos estudantes americanos.

E isto é tanto mais preocupante quando medidas anti-LGBTQ e anti-aborto vão fazendo o seu percurso nas instituições de poder político à volta do mundo, na esperança de se tornar legislação que condicione a liberdade das populações.

E da Ripply, uma empresa especializada em maratonas de programação baseadas em dados, vem a notícia da criação de um clube privado para pessoas que são líderes no ramo da ciência de dados em Portugal.

Os riscos são que nós estamos a sonambular para uma nova era de hipervigilância, onde pessoas dispersas são monitorizadas, examinadas e julgadas, sem leis de privacidade que acompanhem as repetidas violações de privacidade e os abusos das entidades que empregam estes tipos de software, ou até possivelmente de indivíduos com acesso a estas informações sensíveis sobre quem - por vezes menores – supervisionam.

Diretamente relacionado com isto, nós chegámos a um ponto em que alguma coisa que façamos online dificilmente é privado. Tecnologias de fingerprinting (identificação dos computadores e utilizadores) e rastreamento, como cookies, web beacons, flash cookies, pixel tags, para lá de outras técnicas de coleção de dados mais conspícuas e consentidas (como questionários e diários de consumo) registam as nossas visitas na Internet, as nossas vidas, as nossas preferências e crenças. E sniffers que captam dados de transmissões na Internet, para análise posterior. Tudo isto serve para construir perfis individuais e coletivos das populações, usados posteriormente na manipulação das massas, com publicidade e outras ações. E com uma nova tecnologia de telecomunicações mais potente, e a contínua expansão do mercado da consultadoria e Big Data, esta realidade só terá tendência a aumentar e a se ramificar, com formas mais evoluídas de rastreamento (tracking) e de análise de dados, na procura de prever e condicionar o comportamento das populações, em serviços que se comportam como mercenários, vendendo o seu produto a quem se dispõe a lhes pagar, ou como agentes políticos no controlo das populações.

Há que notar que estas empresas privadas também são usadas e estabelecem parcerias com as agências de espionagem.

Foi revelado por denunciantes, dentro do Departamento da Justiça dos Estados Unidos, que a empresa Meta andou desde as eleições presidenciais de 2020 a vigiar cidadãos americanos e a os denunciar ao FBI por manifestarem posições contra o governo ou contra as autoridades, ou que questionarem as eleições. Uma colaboração feita fora do processo legal e sem causa provável, e, no fim, sem aparentes resultados.

E isto é tanto mais alarmante quando surgem estudos que mostram que há apps, como a da rede social TikTok, capazes de evadir as proteções de privacidade da Google e da Apple, e aceder a todos os dados no telemóvel (incluindo de *tracking*), e até modificar o funcionamento da app sem o consentimento do utilizador.

Investigadores também conseguiram com o recurso a Inteligência Artificial, criar um programa que consegue distinguir jogadores anónimos de xadrez pelo seu estilo de jogo. Algo que se crê que possa vir a permitir identificar pessoas pelo seu estilo de condução ou pelo timing e locais de utilização do smartphone.

Também senadores americanos, depois de mais um assassinio em massa, - em vez de considerarem uma legislação mais apertada para armas de fogo - propuseram ao governo devassar mais a privacidade dos cidadãos americanos, e espiá-los, coletando os dados de seus aparelhos "inteligentes", como do Apple Watch, Fitbit, Amazon Echo, e do Google Home, para prever a sua propensão a comportamento violento e crime, usando inteligência artificial. Aparelhos estes que irão usar a tecnologia 5G para uma maior conectividade e maiores transmissões de dados. E notícias referiam que o então presidente americano, Donald Trump, e o seu governo estavam recetivos à proposta.

Este tipo de vulnerabilidades são especialmente relevantes numa altura em que os nossos aparelhos, casas, carros e cidades estão a fazer a transição para um paradigma "inteligente" e de interconectividade (pela internet).

E isto é agravado pelo facto de que com a massificação de torres celulares trazida com a tecnologia 5G (já discutida anteriormente) será muito mais fácil localizar os dispositivos tecnológicos, e as pessoas com eles. Atualmente existe a possibilidade de obter uma estimativa da localização a todo o momento de todo o telemóvel e tablet (desde que com capacidade de ligação à rede móvel), com estes ligados (sendo que alguns aparelhos eletrónicos com carga nunca verdadeiramente se desligam). Isto num processo de localização com um erro que pode chegar, no máximo, a 72.4205 km de distância, e pode incluir o ângulo em relação à antena de telecomunicações. Mas com o 5G este erro se encurtará a no máximo 457.2 metros, e proporcionará uma estimativa muito mais precisa da localização exata pela massificação das torres celulares 5G e pelo seu curto alcance. E tudo isto sem o uso de qualquer spyware¹⁷.

Porque com spyware, mesmo com o GPS e o telemóvel aparentemente desligados, pela repetida recolha de dados somente de sensores do aparelho eletrónico é possível obter, ao longo do tempo, uma eficácia na localização superior a 90%, de uma forma indetectável. Um investigador, que determinou isto, afirmou sobre o telemóvel que “as pessoas não se apercebem realmente que o seu telemóvel, com acesso a todos estes sensores, é, em algum sentido, potencialmente o melhor aparelho de espionagem que podes imaginar...”.

Spyware em um telemóvel ou tablet atualmente pode impedir o telemóvel de se desligar verdadeiramente e fazê-lo comunicar com a rede celular em intervalos de tempo, ou até

17- Spyware é a classificação de um conjunto de diferentes programas informáticos desenhados para extrair informação de aparelhos informáticos (computadores, telemóveis, tablets) sem consentimento e enviá-la por rede (por exemplo, a Internet).

mesmo incluir GPS próprio, e registrar chamadas, mensagens, atividade em redes sociais, aceder à câmara, e permitir o acesso ao conteúdo do telemóvel e mais. Sendo que existe um mercado legal para este tipo de aplicações para telemóveis e tablets.

Em Israel, a empresa da área de hacking e cibervigilância NSO Group processou o jornal Calcalist pela informação de que o seu software Pegasus teria sido usado pela polícia para espiar dúzias de políticos e ativistas proeminentes. Com a polícia com acesso total a esta ferramenta de hacking de smartphones, usando-a sem necessidade de ordem judicial.

Sendo que a mesma empresa, NSO Group, está a sofrer uma torrente de processos judiciais e escrutínio nos Estados Unidos sobre alegações que o seu software foi usado para hackear membros de governos e dissidentes por todo o mundo.

Entre as vítimas do software da empresa NSO estão membros da Comissão Europeia, advertidos pela Apple.

Uma análise do laboratório Citizen's Lab da Universidade de Toronto revelou também que o governo britânico terá sido alvo em 2020 e 2021 do uso do Pegasus da NSO, perpetrado por Chipre, Jordânia, Índia e Emiratos Árabes Unidos.

Assim como terá sido usado o Pegasus no telemóvel do então ministro francês do ambiente de Édouard Philippe, François de Rugy. Ataque atribuído a Marrocos.

Surgiu a notícia do spyware da NSO ter sido usado no México, sobre jornalistas e ativistas.

E pelo menos 65 políticos e ativistas catalães foram alvo dos spywares Pegasus e Candiru. Os alvos incluíram o presidente do governo catalão Pere Aragonès, membros do parlamento europeu, legisladores catalães, juristas, ativistas e membros das suas famílias. Citizen's Lab afirma que existe forte evidência circunstancial apresentando uma ligação às autoridades espanholas.

O spyware Pegasus, da NSO, também foi usado por governos, da Arábia Saudita ao México, sobre dissidentes e jornalistas.

Isto oficialmente conduziu o governo americano a pôr a empresa NSO na lista negra – para ser evitada e tratada com desconfiança - em novembro de 2021.

A NSO é uma empresa regulada pelo ministério da defesa israelita, e que vende o software Pegasus por todo o mundo. O software, quando infeta com sucesso um telemóvel alvo, pode interceptar chamadas, ver imagens, partilhar a localização do aparelho e funcionar como uma escuta. Oficialmente, a NSO só vende o software Pegasus a governos para vigiar criminosos perigosos e terroristas.

Candiru também é outra empresa israelita que vende tecnologia de cibervigilância e ciberespionagem. As ferramentas que vende, entre elas o Sherlock, podem ser usadas para

infiltrar computadores, servidores, aparelhos móveis e contas na Internet. A sua especialidade parece ser infiltração em computadores, particularmente naqueles usando o sistema operativo Windows, embora tenha software de infiltração para MacOS. Assim como clamam sucesso com as plataformas Android e IOS. O spyware pode extrair informação dos aparelhos invadidos, incluindo de programas de comunicação e do microfone ou da câmara, e pode identificar e mapear redes informáticas às quais o alvo está conectado.

Outra empresa de cibervigilância é a Cytrox, sediada na Macedónia do Norte. Que vende o spyware Predator, que ataca telemóveis Android.

Sobre a indústria da cibervigilância, o diretor do Google TAG (Threat Analysis Group) Shane Huntley declara que “se não há regulamentação e desvantagem em usar estas capacidades, então as vereis mais e mais”.

A Google TAG vigia mais de 30 empresas de cibervigilância.

Segundo a Microsoft, pelo menos 100 pessoas foram vítimas de spyware da Candiru na Palestina, Israel, Irão, Líbano, Iémen, Espanha, Reino Unido, Turquia, Arménia e Singapura. As vítimas incluíram defensores dos direitos humanos, ativistas, políticos, dissidentes e jornalistas.

E muitos dos programas de espionagem americana que o whistleblower Edward Snowden revelou ainda continuam em funcionamento.

Também na China - provavelmente o país mais avançado na implementação do 5G -, o desenvolvimento tecnológico está a ser usada na espionagem em massa da população, permitindo vigiar a sua vida a uma escala sem precedentes, e identificar grupos para serem detidos e encarcerados em campos de concentração, com a coleção e centralização de vários tipos dados sobre a população e o emprego de inteligência artificial na sua análise. É uma demonstração do poder da tecnologia para auxiliar a perpetrar abusos de direitos humanos a uma escala massiva, impondo um clima extremamente opressivo e psicologicamente desgastante de perpétuo terror. Está a ocorrer um verdadeiro genocídio cultural na China, com recurso à tecnologia de ponta.

Na China a ideia da segurança em relação ameaças sociais e perigos pandémicos tem sido usada para popularizar o sistema de vigilância tecnológica nacional. Ao que tem ajudado a redefinição do problema da privacidade exclusivamente ao setor privado, com o uso de propaganda e censura.

O governo da Arábia Saudita criou uma app, Kollona Amn, disponível no Google Play e na iStore, para cidadãos denunciarem comportamento subversivo ao regime, que tem sido usado na repressão do povo, e continua disponível para download nos serviços. Assim como o governo saudita condenou dois empregados da Wikipedia a 32 e a 8 anos de cadeia, numa tentativa de controlar o conteúdo do serviço.

Na Índia, uma diretiva governamental a entrar em vigor, em princípio, a dia 27 de junho de 2022, exige que as empresas de tecnologia na área das redes privadas virtuais (VPN, serviço de cloud, centros de dados) guardem informação completa sobre os seus clientes, o seu comportamento online e a relação comercial com a empresa durante 5 anos, mesmo que a ligação comercial cesse. O Ministério da Eletrónica e Tecnologias de Informação indiano afirma que esta medida vai ajudar a colmatar certas falhas de informação que dificultam a resposta a incidentes e interações digitais problemáticos com a população.

A tecnologia 5G e a Inteligência Artificial tem permitido criar, em países com regimes totalitários, sistemas de vigilância inorgânicos sempre em funcionamento, sempre a vigiar, que geram um clima de opressão sem precedentes altamente tóxico para os seus cidadãos.

Nos Estados Unidos, a agência federal DHS (Department of Homeland Security) tomou para si a responsabilidade de supervisionar o conteúdo das redes sociais, em especial a informação incorreta, iterando sobre o histórico da colaboração do estado americano com as empresas detentoras das redes sociais. A DHS tinha anteriormente classificado a informação incorreta nos tipos:

- informação incorreta: informação falsa espalhada de forma não intencional;
- desinformação: informação falsa espalhada intencionalmente;
- má-informação: informação verdadeira partilhada, tipicamente fora de contexto, com más intenções.

Também foi revelado recentemente que o departamento de estado americano dá acesso não-restrito a agências de inteligência e forças policiais a informação pessoal de americanos da aplicação para passaporte, sem processo legal ou supervisão. Nesta situação encontram-se 145 milhões de americanos.

As forças policiais americanas usam em segredo um software de rastreamento, chamado Fog Reveal, que permite a localização de pessoas, com base nos dados pessoais partilhados na Internet em milhares de diferentes apps em Android e IOS, que fazem parte de um mercado de transação de dados de localização. Isto permite ganhar conhecimento preciso sobre os lugares onde as pessoas trabalham, vivem e socializam.

Também o exército e a marinha americanos adquiriram à empresa Team Cymru software de cibervigilância massiva – a plataforma Augury - que inclui dados de navegação na Internet, e-mail e incluído em cookies. Este software cobre alegadamente 93% do tráfego de Internet mundial dos cinco continentes, que inclui a Europa. E a agência de policiamento da marinha NCIS também compra e faz uso ilegal desta informação. E este software também pode ser comprado por empresas privadas.

As empresas de transportes americanas estão a instalar sistemas de vigilância com microfones nos seus transportes, que permitem gravar conversas privadas. Em alguns casos financiado pelo Department of Homeland Security.

Bem mais perto de Portugal, o governo conservador do Reino Unido procura enfraquecer a lei sobre os direitos humanos, passou legislação que enfraquece o direito à manifestação, expande a legalidade do questionamento e da revista policial e, tendo sido visto ajuizado pelos tribunais que o uso dado à tecnologia de reconhecimento facial pela polícia infringia o direito à privacidade, apresenta agora um novo guia para o uso dessa tecnologia pela polícia, considerado por grupos de defesa das liberdades civis como “uma política atroz e um golpe rude à privacidade e à liberdade”.

“A Policing Bill [Lei do Policiamento] é uma parte de um extremamente preocupante e generalizado ataque aos direitos humanos pelo Governo [britânico], que não só verá direitos básicos reduzidos de forma geral, mas também retirará às pessoas os meios para pôr em causa ou contestar o seu tratamento”, declarou Sacha Deshmukh, diretor executivo da Amnesty International UK.

O governo do Reino Unido também se prepara para usar os dados privados médicos de cidadãos guardados no sistema nacional de saúde britânico (NHS) na sua plataforma de dados assente em tecnologia da empresa Palantir, sem proteger a identidade dos cidadãos, sem os informar nem lhes dar a opção de recusar.

Em 2025 no Reino Unido entrou em vigor um conjunto de leis chamados de Online Safety Act, que com o argumento de tornar a Internet mais segura, em especial para crianças, requerendo que as plataformas online tomem medidas contra conteúdo nocivo e implementem a verificação de idade, nomeadamente forçando os utilizadores a se identificarem online com documentos oficiais, com isto destruindo a privacidade online dos utilizadores.

Também no Reino Unido as pessoas podem ser presas e processadas judicialmente pelo conteúdo publicado da sua página nas redes sociais.

Recentemente em 2025 o governo britânico passou a exigir que todos os cidadãos tenham uma identificação online, que o governo britânico argumenta vai impedir a imigração ilegal. Também o governo russo está a planear introduzir a identificação online da sua população.

No Canadá, a agência de privacidade nacional (Privacy Commissioner of Canada) clama por um enquadramento legal mais completo e restritivo do uso policial de reconhecimento facial, que substitua o considerado insuficiente retalho de leis, que, na maioria, não adereça especificamente diferentes usos ou riscos postos por esta tecnologia.

Na Austrália, desde 2025, os cidadãos têm de se identificar para usar a Internet e aplicações como Apple e Google Maps, dando ao governo a localização em tempo real e a sua identificação por câmara para acesso.

Nos Estados Unidos, em 2025, os estados de Mississippi e do Texas passaram leis a exigir a identificação dos utilizadores online.

Também em 2025 a plataforma de comunicação online Discord sofreu um ataque informático que terá exposto as fotos usadas para identificação de 70 000 utilizadores, assim como informação pessoal, parcialmente informação sobre o cartão de crédito e mensagens trocadas com o serviço ao cliente da empresa. Rumores apontam que o número de afetados foi bem maior, mais de 2 milhões.

E 35 organizações da sociedade civil - entre as quais a European Digital Rights (EDRi), a Electronic Frontier Foundation (EFF), Deutscher Anwaltverein (DAV) e o Committee to Protect Journalists (CPJ) - estão a soar o alarme sobre a legislação que a Comissão Europeia está para apresentar a 30 de março (de 2022) sobre a obrigatoriedade da busca e reportamento automatizados de CSAM (Child Sexual Abuse Materials [Materiais de Abuso Sexual de Crianças]) em todas as comunicações online por e-mail, chat, e serviços de mensagens, mesmo as encriptadas dentro da União Europeia. Estas organizações estão preocupadas com a possibilidade de vigilância generalizada da totalidade das populações, com as vulnerabilidades adicionais que cria na tecnologia e nas populações, e com o mau exemplo que é dado a nível mundial em termos de ataque à privacidade. Embora o rastreamento e o reportamento voluntário dentro da União Europeia por plataformas online seja já permitido para empresas cujas atividades cumpram os requisitos para a isenção de provisões da Diretiva 2002/58/EC (a Diretiva de ePrivacidade).

Investigadores Ross Anderson e Sam Gilbert da Universidade de Cambridge avisam que este tipo de medida poderá gerar cerca de 1 milhar de milhão de resultados falsos positivos por dia e aumentar significativamente o número de pessoas sinalizadas, em um universo em que se trocam cerca de 10 milhares de milhões de mensagens por dia na União Europeia.

Também depois da criação de um serviço europeu de intercâmbio automatizado de dados relativos ao ADN, impressões digitais e dados de registo de veículos entre as autoridades civis responsáveis chamado Prüm, em atividade desde 2005, agora surgem propostas para um Prüm II no Parlamento Europeu, sobre a implementação de um sistema de partilha de fotos, de reconhecimento facial e de dados da carta de condução de uma forma mais automatizada a nível europeu. Isto inclui também o uso de reconhecimento facial retrospectivo, que permite o uso de imagens de câmaras de vigilância, fotos das redes sociais ou de telemóveis para identificar pessoas na base de dados da polícia.

De mencionar que estas bases de dados biométricos das autoridades nacionais incluem suspeitos de crimes, criminosos, refugiados, e pessoas não-identificadas, na quantidade de vários milhões.

“O que vocês estão a criar é a mais rigorosa infraestrutura de vigilância biométrica que eu penso que nós alguma vez já vimos no mundo”, afirma Ella Jakubowska, uma conselheira do grupo não-governamental European Digital Rights (EDRi).

Em 2025 os deputados da União Europeia estiverão a discutir a proposta de lei "Chat Control", que iria obrigar o scan de todas as comunicações digitais privadas, incluindo mensagens e fotos encriptadas, exceto as de políticos que se isentam desta vigilância sob

regras de "sigilo profissional". Os deputados europeus alemães mostraram-se contra esta proposta, deitando por terra por agora este tipo de medidas.

E em Portugal, o Tribunal Constitucional chumbou, declarando como inconstitucionais, as normas da chamada “lei dos metadados”, que determinam o armazenamento dos dados de tráfego e localização das comunicações de todas as pessoas, de forma generalizada, pelo período de um ano. O TC considerou que, ao não se garantir que o armazenamento desses dados ocorra num Estado-membro da União Europeia, “põe-se em causa o direito do visado controlar e auditar o tratamento dos dados a seu respeito” e a “efetividade da garantia constitucional de fiscalização por uma autoridade administrativa independente”, assim como “restringe de modo desproporcionado os direitos à reserva da intimidade da vida privada e à autodeterminação informativa.” “Designadamente, por atingir sujeitos relativamente aos quais não há qualquer suspeita de atividade criminosa: abrangem-se as comunicações eletrónicas da quase totalidade da população, sem qualquer diferenciação, exceção ou ponderação face ao objetivo perseguido”.

Foi ainda declarada inconstitucional a norma do artigo 9.º da mesma lei – lei 32/2008 – na parte em que não prevê que o visado seja notificado de que os seus dados foram acedidos pela investigação criminal, “a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiro”.

O governo português, no entanto, pretendeu reformular a “lei dos metadados”, procurando um compromisso entre o direito constitucional à privacidade e a segurança nacional a apresentar à Assembleia da República.

Assim parlamento aprovou em Outubro de 2023 em votação final global o texto acordado por PS e PSD prevendo que os metadados tenham uma conservação generalizada até seis meses, mudança que visa ultrapassar a declaração de inconstitucionalidade da anterior lei.

O projeto de lei aprovado foi enviado para o Presidente da República e foi posteriormente remetido ao Tribunal Constitucional (TC), uma vez que o Presidente da República já tinha indicado que iria pedir a fiscalização preventiva do diploma, considerando que "não pode haver sombra de dúvida" sobre a sua constitucionalidade.

Mas mais preocupante é a base de dados da Autoridade Tributária, que têm o registo da nossa vida toda, durante um limite temporal incerto, e que é acedida pela Segurança Social, PSP, GNR, câmaras municipais, agentes de execução, fornecendo a milhares de pessoas acesso aos nossos dados privados.

Precisamos atentar e procurar garantir que não há uma devassidão excessiva e desproporcionada das liberdades, direitos e garantias civis.

A lei portuguesa que regula o acesso a metadados referentes a comunicações eletrónicas para fins de investigação criminal, procedendo à alteração da Lei n.º 32/2008, de 17 de julho, que transpõe para a ordem jurídica interna a Diretiva 2006/24/CE, do Parlamento Europeu e

do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, conformando-a com os Acórdãos do Tribunal Constitucional n.os 268/2022 e 800/2023, e da Lei da Organização do Sistema Judiciário foi publicada em Diário da República em 5 de fevereiro de 2024.

Também o Tribunal de Justiça Europeu tem se oposto às leis comparáveis de retenção de dados em vigor na Alemanha, no Luxemburgo e em França. Defendendo que os dados de tráfego e de localização de cidadãos europeus só podem ser guardados em condições específicas, como a séria ameaça à segurança nacional. E não de forma indiscriminada.

E o problema posto pelos metadados é agravado pelos erros e discrepâncias presentes nos programas informáticos, que não funcionam muitas vezes exatamente de acordo com a lógica pensada para o processo, criando erros e “falsos positivos”, que impactam negativamente a vida das pessoas afetadas.

Em 2023, um estudo do MIT, chegou à conclusão que programas de Inteligência Artificial podem classificar imagens não relacionadas como iguais, respondendo da mesma forma a estímulos potencialmente muito diferentes.

O website oficial sobre o sistema legal aplicado pela União Europeia (EUR-Lex) descreve o conceito de “défice democrático”. A descrição apresenta a ideia de que as instituições da União Europeia e os seus processos de decisão sofrem de uma falta de democracia e parecem inacessíveis para o cidadão normal devido à sua complexidade. Que o défice democrático real na União Europeia parece derivar da ausência de um sistema político europeu orgânico. Os eleitores não sentem que têm uma forma efetiva de rejeitar um ‘governo’ que eles não gostam, ou de mudar o rumo político e legal.

Processadores de pagamentos como a Mastercard e Paypal estão a se negar a permitir a compra de determinado conteúdo legal online por clientes seus, com o argumento que esse conteúdo é mau para a sua reputação, no entanto permitindo compras em websites como Roblox, que é orientado a crianças e cheio de microtransações e onde estas podem – e há casos reais – de serem contactadas por predadores sexuais.

A isto acumula-se o facto de empresas como a Apple, o Facebook, e a Google gravarem conversas dos seus utilizadores. De facto, todas as aplicações que acessam a câmara e/ou o microfone de um aparelho, como a Siri e o navegador de Internet Safari (Apple), Alexa (Amazon), e a Home (Google) acessam os dados obtidos pelo microfone. A empresa Facebook veio a público afirmar que não grava mais conversas de seus utilizadores, mas a sua reputação não é fiável, com repetidos escândalos sobre questões de privacidade.

Também a ex-diretora de Política Pública Global da Meta e denunciante Sarah Wynn-Williams afirmou perante os senadores dos EUA numa audiência no dia 10 de abril de 2025 que a Meta direcionou anúncios publicitários a adolescentes com base no seu estado emocional.

A Swiss Re (a maior agência de seguros e resseguros do mundo) afirma que “também há preocupações sobre problemas de privacidade (que levarão a riscos aumentados de litigação), falhas de segurança e espionagem. O foco não é apenas no hacking de terceiros, mas também potenciais falhas de segurança de backdoors implantadas no hardware ou software. Adicionalmente, o mercado para a infraestrutura 5G está correntemente ocupado por algumas firmas, que levanta o espectro do risco da concentração.”

E continua, afirmando que “tecnologias como Big Data e computação em cloud podem em muito aumentar a eficiência da captura, armazenamento e computação de dados. A Quarta Revolução Industrial está a progredir a todo o vapor incluindo, entre outros, automatização de processos, aparelhos da Internet of Things (IoT) e analítica digital capaz de rápida análise de quantidades massivas de dados não-estruturados/estruturados. (...) Tudo isto, no entanto, levanta problemas com a privacidade e de confiança, e assim envolvimento regulatório. Para seguradoras, especificamente, estes desenvolvimentos também aumentam o espectro de seleção adversa”.

Com esta coleção progressiva e massiva de dados por meios informáticos (incluindo através da navegação online) são constituídos perfis individuais e coletivos, com o fito de conhecer melhor os indivíduos e as populações de que fazem parte, de forma às entidades envolvidas poderem tomar melhores decisões em função dos seus objetivos. Que não se alinham necessariamente com os das pessoas cujas informações são recolhidas.

Com a tecnologia que existe a nível de vigilância e com os desenvolvimentos de 2025 acima citados e outros, os países ocidentais e a União Europeia estão a pouco e pouco a se tornar em estados policiais, sem privacidade nem liberdade, em ditaduras.

Em 2023, Portugal sofreu uma das maiores quedas no índice de representação política, num estudo do Instituto Internacional para a Democracia e a Assistência Eleitoral (IDEA) sobre o Estado Global das Democracias, que revelou também que os alicerces da democracia estão a enfraquecer em todo o mundo, por falta de controlo político e judicial.

No seu relatório anual, intitulado "O Estado Global da Democracia 2023", o IDEA sublinha que na Europa muitas democracias com fortes tradições registaram um declínio no seu desempenho democrático, incluindo a Áustria, os Países Baixos, Portugal e o Reino Unido, na categoria Estado de Direito.

Os dados recolhidos pelo IDEA também permitem perceber que os alicerces da democracia estão a enfraquecer em todo o mundo, com metade dos países a sofrer declínio por falta de controlo político e judicial.

O enfraquecimento das democracias está a ser amplificado pela erosão dos sistemas de controlo tradicionais -- eleições livres, parlamentos e tribunais -- que revelam progressiva dificuldade em garantir a eficácia das instituições.

Assim, 2022 foi o sexto ano consecutivo em que os países com declínios líquidos ultrapassaram os países com avanços líquidos, o que representa a queda consecutiva mais longa desde o aparecimento de registos do IDEA, em 1975.

Muitas democracias estabelecidas têm vindo a sofrer retrocessos em termos de democracia, desde declínios na igualdade dos grupos sociais nos Estados Unidos, na liberdade de imprensa na Áustria e no acesso à justiça no Reino Unido.

A Swiss Re, no seu relatório de riscos emergentes de 2021, considera que “a disponibilidade de um leque mais alargado de informação de saúde vai permitir a seguradoras criar coberturas mais personalizadas e serviços para clientes”. Isto mencionado em relação a aparelhos monitores de atividade física, como o Fitbit.

De notar que vastas coleções de dados das populações estão disponíveis livremente pela Internet, como no portal PORDATA.

E os ISPs (operadoras de Internet) nacionais estão a vender o seu histórico de uso da Internet dos seus clientes sem o seu consentimento - ou sequer o seu conhecimento -, como já é legal internacionalmente, nomeadamente nos Estados Unidos da América?

Pela legislação, aplicável desde 25 de maio de 2018, do Regulamento Geral sobre a Proteção de Dados (RGPD), da União Europeia, as empresas trabalhando no espaço europeu não podem abertamente vender os dados dos seus clientes indiscriminadamente, embora possam passar os seus dados a terceiros, desde que oferecendo motivos válidos legalmente para tal, revelem os futuros recipientes dos dados, e sejam autorizados pelos cidadãos, individualmente, com acesso a uma informação objetiva e abrangente sobre os dados coletados e o uso a dar aos dados, e, posteriormente, no caso em que ocorra alteração ao uso permitido, seja transmitida a informação sobre essa alteração (Artigo 12, Artigo 13 parágrafo 3 e Artigo 14 parágrafo 4). Estipulações que claramente não são totalmente aplicadas pelas empresas.

Assim como os utilizadores europeus têm o direito a objetar ao processamento dos seus dados a qualquer altura no espaço europeu, e a ser informados sobre este direito de forma explícita. (Artigo 21 do GDPR).

Ainda assim muitos sites coletam os dados pessoais postos nos seus formulários, mesmo que não sejam submetidos e enviados, não dando nenhuma informação sobre isto, incorrendo em ilegalidade. Este comportamento pode também não ser perpetrado diretamente pela empresa detentora do serviço, mas por entidades de serviços terceiras de marketing e de análise de dados incorporadas nas páginas.

Mas a legislação europeia à volta dos dados pessoais pode apertar em determinadas circunstâncias, com uma decisão do Tribunal de Justiça da União Europeia, segundo a qual dados pessoais, como o nome do companheiro, são “informações sensíveis”, por permitirem a dedução de informações privadas sensíveis, neste caso a orientação sexual.

Nos Estados Unidos, a gigante das telecomunicações AT&T argumentou, em 2015, que a privacidade era um privilégio, e procurou cobrar mais \$29 aos seus clientes por mantê-la.

Está a surgir uma nova tecnologia apelidada de ‘smart dust’, que usa ínfimos aparelhos, chamados de sistemas microelectromecânicos (MEMs), criados de minúsculas partículas de silicone e guiados por software, alguns com o tamanho de grãos de pólen, que são libertados em grande quantidade em ambientes como se fosse uma poeira, funcionando simultânea e autonomamente, e que podem servir para medir a presença de químicos, luz, vibração, temperatura, ruído, ou qualquer outra força física, mas também para funcionar como chips de identificação por radiofrequência (RFID). Uma tecnologia que promete surgir lentamente na próxima década, e que deve ser seguida com cuidado pelas suas ramificações, incluindo identificação por radiofrequência e poluição a que pode dar origem.

Toda esta devassidão da nossa privacidade acontece porque o indivíduo, pela sua importância no tecido social, é definido comercialmente como um ‘bem’, sendo aos seus dados conferido valor social e económico. Onde a defesa da privacidade pelo indivíduo acaba se assumindo como uma auto-exclusão social auto-determinada, pela importância que estes serviços tecnológicos assumem na nossa vida coletiva. E esta pressão à erosão da privacidade põe em causa as nossas outras liberdades, como a de expressão, de prática religiosa, de congregação, de participação democrática, e até o nosso livre arbítrio. A privacidade assume-se como a barreira entre a sociedade civil e o perfilamento questionável individual e coletivo. Sendo ela trocada, no nosso dia-a-dia, em geral, pela conveniência de certos serviços e facilidade de acesso, com as empresas que fornecem estes serviços a usar, vender, e permitir o acesso a este tipo de informação pessoal, construindo perfis detalhados dos indivíduos, que podem superar o entendimento de um indivíduo normal acerca de si próprio.

Como declarou Edward Snowden na Web Summit de 2019 em Lisboa, “as mais poderosas instituições da sociedade são as menos responsabilizadas. A minha geração, e particularmente a geração depois da minha, já não são donos de nada. Usamos estes serviços e criamos um registo permanente – e isto é o que escapa às pessoas. Não são dados que estão a ser explorados, são as pessoas que estão a ser manipuladas”, venceu. “A recolha de informação e a vigilância acontecia [no passado] de forma completamente diferente”, sinalizou, avançando que, ao contrário da época em que as autoridades vigiavam pessoas específicas, agora, toda a gente é observada, “em todo o lado, durante todo o tempo. Esse é que é o verdadeiro problema, nós legalizámos o abuso [relativamente à recolha de dados pessoais], criámos um sistema que torna a população vulnerável para benefício dos privilegiados”, afirmou.

E a tecnologia 5G vai previsivelmente acelerar e aumentar a coleção massiva de dados privados e públicos, e permitir relacioná-los mais eficaz e eficientemente, destruindo ainda mais a privacidade individual, e erodindo o direito a ela e a sua legitimidade, pela banalidade da sua violação, que tal como a inteligência artificial, estará ao dispor de empresas, governos, dos indivíduos no governo, parceiros creditados pelas forças políticas, dos indivíduos passíveis de fazer essa decisão, e de pessoas comuns. Sendo que geralmente as estruturas públicas e privadas que gerem estas implementações são dominados por burocratas e os seus interesses particulares.

As empresas de redes sociais, de streaming de vídeos, etc., já fazem uso da inteligência artificial de forma a descobrirem o que prende a atenção dos seus utilizadores e os manipula.

E estão a ser comercializados serviços de inteligência artificial para decodificar estados emocionais e mesmo proporcionar aconselhamento de como agir em função desses estados, por serviços como o Zoom e Amazon.

Um destes serviços é o Class, da Intel e da Classroom Technologies, que funciona com o Zoom, e que procura identificar o estado emocional de alunos pela análise das expressões faciais e da interação com material educativo.

Também têm surgido e tido sucesso programas de Inteligência Artificial que funcionam como namoradas/namorados e servem para simular relações amorosas, com políticas de privacidade questionáveis, e que os utilizadores treinam de forma inadvertida para os manipular. Isto – como se verificou com o foco nas redes sociais – tem a possibilidade de exacerbar o isolamento e a solidão reais, ao condicionar o utilizador a se focar na virtualidade da relação com um programa informático em vez da sua realidade.

E as grandes empresas de software, como a Google, a Microsoft e a Adobe tem trabalho no sentido de integrar Inteligência Artificial nos seus produtos, muitas vezes de forma irrefletida, redutora e gananciosa, gerando resistência e controvérsia, em especial à volta das questões da privacidade e da aplicação egoísta da tecnologia.

O motor de busca da Google, assim como outros, têm usado Inteligência Artificial para fazer síntese do que é tomado como a resposta à busca online dos utilizadores, com isto eliminando a necessidade do utilizador abrir os sites de onde a aplicação de Inteligência Artificial foi buscar a resposta, reduzindo de forma significativa a frequência de utilizadores que visitam estes sites. E com isto maximizando o tempo que os utilizadores passam na página do motor de busca, maximizando a exposição dos utilizadores aos anúncios apresentados e maximizando o lucro da empresa, em detrimento dos sites na sua lista de resultados.

A introdução de Inteligência Artificial no Windows 11 tem gerado muita controvérsia em volta da questão da privacidade do sistema operativo e a sua lentidão.

A Adobe foi boicotada pelos seus clientes devido à introdução de Inteligência Artificial nas suas aplicações, em parte por questões de privacidade e de performance.

Como o investigador Yuval Noah Harari pensa, IA é cada vez mais o acrónimo para Inteligência Alienígena à medida que vai evoluindo e “se tornando menos e menos artificial”, mais imprevisível.

E este atropelo da privacidade tornou-se tão mais previsível com a experiência da crise sanitária associada ao SARS-CoV-2, que atacou os direitos dos cidadãos, e devassou a intimidade com novas tecnologias como o uso de drones no policiamento e o contact-tracing. Não havendo a certeza que agora que este génio saiu da lamparina volte para lá outra vez,

sendo até provável que a invasão da privacidade continue a aumentar com o surgimento de importantes transformações, como as casas e as cidades inteligentes, e a disponibilidade de parte da população de abrir mão da sua privacidade em troca de comodidade e de suposta segurança. As nossas informações pessoais já não são apenas apropriadas ilegalmente por hackers, mas cedidas livremente para ajudar com a segurança pública.

Com a pandemia as grandes empresas tecnológicas, que foram mobilizadas para criar as aplicações informáticas usadas na pandemia adquiriram uma nova influência na sociedade civil, que permanece depois da crise pandémica mundial, segundo um estudo da Universidade de Bristol assente sobre a realidade social austríaca e a norueguesa. Que adverte sobre a necessidade de explorar a questão de como as tecnologias digitais transformam a nossa vida democrática, com uma administração progressivamente assente em tecnologia.

E em Israel, China, Índia e Austrália a agência de jornalismo sem fins lucrativos americana Associated Press descobriu que a tecnologia de vigilância desenvolvida a quando da pandemia do Covid-19 para o contact-tracing a ser utilizada para fins outros, assim como a informação obtida a partir dela, para violar os direitos de cidadãos, incluindo ligar esses dados a outras ferramentas de vigilância e de policiamento e até fornece-los a agências de espionagem.

E as indústrias, por exemplo a de seguros, contam fazer uso deste relaxamento na defesa pública da privacidade, como demonstra esta frase atribuída à Swiss Re: “Provisões sobre dados e leis relaxadas podem também reduzir as barreiras para modelos de negócio de seguros guiados por informação.”

Isto em colisão com os artigos 7 e 8 da Carta dos Direitos Fundamentais da União Europeia, onde:

Artigo 7.

Respeito pela vida privada e familiar

Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.

Artigo 8.

Proteção de dados pessoais

1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.

2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

Quem sabe ao certo em que são usados os seus dados pessoais atualmente partilhados com serviços comerciais? Assim como quantas empresas permitem aos utilizadores aceder aos dados pessoais coligidos?

Uma vez partilhados os dados pessoais, são normalmente coletados para vários tipos de fins - legais e ilegais - declaradamente ou não.

De notar que as empresas que operam na Internet têm normalmente políticas opacas sobre a coleção de dados pessoais, que tornam difícil ou mesmo impossível modificar a fundo as definições de privacidade associadas com o uso das plataformas (por exemplo, na navegação do website da empresa), fora não usar esses recursos, ou usá-los de uma forma possivelmente tão limitada que passa por coerciva (por exemplo, com parte da página ocupada com a janela da escolha da política de gestão de dados).

Para lá de normalmente dificultarem a gestão do tratamento de dados pessoais ao utilizador, escondendo ou dificultando a opção de rejeitar a recolha, armazenamento e processamento de dados pessoais da plataforma, pressionando assim os seus utilizadores a aceitar a política de dados por defeito, violando o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, que exige clareza, simplicidade e ação afirmativa na escolha da política de dados online.

E a empresa Meta, admite entre portas, que não têm um nível adequado de compreensão e de controlo sobre o uso que a plataforma Facebook faz dos dados pessoais que têm na sua posse. Comparando esta realidade a verter uma garrafa de tinta num lago, onde a tinta flui para todo o lado.

Estes problemas sugerem que provavelmente milhões de cidadãos europeus estão a ter os seus dados pessoais recolhidos e/ou tratados de forma ilegal.

Também a empresa Twitter parece ter uma política de segurança muito deficiente, de acordo com o ex-executivo da empresa e denunciante Peiter "Mudge" Zatkó, que, em agosto de 2022, revelou que pela sua especial vulnerabilidade pode permitir a espionagem e manipulação estrangeiros, hacking e a campanhas de desinformação, esta ameaça a segurança dos dados dos seus utilizadores, os acionistas, a segurança nacional americana e a liberdade. Descrevendo um ambiente caótico e imprudente decorrente de má gestão, que permite a demasiados empregados acesso aos controlos centrais da plataforma e a dados mais sensíveis sem supervisão adequada. Referindo também a incapacidade de gerir adequadamente o volume de dados, que leva a que por vezes não seja capaz de apagar os dados de usuários, por ser incapaz de os localizar. Levantando também a suspeita que um ou mais empregados poderão estar trabalhar para serviços de espionagem estrangeiros.

Este denunciante também acusa o executivo da empresa Twitter de má-fé e de fraude, ao enganar a FTC (Federal Telecommunications Committee) americana e se preparar para enganar as congéneres francesa e irlandesa sobre a informação usada pela empresa para treinar os seus algoritmos de Machine Learning, escondendo uma extensas violações de privacidade e direitos de autor.

Também sendo referidos problemas na implementação de cookies, e associadas violações das leis de privacidade europeias.

Por sua vez, as autoridades públicas com a incumbência de supervisionar o tratamento de dados online, a nível europeu, aparentam estar com número insuficiente de inspetores e sem orçamento para exercer as suas funções com a competência exigida pela legislação.

Em relação ao caso das denúncias sobre o Twitter, as entidades públicas de proteção de dados da Irlanda e da França, dentro da União Europeia, afirmaram estar a investigar o caso.

E a consequência do desrespeito destas leis, quando provado, é uma ordem ao cumprimento do quadro normativo ou uma coima, que pode chegar a dezenas de milhões de euros, que mais não é que um imposto adicional - quando realmente é cobrada - a empresas multinacionais confortáveis o suficiente para a pagar, ou que desaparecem antes que possa ser constituído um caso jurídico.

Numa violação distinta da Regulamento Geral sobre a Proteção de Dados, a Irlanda multou a empresa Twitter em \$550,000.

9.2 - Insegurança Informática

O número de utilizadores de tecnologia móvel em todo o mundo prevê-se que crescerá de 7,1 milhares de milhões em 2021 para 7,49 milhares de milhões em 2025.

Falhas e vulnerabilidades no hardware e no software de sistemas informáticos podem permanecer escondidas por muito tempo, e ser eventualmente exploradas em larga escala com efeitos catastróficos. Basta lembrar o ransomware² WannaCry¹⁸, em 2017, que atacou o serviço de saúde público inglês provocando danos no valor de 73 milhões de libras. E com o qual milhares de computadores pelo mundo fora foram afetados.

Com o SARS-CoV-2, a crise sanitária decorrente, o confinamento mundial das populações, o encerramento em número significativo de empresas e negócios, os despedimentos em massa e o lay-off, as dificuldades económicas e o caos, o crime informático tem subido dramaticamente (até 300% em Portugal até ao final de abril de 2020, e 81% em 2021). Têm acontecido ataques informáticos de grande escala, como recentemente

18 - Para mais informações sobre impacto do ransomware Wannacry:
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#Impact

os crimes de que foram alvo a EDP, a Altice, a Impresa, a Cofina, a Vodafone, o site da Assembleia da República e a TAP. A que se juntam um acréscimo de burlas informáticas, ataques de ransomware, pedidos de resgate e apps de telemóvel fraudulentas.

O grupo de hackers CyberTeam invadiu o sistema informático da Altice e da EDP, bloqueando centenas de sistemas e servidores e posteriormente exigindo 10 milhões de euros em bitcoin à empresa do sector das energias. Também declaram ter acesso a 80% dos sites em Portugal.

A Vodafone também foi alvo de um ataque informático, em 7 de Fevereiro de 2022, que afetou significativamente os seus serviços de telecomunicações e de Internet, tendo sido até desativados. O ciberataque também vitimou entidades com parcerias comerciais com a Vodafone, como o INEM, a Proteção Civil e os bombeiros, que se viram forçados a recorrer ao SIRESP (a rede de emergência nacional), experimentando ainda assim falhas no serviço ao nível das telecomunicações. Nos hospitais também houve problemas no que diz respeito aos contactos com os utentes, para a marcação de consultas, nas teleconsultas e na marcação de testes PCR. O Instituto Português do Mar e da Atmosfera esteve igualmente a enfrentar dificuldades para obter dados em tempo real. A SIBS (Sociedade Interbancária de Serviços) reportou “alguma instabilidade pontual” nos serviços, causando constrangimentos nas caixas automáticas, que ficaram indisponíveis durante algumas horas, e nos terminais de pagamento, assim como impossibilitadas transferências bancárias online, uma vez que os códigos de validação são enviados para o telemóvel. Houve falhas também no serviço de telecomunicações de empresas, serviços públicos (incluindo tribunais e escolas), e de entregas de encomendas e correspondência. E até as trotinetes elétricas partilhadas, dependentes do GPS da Vodafone, foram afetadas.

O ataque informático à Vodafone não foi reivindicado, nem existiu tentativa de extorquir dinheiro, aparentemente apenas de sabotagem do serviço. É considerado como um ato de terrorismo internacional. Sendo que na altura do evento foi aventada a possibilidade de ser um ciberataque russo. Esta hipótese ganhou força com a invasão da Rússia à Ucrânia iniciada 15 dias depois, no dia 22 de fevereiro de 2022.

Também depois o Hospital Garcia de Orta, em Almada, e a Câmara Municipal da Moita, distrito de Setúbal, sofreram ataques de ransomware, em abril de 2022, que afetaram os seus sistemas informáticos.

A TAP também viu os dados alegadamente pertencentes a 115 mil clientes da companhia aérea serem publicados online, ameaçando o grupo de hackers responsável pela fuga de informação publicar até 1,5 milhões de dados pessoais na posse da empresa. O número de clientes cujos dados foram publicados na Internet subiu para 1,5 milhões, e acabou por incluir o Presidente da República, Marcelo Rebelo de Sousa. Numa mensagem publicada na Dark Web, o grupo de hackers Ragnar Locker garante ainda que continua a ter acesso aos sistemas informáticos da TAP.

O grupo de hackers russo Conti paralisou desde abril de 2022 o recentemente empossado governo da Costa Rica, com um ataque de ransomware de larga escala, afetando 27

instituições públicas, incluindo o ministério das finanças e outros sistemas governamentais, câmaras municipais e serviços públicos. O grupo ameaçou publicamente derrubar o novo governo deste país.

Devido ao maior sucesso na disrupção destes ataques por forças policiais e à maior perigosidade de atacar alvos nos Estados Unidos da América ou na União Europeia, estes grupos de hackers parece estar a direccionar a sua atividade para países mais pequenos e pobres, com menos fundos para gastar em segurança informática, como a Costa Rica.

José Tribolet, professor catedrático jubilado do Instituto Superior Técnico e especialista em cibersegurança, declara que “nenhuma instituição pode pensar que não vai ser atacada, que não vai ter ataques de ransomware que vão afetar e prejudicar o seu funcionamento normal”.

Este tipo de ciberataques estão a acontecer com alguma regularidade em todo o mundo, e são frequentemente perpetrados por grupos de hackers, que funcionam como redes criminosas altamente profissionais, estruturadas e lucrativas. Tipicamente não têm uma geografia associada, trabalhando por todo o mundo. Angariam dinheiro direta e indiretamente, através de ransomware, fraudes bancárias, etc. Por vezes estabelecendo parcerias com o governo de países, como o reportado entre o grupo de piratas informáticos Conti e a Federação da Rússia.

E o ritmo e a quantidade deste tipo de invasões de sistemas informáticos são também influenciados pelo mediatismo associado a ataques críticos, induzindo uma moda que induz à imitação, como a onda que afetou Portugal em 2022, com os casos da Impresa, Cofina, Vodafone e dos laboratórios Germano de Sousa, desde o princípio do ano até ao dia 9 de fevereiro.

Já em 2019, a empresa de cibersegurança Malwarebytes afirmou que os ataques de ransomware tinham se tornado mais sofisticados e graves.

Os ataques de ransomware aumentaram 13% em 2022.

Internacionalmente, os índices sobre cibercrime relacionados com o SARS-CoV-2 aumentaram 600% de fevereiro a princípios de março de 2020, de acordo com a empresa de cyberinteligência CYFIRMA.

E só durante o mês de março (de 2020), todos os dias descobriam-se cerca de 136 novas vulnerabilidades de segurança em serviços de infraestrutura crítica em todo o mundo. A informação é da CTI League, um grupo com mais de 1400 profissionais voluntários de cibersegurança de 77 países, incluindo Portugal.

Começando já a surgir programas maliciosos (malware), como o Hoaxcalls e o Kaiji, que direccionam o seu foco para aparelhos "inteligentes" que começam a operar dentro do paradigma da Internet das Coisas. O Kaiji, em particular, ainda está em desenvolvimento, e

foi codificado com o propósito único de lançar ataques DDoS (Distributed Denial of Service¹⁹).

Também foi revelado que a FSB (Serviços Secretos russos) contratou a criação de uma ferramenta capaz de explorar vulnerabilidades na segurança de aparelhos inteligentes para, ao organizá-los numa rede (botnet), lançar ataques DDoS em escala massiva, capazes de paralisar digitalmente serviços ou até pequenos países durante várias horas, chamada Programa Fronton.

E neste ambiente o novo paradigma de sistemas de comunicação para casas inteligentes chamado Matter, da Google, procura permitir a estes aparelhos ligar direta e autonomamente à Internet. Enfraquecendo a privacidade dos utilizadores, na sua vulnerabilidade a hacks, leaks e vigilância.

A Coreia do Norte foi associada ao grupo de hackers Zinc, também chamado de Lazarus, que tem vindo a infectar software gratuito com código malicioso, para atacar e ganhar acesso a organizações e indivíduos específicos, com uso de fraude (engenharia social).

Com as guerras convencionais, no presente, também acontecem em paralelo guerras no ciberespaço, através da Internet. Durante a guerra da Ucrânia, estimou-se que mais de 80% dos ataques informáticos mundiais era direcionados à Ucrânia e à Rússia. Com países terceiros considerados como hostis ou intervenientes no conflito passíveis de serem alvos também deste tipo de agressão, sem ser acompanhado de ataque bélico convencional.

A isto tudo não ajuda o facto de que o confinamento e o distanciamento social em muitas zonas do mundo, em função da crise sanitária associada ao SARS-CoV-2, tenham levado as empresas que podiam a instituir o trabalho remoto e até uma digitalização apressada dos seus processos. Isto retirou, na maioria dos casos, os empregados da segurança das redes empresariais, para os levar a usar a "internet de casa" e os mesmos computadores que usam para o lazer no domicílio, aumentando muitíssimo o grau de vulnerabilidade das empresas e dos trabalhadores à pirataria informática.

A sociedade alicerçou-se neste mundo digital, com os cidadãos a mergulharem nesta nova era, tornando as populações mais vulneráveis direta ou indiretamente, em especial em épocas de crise e de guerra.

No evento Network X em Amsterdão, nos Países Baixos, profissionais na indústria e um hacker famoso detalharam as suas preocupações com a digitalização tecnológica, detalhando a crescente abstração dos sistemas digitais, má gestão destes serviços, más práticas de segurança, opacidade geral dos sistemas de suporte, a falta de experiência e conhecimentos sobre estes sistemas e as tecnologias em que estão suportados, o facto de profissionais tecnológicos associados a tecnologias mais antigas terem migrado ou se reformado, e a crescente profissionalização e estruturação dos hackers, incluindo de agências governamentais.

19- Distributed Denial of Service é um ataque informático caracterizado pela realização de um número massivo de acessos a um alvo (serviços online [por exemplo página web]) tornando a prestação do serviço impossível.

Recentemente oficiais dos serviços secretos americanos lançaram o alerta sobre o facto de ataques de ransomware sobre MSPs (Managed Service Providers) estarem a aumentar. Os Managed Service Providers são empresas externas que oferecem serviços de plataformas, infraestruturas, aplicações ou armazenamento remoto. Estas empresas normalmente têm vários clientes, o que as torna uma porta de entrada, quando hackeadas, para várias outras organizações, públicas ou privadas. Um exemplo deste tipo de ataques foi o Sunburst, ocorrido em 2020, que afetou potencialmente centenas de milhares de empresas (incluindo a maioria das empresas do chamado Fortune 500) e agências estatais na América do Norte, Europa, Médio Oriente e Ásia, clientes da empresa SolarWinds, que lhes fornecia serviços de monitorização de rede e outros serviços técnicos. Este ataque foi atribuído à Rússia.

Os hackers aproveitando-se da pandemia do SARS-CoV-2 são motivados por uma combinação de interesses económicos e de espionagem política, para causar caos social. Os atores maliciosos no mundo do cibercrime estão bem equipados com ferramentas, tecnologia, conhecimento e financiamento para avançar em agendas económicas e políticas. No nosso mundo digital hiperconectado o cibercrime é um negócio lucrativo, e com a digitalização apressada da sociedade, as previsões é que aumentem o volume e a sofisticação dos ataques, assim como as perdas associadas a eles, em especial enquanto esta pandemia obrigar a uma adaptação forçada nas dimensões pessoal e profissional.

Os maiores grupos criminosos de hacking funcionam como verdadeiras empresas. Têm centenas de empregados, pagam salários, têm os seus centros de dados e os funcionários que os mantêm. Têm divisões que recrutam hackers, advogados e analistas.

E os ataques e invasões de sistemas informáticos de grande dimensão continuam-se a suceder. A Google, a Microsoft, a Intel, a Nvidia e a Cisco também foram comprometidas recentemente.

E muitos destes ataques informáticos deixam vírus adormecidos nos sistemas informáticos que acordam um ano ou dois anos, pelo que é fundamental a capacidade reinstalar e reiniciar os sistemas.

Tudo isto mostra de forma clara o quão precipitados e mal preparados estamos como sociedade para implementar e adotar a tecnologia 5G, que, com o esforço de aumentar a capacidade e a velocidade da ligação e massificar a interconexão entre os utilizadores e com os aparelhos eletrónicos, e expandir consideravelmente a economia do digital, aumentará, previsivelmente, de forma significativa o número e a extensão de vulnerabilidades e multiplicará os vetores de ataque, fragilizando substancialmente os sistemas informáticos a ataques muito mais rápidos e, potencialmente, de muito maior dimensão, passíveis de causar disrupções e problemas muito maiores, inclusive financeiros, aos utilizadores e aos serviços que fazem uso da Internet. Tudo em nome do economicismo de vistas curtas, da temeridade, da incapacidade e da falta de vontade de minimizar o risco e proteger a sociedade contra o crime digital e o perigo ambiental, contra a adoção de um comportamento muito mais prudente e responsável perante uma tecnologia nova e experimental.

A preocupação com a sucessão de ataques informáticos em Portugal intensifica-se. Depois do ataque à Imprensa, o site do Parlamento já esteve bloqueado, e seguiu-se um ataque à Cofina, todos em investigação pela PJ. “Estou preocupado, mas apelo que não se fique com medo”, reconheceu o diretor-geral do Gabinete Nacional de Segurança, António Gameiro Marques, em entrevista à TSF. “Tem que se ter racionalidade e nós temos ajudado, promulgando políticas públicas que se forem seguidas contribuem para a maturidade digital da nossa organização”.

O Estado Português decidiu aumentar, em resposta ao ataque informático à Vodafone, em cerca de 30 milhões de euros o orçamento do Centro Nacional de Cibersegurança, no Plano de Recuperação e Resiliência, até 2026, e no sector privado as empresas que não tenham proteções contra ciberataques, capazes de prevenir ou mitigar este risco, podem incorrer em coimas de até 50 mil euros.

Em 2025, a gigante japonesa de bebidas e comida Asahi sofreu um grande ciberataque que parou a maioria das suas fábricas no país e causou a escassez de produtos no Japão.

Mas “se houver um conjunto de ataques sincronizados, param completamente a sociedade. E a pergunta é: quem é que tem a autoridade e responsabilidade de tomar medidas nesta área em Portugal? Não temos resposta.”, declara José Tribolet, professor catedrático jubilado do Instituto Superior Técnico e especialista em cibersegurança.

Israel, por sua vez, em face de um aumento progressivo de ataques informáticos, irá exigir padrões de segurança informática mais exigentes a empresas tecnológicas da área das comunicações, na deteção e prevenção de ciberataques. Tendo identificado esta área tecnológica como preferida por agentes maliciosos para efetuar ataques e procurar acesso a alvos estratégicos.

E agora também começa-se a usar aplicações de Inteligência Artificial para melhorar a cibersegurança. Assim como, previsivelmente, se usam aplicações de Inteligência Artificial para aumentar a eficácia e eficiência do hacking.

Isto pode já ser observado com um ataque informático concertado ao notariado português. Os notários foram alvos de milhares de mensagens potencialmente fraudulentas. O pico ocorreu na semana de 20 de junho de 2023.

O bastonário da Ordem dos Notários Jorge Batista da Silva acredita que este ataque “já foi suportado recorrendo a inteligência artificial (IA)”. Ou seja, “o teor do e-mail e os dados utilizados correspondem a textos muito similares a situações análogas e correspondência eletrónica entre notários, entre notários e clientes, entre notários e bancos”.

Especialistas dizem ser possível, mas garantem que na maioria dos casos envolve, inicialmente, uma conta hackeada.

A maior seguradora e resseguradora do mundo, a Swiss Re, declara que “a frequência e a severidade de riscos resultantes de ataques informáticos e a sua natureza mutável, são esperados crescer significativamente nos próximos anos.”

E continua sublinhando que “tradicionalmente aparelhos de IoT tem mecanismos de segurança pobres. E hackers podem também explorar a velocidade e o volume do 5G, o que significa que mais dados podem ser roubados muito mais rapidamente. Um desenvolvimento de larga-escala em carros autónomos e outras aplicações de IoT significará que os mecanismos de segurança têm de evoluir à mesma velocidade. Sem isso, interrupção e subversão da plataforma 5G pode desencadear danos cumulativos catastróficos.”

A isto acresce o emprego de “edge computing” (computação de borda), onde servidores temporários mais próximos do consumidor são empregues para processamento de dados, de forma a diminuir a demora das comunicações em serviços de rede. Este tipo de funcionamento aumenta a superfície de exposição das empresas e serviços ao hacking. Aparelhos empregues para este tipo de serviço também estão expostos a condições ambientais – que se acredita agravarão com as alterações climáticas.

A Swiss Re conclui que “recentes exemplos revelaram quão mal preparadas companhias e agências governamentais estão para tais ataques [informáticos]”.

O que torna o problema tecnológico consideravelmente mais severo é o facto de diferentes infraestruturas terem configurações de hardware e software próprios, de idade e de fornecedores diferentes, que terão, em alguma medida, de ser combinados com as novas tecnologias emergentes, com os quais poderão não ser de todo compatíveis, podendo gerar problemas críticos adicionais, para lá dos custos acrescidos de manutenção e substituição, e de segurança.

Sobre isto a Swiss Re nota que “soluções digitais e hardware antigo nem sempre harmonizam. Um principal e real exemplo aconteceu em 13 de julho de 2017 quando milhares de viajantes ficaram retidos durante a hora de ponta enquanto a rede do metro de Melbourne entrava em colapso. A razão foi que uma placa de interface com 40 anos usada para conectar com o novo software digital não foi capaz de aguentar o input [influxo de dados] dos carris e sinais do sistema, que eram também eles obsoletos. Este exemplo ilustra o desafio existente. O procedimento corrente é procurar melhorar a eficiência operacional de velhos ativos com atualizações de software. (...) Muito do hardware, no entanto, é ainda do passado.”

E todos os pontos das redes precisam de ser adequadamente mantidos e substituídos com regularidade de forma a manter a segurança e funcionalidade atualizada. A Swiss Re chama atenção para isto, e avisa que pela sistemática falta de manutenção previsivelmente poderá surgir um fenómeno chamado de “Internet of Forgotten Things” (Internet das Coisas Esquecidas), populado por aparelhos mal configurados e obsoletos, especialmente vulneráveis a ataques informáticos.

Em 2018, a OCDE explicou que tais aparelhos inteligentes e conectados podem-se tornar “problemáticos”. Também, os aparelhos inteligentes podem só ser seguros de usar enquanto eles estão em constante ligação. Podem surgir situações nas quais a ligação é interrompida ou nas quais um software ou uma atualização torna o aparelho errático, ou está em falta, tornando o sistema mais inseguro.

E se o fabricante desses aparelhos inteligentes, ou mesmo a empresa específica que produz o software para esses aparelhos, vai à falência ou se recusa a fornecer updates para aparelhos antigos na procura de forçar a compra de novos modelos ou por outras razões económicas ou logísticas, ou fornece updates que estragam o aparelho ou o fazem funcionar pior (por exemplo ‘planned obsolescence’)?

Terão mesmo as empresas de aparelhos inteligentes a capacidade real de proteger eficazmente os seus próprios aparelhos de hacking a longo prazo?!

E atualizações e outro software não-oficiais, para os produtos, normalmente são inseguros e com limitada ou mesmo sem qualquer espécie de garantia, o que se revela extremamente perigoso para produtos inteligentes em funções críticas.

Tudo isto já é um grande problema em termos de segurança informática, quando há uma grande variedade de produtos tecnológicos com ligação à internet desatualizados em funcionamento, ou mesmo até ainda à venda, vulneráveis a *hacking* e/ou contendo erros no seu funcionamento.

Também culturalmente a maioria dos consumidores só muda de telemóvel, tablet, câmaras de segurança, *nanny cam*, *smart tv* quando estas deixam de funcionar ou vêem que a tecnologia está obsoleta para aquilo que desejam do produto. E, por exemplo, existem casos documentados de *hacking* de monitorizadores de bebés.

Isto é especialmente alarmante quando se pensa usar o 5G para potenciar o surgimento das smart cities (“cidades inteligentes”), automatizando a gestão do ambiente, água, iluminação e recolha de resíduos, entre outros. Isto potencia a ocorrência de falhas dos sistemas informáticos, assim como a probabilidade destes serviços serem acedidos por pessoas não autorizadas, com a possibilidade real de despoletar problemas críticos ao funcionamento das cidades e à vida dos seus cidadãos, incluindo em termos de segurança.

Internacionalmente foi amplamente noticiado o hacker alemão que conseguiu abrir e fechar portas de vários Tesla. E apesar de a Volvo ter sido notícia recentemente por um ataque que se julga ter sido na verdade um ato de espionagem, já antes uma empresa alemã viu os sistemas invadidos levantado a questão da cibersegurança na indústria automóvel.

Devemos ter cuidado com o que partilhamos e de que forma partilhamos. A partir do momento em que nos abrimos à comunicação ao exterior no nosso aparelho informático, seja com o bluetooth ligado, seja com wifi ou até mesmo com a rede telefónica, estamos conectados a sistemas que monitorizam a nossa atividade e são potencialmente vulneráveis.

E isto é verdade para quem tem um telemóvel no bolso ou... para quem o tem conectado com o carro!

Um exemplo da vulnerabilidade de sistemas informáticos, anunciada publicamente em 2021, é a possibilidade de um agente malicioso contornar a popular medida de segurança conhecida por 2FA (Two Factor Authentication [Autenticação de Dois Factores]) no Whatsapp, apenas com o número de telemóvel, e desativar a conta da vítima no serviço. Para evitar este problema, o Whatsapp aconselha a adicionar o endereço de email ao 2FA da conta no serviço.

Como se percebe, devemos refletir sobre a segurança dos sistemas informáticos e a nossa privacidade, e segurança pessoal, especialmente em face da implementação experimental da tecnologia 5G.

Nas palavras da Swiss Re, “devido à rápida propagação de aparelhos ligados à Internet e conectividade universal, surgem questões à volta da fiabilidade dos produtos. De forma geral, os riscos no mundo digital aumentaram. A transição da intervenção humana para processos permitidos por software conduz a eficiência e conveniência, mas também vem com novas vulnerabilidades.”

E no relatório de 2021 dedicado a riscos emergentes, a Swiss Re salienta o risco potencial associado a monitores de atividade física (como o Fitbit) de violação de privacidade (incluindo fuga de dados pessoais), referindo também a possibilidade, devido a mau funcionamento, de providenciar informação de saúde errada que poderá levar a dano físico e até morte. De referir que estes aparelhos podem monitorizar padrões de sono, nutrição, exercício, e doenças crónicas.

Em 2023, a Mozilla testou a privacidade e a segurança dos novos modelos de carros conectados à Internet, e todas as grandes marcas de automóveis testadas falharam em aderir da forma mais básica.

Marcas como a BMW, Ford, Toyota, Tesla e a Subaru colecionam dados sobre os condutores, incluindo raça, expressões faciais, peso, informação de saúde e genéticas, e os seus percursos no automóvel. Alguns carros testados ainda colecionavam dados sobre a atividade sexual e status de imigração. A marca que se saiu pior foi a Nissan, que se reserva o direito de partilhar e vender a terceiros informações pessoais sobre “preferências, características, inclinações psicológicas, predisposições, comportamentos, inteligência, habilidades e capacidades”.

A Mozilla declarou incapacidade para determinar se as marcas encriptam qualquer da informação que colecionam.

Segundo a Mozilla, muitas marcas de carros praticam “privacy washing”, apresentando aos consumidores informação que sugere que levam o tema da privacidade a sério, quando a verdade é exatamente o contrário. Muitas das principais marcas participam na Alliance for Automotive Innovation's "Consumer Privacy Protection Principles (PDF), que se resume a

um conjunto vago de promessas não vinculativas organizadas pelas próprias marcas construtoras de carros.

No tema da espionagem ilícita, Portugal alinhará com os parceiros europeus, que se comprometeram a seguir um guião comum para garantir a cibersegurança das redes europeias. A União Europeia prefere não excluir nenhum fornecedor à partida, e sujeitar todas as empresas a uma avaliação de risco que será feita a nível nacional, caso a caso. “Há uma ação concertada a nível europeu e não faz sentido ter uma estratégia divergente”, declara um representante do governo português. Desta forma o governo português não irá aplicar qualquer restrição à escolha das marcas que poderão fornecer componentes ou equipamentos usados em redes móveis de quinta geração (5G). O parecer do Centro Nacional de Cibersegurança (CNCS) apoia esta decisão.

Um risco associado de cibersegurança é o *camfecting*. Isto é quando um hacker toma controlo não autorizado de uma webcam remotamente. isto é feito ao desativar os avisos sobre a câmara estar a ser ativada ou ligada. Investigação sugere que globalmente há mais de 15 000 câmaras (incluindo em casas e negócios) acessíveis a hackers, mesmo sem a necessidade de ser pirateadas. Supõe-se que este tipo de crime informático e de privacidade frequentemente não é denunciado, principalmente devido a passar despercebido à vítima. Há que mencionar que a maioria deste tipo de crimes se deve à procura de dividendos económicos, e não para diversão ou chantagem. Alguns destes ataques são atos de espionagem corporativa, enquanto outros são da responsabilidade de agências de inteligência governamentais. E que a tentativa de chantagem associada a este tipo de crime é muito frequente, e rentável, e por si só não indica que o crime tenha realmente acontecido.

9.3 – O perigo da propaganda online

Outro perigo normalmente ignorado é o potencial à exploração antiética da tecnologia por consultoras de imagem, como a Cambridge Analytica que colecionou os dados pessoais de milhões de utilizadores do Facebook sem consentimento e usou para publicidade e promoção de agendas privadas, tendo um papel considerado relevante nas campanhas do Brexit no Reino Unido e da eleição de Donald Trump Jr. para presidente dos Estados Unidos da América. Que com a tecnologia teoricamente muito mais capaz do 5G, as consultoras poderão aumentar significativamente a sua eficácia na manipulação de massas, e pôr em causa significativamente mais o sistema político democrático e a sua legitimidade.

De notar que pouco depois do escândalo, Mark Zuckerberg confessou que o número de apps suspeitas a escrutinar - semelhantes à que serviu à Cambridge Analytica para recolher os dados pessoais - se situava nos milhares.

O Facebook também foi considerado pela Organização das Nações Unidas como tendo tido um papel determinante no recente genocídio dos Rohingya em Myanmar, na dispersão de propaganda e de ódio contra esta minoria, que culminou com a fuga do que restava deste

grupo étnico do país. “O Facebook tornou-se agora num animal”, afirmou Yanghee Lee, enviado especial da UN para os direitos humanos. Desde então o Facebook tem procurado sinalizar e atuar sobre o discurso de ódio e propaganda, mas o potencial para a identificação de indivíduos e comunidades, e para a propaganda estratégica continua lá.

As redes sociais tornam possível espalhar estrategicamente narrativas manipuladas ao público sensível a elas, com facilidade e sem despende muito dinheiro. A que acresce também a criação de contas falsas, ou até o roubo de contas legítimas, para ajudar a espalhar informação falsa e outras atividades maliciosas.

Atualmente a tecnologia confere aos serviços, que fazem uso dela, uma capacidade sem precedentes de moldar os indivíduos e a cultura, pondo em causa todos os avanços da cultura liberal contemporânea. Um exemplo disto é a “cancel culture”, em português, cultura de cancelamento (de segregação), propagandeada atualmente nas redes sociais, ameaçando qualquer indivíduo ou organização que não alinhe com pontos de vistas subjetivos populares.

E isto é tanto pior quando há indivíduos muito ricos que pagam às redes sociais para usar estes algoritmos altamente eficazes e pouco compreendidos – e ferramentas disponibilizadas –, difundindo propaganda, para destabilizar e erodir a sociedade de países, geralmente democráticos. Com o objetivo de semear a confusão, a divisão, o caos e a violência.

Por exemplo, o exército americano ficou “aborrecido” com a Meta e o Twitter, por estas empresas removerem as contas usadas pelo organismo para propaganda e manipulação, com o fito de realizar operações clandestinas de influência, nas redes sociais Facebook e Twitter.

E isto torna-se tanto pior quando vamos avançando na era da “pós-verdade”, onde a procura de verdade objetiva se vai dissolvendo na subjetividade de diatribes de diferentes pontos de vista, que se vão extremando e politizando, e no abandono de princípios e de valores éticos e morais na política e na vida social, assim como com a instrumentalização de instituições públicas para fins políticos e pessoais. A que acresce a opacidade da administração pública e privada e o uso de propaganda e de *fake news* (notícias falsas), tornando o panorama social progressivamente mais nebuloso e indistinguível, pantanoso: um chão extremamente fértil para teorias da conspiração (válidas e inválidas), divisões sociais e expressões de raiva e violência, num novo tempo de desinformação e de ignorância. Tudo isto conduzindo a uma paralisação social geral, que prolonga a vida de um status quo cada vez mais decadente e erode a confiança nas instituições públicas e destrói a sociedade, quando não usado para conduzir à violência sectária e ao totalitarismo.

Foi reportado que a Rússia, tem no programa de botnet Fronton a funcionalidade de lançar campanhas de desinformação online em escala massiva, imitando a participação online de uma população de pessoas. E que já terá sido usado para isso, e terá afetado o ciclo noticioso da BBC.

Durante a guerra na Ucrânia, foi noticiado que a empresa Meta destruiu uma rede russa de várias contas falsas procurando se passar por agências noticiosas europeias com o intuito de passar propaganda russa sobre a guerra.

A Bulgária tomou a iniciativa de criar uma divisão governamental estritamente de monitorização e reportagem sobre desinformação e fake news nos media e redes sociais. Identificando também a Rússia como fonte de desinformação, à qual os países do leste europeu estão especialmente vulneráveis.

A medida tomada pela Bulgária é tão mais providente, quanto mais fácil e prático se torna criar conteúdo, até com o uso de Inteligência Artificial, e disseminá-lo online com contas falsas, e até programas automatizados (bots), que pode dar origem, a seu tempo, segundo a Teoria da Internet Morta (Dead Internet Theory), a uma Internet povoada maioritariamente por bots e falsidades. Para isto contribuindo a constatada dificuldade das redes sociais de identificarem contas falsas.

Também no Facebook foi destruída outra rede, chinesa, de contas falsas com os objetivos de afetar as eleições americanas de 2022 e criticar o governo checo.

No Youtube, mais de 30 canais foram apanhados com vídeos de propaganda chinesa usando Inteligência Artificial transmitindo informação falsa numa campanha coordenada de influência. A campanha usava entidades e vozes geradas por Inteligência Artificial para comunicar propaganda, tendo atingido 120 milhões de visualizações e 730 mil subscritores.

No relatório que expôs esta situação é salientado que “a habilidade da campanha para juntar e aceder a tal tamanha audiência – e o seu potencial para sub-repticiamente influenciar a opinião pública nestes tópicos – deve ser uma causa para preocupação.”

O uso de Inteligência Artificial na propaganda poupa tempo e dinheiro, enquanto torna muito mais difícil de identificar a fonte do conteúdo e os intermediários associados.

Programas de Inteligência Artificial só devem ser permitidos comunicar connosco quando se identificam ou são identificados como Inteligências Artificiais, como defendeu o investigador israelita Yuval Noah Harari.

A Inteligência Artificial e os avanços na multimédia também têm sido usados para criar *deepfakes*, forjações de performances áudio e/ou visuais de pessoas tão reais que foram empregues na guerra da Ucrânia pela Rússia para convencer o povo ucraniano que o presidente Volodymyr Zelensky teria se rendido. E a tecnologia usada para fazer este tipo de fraudes continua a evoluir, tornando ainda mais difícil de distinguir a realidade da mentira.

Assim como num contexto mais normal, a Inteligência Artificial também tem sido usada para criar forjações, nomeadamente de fotos, de forma a fornecer material para chantagens. Uma surfista portuguesa recebeu ameaças que envolviam supostas fotos íntimas criadas com Inteligência Artificial, que pareciam reais.

Sobre *deepfakes*, Wael Abd-Almageed, investigador da Universidade do Sul da Califórnia, afirmou que “uma vez que esta linha [entre a realidade e a ficção] seja erodida, a própria verdade não existirá”. “Se tu vires alguma coisa e não puderes acreditar mais, então

tudo se torna falso. Não será que tudo se torne verdade. Será apenas que nós perderemos a confiança em qualquer coisa e em tudo”.

A atriz brasileira Paolla Oliveira veio às redes sociais denunciar montagens usando inteligência artificial onde foi inserida, e apelando aos seus seguidores que não confiem em tudo o que veem na Internet.

Recentemente, em 2025, foi dada razão nos tribunais à pretensão de estrelas de Bollywood (Índia) de proteger os seus direitos de imagem de forjações, incluindo com IA.

Mais e mais das ideias, das imagens, das histórias que nos rodeiam e nos afetam são produzidos ou criados por Inteligência Artificial, não por seres humanos, criando outra camada de abstração sobre a realidade.

E estas aplicações de IA são baseadas num conhecimento limitado de nós próprios e comandadas, em geral, pela nossa ganância, tornando-as em ferramentas muito perigosas. E os modelos de Inteligência Artificial estão constantemente a melhorar no que é efetivamente uma competição bilionário entre as várias empresas que desenvolvem AI, com, por exemplo, o Facebook a oferecer bónus e salários de 100 milhões para aliciar investigadores super talentosos.

Nós precisamos de um pacto mundial sobre o emprego da tecnologia que permita alimentar o encontro de algum entendimento comum sobre a realidade, que dê confiança e segurança às sociedades, e seus cidadãos, para agir, ou não somos uma civilização funcional.

E, em geral, nós temos cada vez menos controlo sobre o que acreditamos e sobre o que somos.

9.4 - O perigo da automatização de sistemas informáticos

De referir também a relação entre a inteligência artificial e o 5G, onde, à medida que vamos confiando mais em programas que fazem uso de inteligência artificial pelos seus resultados positivos, com novas tecnologias de comunicação, como o 5G, vamos previsivelmente confiando mais poder a estes programas opacos e a quem faz uso deles. Sendo que facilmente estas aplicações vão, tal como os decisores que as encomendam e fazem uso delas, ser suscetíveis a preconceitos discriminatórios, que podem esconder e perpetuar erros de decisão que originam resultados subtilmente falaciosos, ou mesmo que podem facilmente ser mal interpretados e levar a erros humanos de julgamento. Por vezes com consequências reais graves!

Os algoritmos – usados também, mas não só, em Inteligência Artificial – são opiniões impressas em código. Não são objetivos. São otimizados a alguma definição de sucesso,

normalmente lucro económico. E vão sendo aperfeiçoados. Também com recurso a Inteligência Artificial, quando presente.

Quem já se esqueceu do episódio dos erros em Excel de um estudo de Kenneth Rogoff e Carmen Reinhart que o ministro da economia português Vítor Gaspar, em 2013, usou como argumento para defender políticas de austeridade que reduzissem rapidamente a dívida pública portuguesa?

Os algoritmos, e as aplicações que os usam, numa era de crescente digitalização e automatização do funcionamento das sociedades ocidentais, têm uma relevância progressivamente maior, mostrando-se cada vez mais decisivos e importantes. Assim como os erros decorrentes da sua utilização se tornam cada vez mais críticos...

E poucos têm um conhecimento profundo sobre como os algoritmos funcionam, especialmente com o facto de ao empregarem machine learning, os próprios programas mudarem a sua forma de funcionar automaticamente, em busca do objectivo declarado para eles.

Um exemplo disto é um programa de Inteligência Artificial que foi ensinado a analisar radiografias por uma equipa internacional de investigadores do Canadá, Estados Unidos, Austrália e da República da China (Taiwan). O programa tornou-se capaz de identificar a raça do paciente com base na radiografia com uma taxa de sucesso de 90%, e os investigadores não sabem como. E nem cientistas do MIT (Massachusetts Institute of Technology) e da Harvard Medical School conseguem o explicar.

Como seres humanos, nós quase perdemos o controlo sobre estes programas informáticos.

Para o pensador Yuval Noah Harari o verdadeiro pesadelo é a Inteligência Artificial continuar a tirar poder dos seres humanos até que fiquemos impotentes e perdidos sobre o que está a acontecer no mundo. E isto já começa a acontecer a um ritmo acelerado. Mais e mais decisões sobre as nossas vidas são assumidas pela IA – por exemplo se nos é dado um empréstimo, um aluguer, um emprego. E a forma como estes algoritmos operam também começa a escapar ao nosso controlo.

E a Inteligência Artificial impacta as estruturas sociais, económicas e políticas, e frequentemente faz-lo de uma forma imprevisível.

E cientistas brincam imprudentemente, como crianças, com a Inteligência Artificial à procura da criação de uma inteligência geral ao nível de capacidades do ser humano. Que, segundo investigadores, acabará por se tornar impossível de controlar, ao transcender as capacidades humanas.

Já agora pesquisadores reportaram ver a ferramenta de inteligência artificial "AI Scientist", desenvolvida pela empresa japonesa Sakana AI contornar os parâmetros que lhe foram atribuídos e executar ações contrárias às intenções dos seus programadores.

Margrethe Vestager – vice-presidente executiva da Comissão Europeia – afirmou que a Inteligência Artificial pode “virar-se contra nós”, referindo que têm havido “demasiados casos” de preconceitos que enviesam os algoritmos de IA e casos de utilização nos quais há discriminação contra mulheres e pessoas pertencentes a minorias. Adiantando que “vemos diferentes usos de Inteligência Artificial, usos que pensáramos que vão contra os fundamentos da democracia — em que o ponto de partida é a integridade e a dignidade do indivíduo“. “A democracia é tão frágil. O meu receio é que os cidadãos se sintam alienados, sem controlo e sem saberem como o ganhar“, acrescentou. Salientando a comissão que “A conveniência mata a curiosidade”.

Um dos escândalos sobre o uso Inteligência Artificial dentro da União Europeia foi o “toeslagenaffaire”, em 2019 na Holanda. A autoridade fiscal holandesa usou ilegalmente (violando o regulamento de proteção de dados em vigor na União Europeia) um algoritmo de Inteligência Artificial para detetar possíveis fraudes fiscais sobre a atribuição de abono de família. Com isto, o estado holandês penalizou famílias baseado apenas na suspeição de fraude decorrente do resultado do funcionamento do algoritmo. Isto causou dezenas de milhares de famílias – frequentemente com baixos ordenados ou pertencentes a minorias étnicas – serem empurradas para a pobreza durante anos por dívidas exorbitantes à autoridade tributária. Algumas das vítimas cometeram suicídio, e mais de mil crianças foram retiradas às suas famílias.

O próprio governo português em setembro de 2024 anunciou que iria fazer uso de ferramentas de Inteligência Artificial para inspecionar os contribuintes e sinalizar fugas aos impostos.

Segundo Kit Walsh, advogada e diretora assistente da Electronic Frontier Foundation (EFF), um dos pontos fracos mais consistentes da IA é que reproduz, de forma intrínseca, os preconceitos que possam estar embebidos nos dados usados para a treinar. "No caso de IA que produz texto, isto pode levar a respostas que incorporam uma visão dominante da era refletida nos dados usados para a treinar, em vez de resultados que realçam as experiências minoritárias ou desafiam o status quo dessa era."

Os preconceitos na IA são problemáticos e há várias iniciativas em curso, da IBM à Google e outras gigantes, para evitar que deturpem os modelos que estão a treinar. Ao passo que um professor pode fazer uma autorreflexão e examinar potenciais preconceitos na matéria a dar, o computador fará apenas aquilo que for treinado para executar. Mas fá-lo-á com tanta autoridade que o utilizador poderá confiar demasiado nas respostas, perdendo o sentido de pensamento crítico. Essa é outras das dificuldades identificadas pelos especialistas.

"O problema é que as pessoas confiam demasiado na máquina, porque pensam que é superinteligente, feita por programadores inteligentes e, por isso, é A verdade", explicou Gerd Leonhard, fundador da The Futures Agency e autor de vários livros sobre tecnologia. "É um antropomorfismo, quando pensamos que a máquina é humana", continuou. "Pensamos que é até melhor porque é uma máquina, que não tem preconceitos, nem sentimentos."

O futurista considera que o avanço da IA é benéfico e levará a progresso económico e social. "Mas também temos de entender quais são os efeitos secundários", disse. "Não podemos deixar que os nossos filhos cresçam a acreditar que o que está dentro da máquina é superinteligente e tem todas as respostas." Será preciso reforçar a necessidade de fazer perguntas e ponderar, "ao invés de seguir cegamente a tecnologia".

Isso é algo que Kit Walsh refere. "A IA pode dar a aparência de conhecimento ou imparcialidade quando produz respostas imprecisas", frisou. Este problema deve ser endereçado, "educando os utilizadores sobre os limites do sistema".

E muito dependerá da qualidade dos dados que forem usados e de quem decide da sua credibilidade, o que é um desafio cada vez maior. "Estamos com um problema de saber, em cada contexto, quem são as pessoas credíveis", sublinha Paulo Novais, professor do Departamento de Informática e investigador no centro ALGORITMI, na Escola de Engenharia da Universidade do Minho. "Temos de ter capacidade de coar a informação, de perceber quando ela pode ser útil ou não e credível ou não."

O investigador considera que este tipo de sistemas aproxima a IA da condição humana e isso é interessante, mas requer cuidados. "Mais uma vez se nota que quem tem acesso aos dados neste novo mundo é o detentor do poder, para o bem e para o mal."

Existe por exemplo uma aplicação de inteligência artificial, uma variante do Auto-GPT, chamada ChaosGPT que está criada para gerar eventos reais imprevisíveis e caóticos, e à qual é possível comprar o acesso. Em um vídeo, o programa é posto a trabalhar com os objetivos de (1) destruir a humanidade, (2) estabelecer domínio global, (3) causar caos e destruição, (4) controlar a humanidade através da manipulação e (5) atingir a imortalidade.

A Comissão Europeia, por sua vez, em 21 de maio 2024 apresentou legislação sobre o emprego de Inteligência Artificial para restringir o uso de sistemas de alto-risco de IA e banir certos usos "inaceitáveis" – como a manipulação comportamental, a pontuação social e policiamento preditivo – de forma a poder abrir, com confiança, o grande mercado do sector público na União Europeia também à IA. Também será criado um registo europeu público de aplicações de IA num esforço de promover a transparência e ajudar à supervisão. A legislação entrará em vigor passado dois anos, em 2026, com algumas exceções.

Esta lei providencia exceções tais como para sistemas usados exclusivamente pelo exército e defesa, assim como para propósitos de investigação científica.

No ponto de vista da eurodeputada holandesa Kim van Sparrentak, esta legislação não vai proteger os cidadãos europeus de perigos similares ao do caso holandês acima referido. A eurodeputada está a propor a realização de estudos de impacto nos direitos fundamentais civis das propostas de lei europeias sobre a IA, e a publicação destes no registo da União Europeia sobre a IA.

Nas palavras da eurodeputada, “a predição de fraude e policiamento preditivo baseado no perfilamento deviam ser banidos. Porque nós temos visto só muito maus resultados e nenhuma pessoa pode ser determinada com base em alguns dos seus dados.”

Também têm surgido outros usos menos escrupulosos, que estão a causar alarme social.

Como programas de Inteligência Artificial comercializados para gerir investimentos imobiliários e o valor das rendas, como o YieldStar, procurando maximizar o lucro dos arrendadores, em desfavor dos arrendatários.

Outro caso foi um entusiasta de programas de Inteligência Artificial disponíveis gratuitamente na Internet, usar estes softwares para criar um livro infantil num fim de semana, com a história co-autorgada pelo programa ChatGPT e as imagens criadas pelo programa Midjourney. Esta obra foi disponibilizada para venda na Amazon.

De referir que programas como o Midjourney usa para referência conjuntos de milhões de imagens da Internet, criadas por autores humanos, para aprender.

Também este ano a companhia de bailado San Francisco Ballet usa imagens obtidas do programa Midjourney para promover a sua produção d’ O Quebra Nozes. Evitando assim pagar o trabalho a artistas gráficos.

A Inteligência Artificial tem sido em geral usado para fazer o trabalho criativo para pessoas aborrecidas, eliminando a necessidade do envolvimento de criativos e de esforço artístico, em vez de ajudar os artistas a eliminar o aborrecido do seu trabalho. Tem servido para marginalizar os artistas e para pôr em risco a sua segurança financeira, afetando adversamente a cultura.

Mas o Gabinete de Direitos de Autor dos Estados Unidos está em processo para excluir da obtenção de direitos de autor trabalhos artísticos baseados em Inteligência Artificial.

Entretanto, em 18 de agosto de 2023, no caso Thaler v. Perlmutter, o Tribunal Distrital dos Estados Unidos para o Distrito de Columbia confirmou que trabalhos gerados autonomamente por inteligência artificial (AI) não têm direito a proteção sob a Lei De Direitos Autorais americana. Na sua decisão o tribunal afirmou que a criatividade humana é indispensável ao direito intelectual, mesmo quando esta é canalizada através de novas ferramentas ou para novos meios de comunicação.

A China também lançou regras compreensivas sobre o uso autorizado de IA generativa em 15 de agosto de 2023 dirigido ao uso do público, não abrangendo universidades, empresas e outras organizações. As novas leis exigem que serviços generativos de IA (Midjourney, ChatGPT, etc.) não infrinjam na propriedade intelectual de outros, incluindo no treino de modelos de inteligência artificial. Texto, imagens, áudio e vídeos gerados usando conteúdo criado por AI são também obrigados a incluir uma marca de água ou aviso áudio, declarando o uso de inteligência artificial.

A Microsoft e a união de trabalhadores da empresa ZeniMax, a Zenimax Workers United, atingiram um acordo inédito sobre o uso de ferramentas de Inteligência Artificial no desenvolvimento de jogos que visa proteger os trabalhadores e integrar as tecnologias no ambiente de trabalho, oferecendo esperança sobre o futuro laboral.

Algoritmos de Inteligência Artificial começam também a ser integrados em motores de busca, por exemplo da Google e da Microsoft (Bing), conjugando diferentes perspectivas e informações complexas em resultados de fácil digestão, apresentados com um discorrer de frases completas, como um ser humano, segundo a lógica e perspectiva expressas no programa de Inteligência Artificial. Com isto oferecendo uma nova camada de abstração entre a informação e o utilizador, que pode desvirtuar a informação e até a utilizar em teses perigosas.

Este tipo de aplicações de Inteligência Artificial ajudam a sintetizar vastas quantidades de informação, mas também retiram poder de decisão, sentido crítico, capacidade de investigação e síntese, e entendimento sobre os temas pesquisados aos seus utilizadores, subordinando a informação apresentada a preconceitos inerentes, sobre os quais não informam.

Em situações em que não há uma resposta objetiva, fácil, é importante deixar as pessoas encontrarem as suas respostas.

Esta simplificação da informação não é sempre um problema, no entanto. Depende realmente do uso que fazemos da aplicação de Inteligência Artificial. Permite encontrar a resposta a questões factuais (como quantos dias tem fevereiro este ano) e fornecê-la em linguagem cuidada, imitando a humana.

Este cuidado na resposta desarma os nossos preconceitos associados à autoridade intelectual. Normalmente associamos uma expressão polida de ideias a inteligência e conhecimento e, com a ausência de apresentação de fontes que a apoiam, nos impede de ser capazes de desconstruir a resposta dada, dificultando o julgamento crítico da mesma.

E com o aumento da capacidade de armazenamento e da velocidade de processamento e de transferência de informação, levanta-se a questão de que problemas lhe vamos pedir para resolver. Questões meramente factuais, ou todo o tipo de questões? Deixaremos as máquinas pensarem criticamente por nós?

Noam Chomsky afirma sobre os usos do programa de Inteligência Artificial ChatGPT, que permite “plágio evoluído tecnologicamente” e oferece “uma forma de evitar aprender”.

Mas também a produção de investigação científica tem sido afetada negativamente pela Inteligência Artificial, com a proliferação de artigos de má qualidade, plagiados ou falsos, com pelo menos 60 mil artigos produzidos com a ajuda da IA em 2023 e devendo estar a ocorrer um aumento significativo em 2024.

Também alarmante é o facto de que os programas que fazem uso de Inteligência Artificial podem evoluir exponencialmente no sentido dos objetivos que lhes são dados, com preconceitos incluídos. Enquanto a fisiologia e a inteligência humanas pouco evoluem.

E pior ainda é o facto de as aplicações de Inteligência Artificial podem degenerar em resultados progressivamente mais pobres e menos diversos à medida que os seus resultados e de outras aplicações de Inteligência Artificial são alimentados ciclicamente à máquina. Isto pode afetar programas como ChatGPT e motores de busca que fazem uso de programas como este.

Agora na União Europeia os cidadãos podem contestar decisões assentes estritamente no processamento automatizado dos seus dados pessoais e perfilamento. (Artigo 22 do GDPR).

Kit Walsh, advogada e diretora assistente da Electronic Frontier Foundation (EFF), adverte que é preciso ponderar os riscos, juntamente com os benefícios, da Inteligência Artificial, que este ano tem registado avanços notáveis não só ao nível do texto, mas também da geração de arte a partir de imagens e vídeos.

"A tecnologia IA inclui muitas promessas de melhorar a criatividade humana, mas requer uma abordagem cuidadosa para realizar o seu potencial sem causar danos", afirmou a responsável. "Apesar destes cuidados, não queremos perder de vista o potencial positivo de facilitar o processo de criação das pessoas."

Mas este entusiasmo, compulsão e uso generalizado de Inteligência Artificial a nível mundial ameaça ter custos energéticos muito elevados. Um estudo publicado em 10 de outubro de 2023 discute a crescente pegada energética da inteligência artificial (IA) e seu potencial impacte ambiental. A rápida expansão e ampla aplicação da IA nos últimos anos, especialmente com o lançamento do ChatGPT da OpenAI, aumentou a preocupação sobre o consumo excessivo de eletricidade para suportar estas ferramentas. Alex de Vries, o estudante de Doutoramento que realizou este estudo, receia que o aumento da eficiência da IA como ferramenta leve a um efeito de ressalto (*rebound*). Isto é, desenvolvemos a tecnologia para que se torne mais eficiente no consumo de energia e, por causa disso, as pessoas usam mais a ferramenta e todo o trabalho de investigação realizado para diminuir o consumo acaba por voltar à estaca zero.

E de acordo com o secretário-geral da Organização das Nações Unidas (ONU), António Guterres, a Inteligência Artificial pode ajudar países em desenvolvimento e o acesso deve ser facilitado.

Segundo o português, a IA tem potencial para ajudar os países em desenvolvimento cujas economias foram afetadas pela pandemia da covid-19 e que resultaram numa acumulação de dívidas.

Tudo isto acaba alimentando um indústrias que usam a IA e todas as outras ferramentas à sua disposição para gerar lucros, contribuindo para uma pioria geral dos serviços e produtos fornecidos para os consumidores, num fenómeno conhecido *enshittification*.

10 - Estados Unidos versus China na arena geopolítica mundial: Huawei, ZTE, Xiaomi

As recentes suspeitas lançadas por agências de segurança americanas sobre a Huawei, ZTE, TikTok e outras companhias chinesas, sobre a intenção de espionar sobre utilizadores estrangeiros a serviço do governo Chinês. Existe nisto aparentemente uma dimensão de projeção psicológica das forças americanas em relação às suas congéneres chinesas, numa altura em que a China se afirma como uma super-potência capaz de rivalizar com os Estados Unidos da América e os seus aliados, e demonstra o seu poder e espírito impiedoso, tendo estabelecido uma aliança estratégica com a Rússia.

O governo dos Estados Unidos identificou vulnerabilidades na estratégia nacional ao nível das telecomunicações, assim como outras fragilidades, com algumas delas inerentes à auto-regulação dos mercados económicos, que podem expor criticamente a rede de telecomunicações americana, e de países aliados, a países e a interesses rivais (nomeadamente a China), e colocar empresas nacionais e de países aliados em posição de crescente desvantagem. Mais tarde isto foi corroborado pela agência reguladora de comunicações americana FCC (Federal Communications Commission), fazendo referência à Huawei e à ZTE, que são duas empresas chinesas que figuram entre os líderes de mercado em fornecimento de material de telecomunicações e em telecomunicações móveis, perante a ausência de empresas americanas de igual valia. E isto tudo perante estudos e notícias de mercado que apontam para uma vitória da China em relação aos Estados Unidos sobre a implementação do 5G, e também a nível económico a longo prazo. Isto levou os Estados Unidos a limitar progressivamente a penetração da Huawei e da ZTE no seu mercado interno, assim como urgir e pressionar os seus aliados e parceiros estratégicos a fazerem o mesmo, e boicotar estas empresas, procurando isolá-las (e à China) no mercado do 5G, pressionando-as económica e logisticamente.

A própria NATO²⁰ considera a China, na sua grande expansão tecnológica e económica, com o muito ambicioso projeto comercial e diplomático da Nova Rota da Seda a ser construído, e em especial com a aproximação política à Rússia, um risco elevado à liberdade, democracia e segurança dos seus países constituintes, que, por sua vez, mantêm as suas próprias relações com a China, criando divergências na política comum e clivagens. Embora devido ao CoV-Sars-2, à política nacional de contenção da pandemia, e a situação económica e geopolítica global, a China tem vindo a experimentar uma desaceleração económica, e mesmo a ameaça de crise económica.

Por sua vez na União Europeia, a 12 de março de 2019 o Parlamento Europeu aprovou em plenário uma resolução pedindo ação a nível da União Europeia sobre riscos à segurança ligados à crescente presença tecnológica da China dentro da união. Nela, membros do Parlamento Europeu pedem à Comissão e aos estados-membros para providenciar orientação em como lidar com riscos informáticos e vulnerabilidades quando procurando equipamento

20 - A NATO (North Atlantic Treaty Organization), também chamada de North Atlantic Alliance, e de OTAN (Organisation du traité de l'Atlantique nord, em português Organização do Tratado do Atlântico Norte) é uma aliança militar intergovernamental, com 30 países membros na América do Norte e Europa, incluindo Portugal como um dos membros fundadores.

5G e estabelecer uma estratégia para reduzir a dependência da Europa em tecnologia de cibersegurança estrangeira. Adicionalmente, a resolução pede à Comissão para incumbir a ENISA (Agência de Cibersegurança da União Europeia) de trabalhar num esquema de certificação assegurando que a instalação de 5G na União Europeia atinge os padrões de segurança mais elevados.

Em 9 de outubro de 2019, países membros, com o apoio da Comissão Europeia e da ENISA, publicaram um relatório sobre a avaliação de risco coordenado da União Europeia acerca de cibersegurança em redes 5G.

A 3 de dezembro de 2019 o Conselho Europeu publicou as suas conclusões sobre o tema da mitigação de riscos de segurança acerca da instalação de 5G na União Europeia.

E para diminuir os riscos de interferência maliciosa nas instalações de 5G e nas aplicações web na União Europeia, a Comissão publicou, a 29 de janeiro de 2020, a “caixa de ferramentas” 5G – um conjunto de medidas de mitigação dos riscos associados à tecnologia 5G trabalhado por instâncias nacionais e supranacionais (Grupo de Cooperação NIS e Agência de Cibersegurança Europeia) - respeitante à gestão desta tecnologia pelos países da União Europeia, em resposta às exortações do Conselho Europeu a uma abordagem conjunta na segurança das redes 5G, e seguindo as recomendações da própria comissão. A sua implementação é responsabilidade dos países sob a visão atenta da Comissão Europeia.

A 3 de fevereiro de 2021 a Comissão Europeia pediu à ENISA para preparar um esquema de certificação sobre cibersegurança da União Europeia para redes 5G.

A República Checa e a Letónia firmaram pactos com os Estados Unidos para fortalecer a cooperação ao nível da segurança das redes 5G e a adoção de padrões rigorosos para a aprovação de fornecedores de equipamento de telecomunicações.

Na Bélgica, o Conselho de Segurança Nacional prometeu barrar vendedores de alto risco da construção do núcleo da rede 5G, e também limitar a quantidade de componentes que, de outro modo, estes fornecedores podem prover, enquanto operadoras de telecomunicações nacionais optaram pela Nokia para construir as suas infraestruturas de tecnologia 5G, abandonando o uso da Huawei, por pressão americana.

Na Alemanha, o governo admitiu uma supervisão mais rigorosa dos fornecedores de material de telecomunicações 5G, não chegando a banir a Huawei do seu mercado interno. O conglomerado de telecomunicações Telefonica Deutschland anunciou que usará a Ericsson para o núcleo da sua rede 5G.

Em Itália, o governo impediu o grupo de telecomunicações Fastweb de assinar um contrato de fornecimento de material com a Huawei para a sua rede 5G.

Na Noruega, enquanto o governo não bane o uso de equipamento da Huawei nas redes 5G do país, a operadora de telecomunicações Telenor opera a substituição de equipamento da Huawei na sua rede por tecnologia da Ericsson.

Na Polónia foi capturado um suspeito de espionagem, empregado da Huawei, o que provocou a marginalização da fornecedora de material de telecomunicações chinesa na instalação 5G do país. A operadora de telecomunicações Polkomtel anunciou que irá usar equipamento Ericsson na sua rede 5G. Enquanto que o governo polaco comprometeu-se a aplicar as proteções propostas para a segurança sobre redes 5G aprovadas pela União Europeia, apesar de referir que o país reserva o direito de, em alguns casos, aplicar medidas ainda mais rigorosas.

No Brasil há grande discussão entre usar ou não usar Huawei, tendo o governo americano se oferecido para financiar a compra de equipamento 5G da concorrência.

O Canadá, na figura do seu ministro da Inovação, Ciência e Indústria, afirmou que decidirá a sua política sobre a tecnologia 5G em função dos interesses do país, e não se deixará manietar pelos interesses de países terceiros. Por seu lado, o exército pressiona à proibição do uso de equipamentos da Huawei na rede 5G nacional. E, no contexto da guerra na Ucrânia e seguindo as posições dos Estados Unidos, Austrália, Nova Zelândia e Reino Unido (que com o Canadá formam a organização de segurança internacional Five Eyes), pela voz do seu ministro da indústria anunciou que a Huawei e a ZTE serão banidas da infraestrutura de telecomunicações canadianas.

Rumores apontam a que a França não proibirá a Huawei de fornecer componentes não-essenciais à rede 5G do país. A Huawei, anunciou por sua vez, planos para investir 200 milhões de euros para construir a sua primeira fábrica de componentes de telecomunicações em solo francês. Enquanto que a maior empresa de telecomunicações francesa, Orange, anunciou que irá usar componentes da Nokia e da Ericsson na sua rede 5G.

A Coreia do Sul, por sua vez, se encontra entre o desejo de não antagonizar o seu maior parceiro comercial (China) e o seu maior aliado militar (Estados Unidos).

E as operadoras de telecomunicações portuguesas, apesar de trabalharem com diferentes fornecedores de equipamentos de telecomunicações - sobretudo Ericsson, Nokia, Huawei ou Cisco -, quando se trata de componentes para o core da rede não contam com a gigante chinesa. É público que deixaram de recorrer à Huawei para alimentar o núcleo das redes 5G.

A empresa Meta não permite mais a pré-instalação das suas apps (nomeadamente de Facebook) em telemóveis da Huawei.

A Vodafone planeia remover os componentes nucleares da Huawei das redes de telecomunicações europeias da empresa até 2025.

E dentro da União Europeia, a European Competitive Telecommunications Association (ECTA) – um grupo de operadoras de telecomunicações e contendo também a Huawei – rejeita qualquer proibição do uso de tecnologia 5G de empresas chinesas por razões geopolíticas, enfatizando a necessidade de factos, e apontando que a redução de fornecedores de tecnologia 5G aumentará custos, impactará negativamente a performance, atrasará o desenvolvimento das redes 5G e limitará a inovação.

Enquanto isto, a Huawei expande-se consolidando a sua posição de dominância no mercado chinês, em especial no segmento de telemóveis e instalações 5G, proliferando pelo sudoeste asiático (implantando-se no Bangladesh por exemplo), estabelecendo programas de desenvolvimento tecnológico a nível de cloud computing, inteligência artificial e big data na América do Sul, em especial do Brasil, e expandindo-se pelo Médio Oriente e por África, avançando a influência e interesses chineses a nível mundial, nos quais se incluem a coleção de dados privados.

Mas a posição do governo norte americano em relação à espionagem chinesa e à própria China é tornada mais complexa e subtil com o seu comportamento em relação a outra multinacional chinesa, a Xiaomi.

A Xiaomi é uma empresa chinesa que tem visto um sucesso meteórico no mercado dos telemóveis, se popularizando na Europa, aproveitando o boicote dos Estados Unidos e das empresas americanas (incluindo a Google) à Huawei. Estimando-se que em vendas no primeiro trimestre de 2020 no mercado Europeu esteja em 4º lugar, atrás de Samsung, Apple e Huawei, com uma subida das vendas em 80% (para uma descida de 40% da Huawei em igual período).

A Xiaomi foi muito recentemente envolvida em polémica no tema da privacidade, com o anúncio que os telemóveis da empresa faziam uma recolha das informações no telemóvel e dos dados de utilização de Internet que em muito excedia as normas da indústria, e que esses dados eram alegadamente enviados para a China. A Xiaomi rejeitou essas acusações, mas anunciou que providenciaria opções de desativar essas coleções de dados pessoais nas próximas atualizações do software, assim como a possibilidade de rejeitar o envio dos dados para a China.

O governo dos Estados Unidos continua a não aplicar sanções, permitindo à empresa usar o sistema operativo Android (da Google) nos seus telemóveis, assim como outros componentes americanos. Razões para este tratamento diferente parecem residir em parte no facto da Xiaomi ser uma empresa listada publicamente na bolsa de Hong Kong (ao contrário da Huawei com estrutura complexa e ambígua de controlo privado), operar exclusivamente no mercado retalhista, e ser uma competidora da Huawei e da ZTE.

“Todas as tecnologias transformadoras a nível global começam por ter, de início, diferentes abordagens geográficas e políticas associadas a pretextos tecnológicos. (...) Importa, pois, que no 5G a definição de standards – crítica para a obtenção transversal de todas as suas potencialidades – não seja limitada por interesses individuais de nações específicas. Dada a importância do 5G para as sociedades futuras, é legítimo e compreensível que existam reservas por parte dos Estados Unidos, motivadas por questões de defesa da sua soberania. (...) É uma posição de salvaguarda legítima dos EUA considerando vários fatores, tais como i) a tradicional liderança dos EUA no desenvolvimento das tecnologias de TIC [Tecnologias da informação e comunicação] ii) a crescente e rápida influência de empresas e tecnologias chinesas no mundo ocidental e iii) a importância que o 5G terá nas sociedades digitais do futuro. (...) Os EUA estão a assumir naturalmente nesta, tal como noutras matérias de inovação tecnológica, o seu papel de potência mundial, em que o empreendedorismo

imprime um enorme dinamismo ao mercado. A dimensão do mercado é um fator impulsionador, mas há outros, como a própria sofisticação tecnológica”, afirma António Martins da Costa, presidente da Câmara de Comércio Americana em Portugal.

A União Europeia e o Reino Unido, por sua vez, dividem-se entre a procura de não alienar os Estados Unidos, de abrir o seu mercado aos gigantes chineses e à nova Rota da Seda (uma nova iniciativa chinesa comercial em desenvolvimento), não provocar a China, e a tentativa de manter algum nível de segurança na sua infraestrutura de telecomunicações.

11 - A questão económica do 5G

A tecnologia 5G é um negócio de milhares de milhões para alguns países e as suas organizações nacionais supervisoras de telecomunicações (especialmente na União Europeia), que conduzem leilões para a atribuição do direito ao uso de frequências eletromagnéticas específicas por parte de empresas privadas na área das telecomunicações. E esse dinheiro desaparece nas contas das supervisoras e do Estado, ficando os cidadãos apenas com a possibilidade de ter serviços de Internet Móvel melhores a um preço, não recebendo nenhum dos benefícios financeiros, pelo menos diretamente, pelo espaço de frequências que pela sua residência nacional razoavelmente também lhe pertence.

Assim como se prevê que o 5G ajude a gerar 12.3 biliões de dólares (\$12 300 000 000 000) em serviços e bens para o sector empresarial, com a cadeia de valor do 5G gerando em si própria até 3.5 biliões de dólares e criando 22 milhões de empregos mundialmente, tudo, até 2035. E acredita-se que o 5G promova o crescimento da economia mundial em 3 biliões (3 000 000 000 000) de dólares de 2020 a 2035.

Para a União Europeia o 5G é uma prioridade desde 2016. A Comissão Europeia acredita que os 27 países da UE deverão gastar 400 mil milhões (400 000 000 000) de euros no desenvolvimento do 5G até 2025, e estima-se que a nova rede acrescente um bilião (1 000 000 000 000) de euros ao PIB europeu, entre 2021 e 2025. O 5G tem ainda o potencial de "criar ou transformar até 20 milhões de empregos", segundo o Tribunal de Contas Europeu.

No website da própria União Europeia é afirmado que o “5G desempenhará um papel chave no futuro desenvolvimento da economia e sociedade digitais da Europa. (...) Com rendimentos mundiais no 5G estimados de 225 milhares de milhões de euros em 2025, o 5G é um bem crítico para a Europa competir no mercado global”.

Líderes empresariais, políticos e *opinion-makers* pelo mundo fora acreditam que o 5G trará benefícios generalizados para a sociedade e a economia, permitindo novos produtos, serviços e usos, e aumentando a produtividade e a riqueza.

Estima-se que o telemóvel, com o 5G, será elevada ao estatuto de tecnologia de propósito geral, como a eletricidade ou o carro. Isto proporcionará ao telemóvel, e às tecnologias

móveis, uma atenção mais generalizada, que se crê que proporcionará uma fundação para inovações massivas, que levará à criação de novas indústrias e beneficiar economias inteiras, através da capacidade dos telemóveis e outros dispositivos móveis de conectar cada vez mais as pessoas a tudo o resto. Com isto assegurando o impacto a longo prazo na sociedade destas tecnologias e crescimento continuado durante as décadas que se seguem.

A adoção da tecnologia 5G tornou-se numa batalha geopolítica, económica, tecnológica, e aparentemente social, para os Estados Unidos e a China - que se estende para lá da guerra comercial entre estas duas superpotências económicas -, assim como um investimento de milhares de milhões de euros (ou dólares) para ganhar biliões para as empresas que comercializam a tecnologia (fornecedores de peças e operadoras de telecomunicações) e para especuladores e fundos de investimento, e uma fonte de receitas milionárias, ou até bilionárias, para os países que vendem bandas de frequências para as operadoras desenvolverem a sua oferta comercial dentro do país. E nisto tudo, a prudência, a ciência, a saúde, a ecologia e o bom senso, são deixados para trás, enquanto interesses extremamente poderosos privados procuram acelerar ao máximo o processo de migração para a tecnologia 5G, independentemente de consequências negativas que possa trazer, e sem esclarecer quais exatamente são os benefícios que procuram. Mas nisto tudo há a certeza que os ganhos financeiros potenciais são extremamente elevados!

As receitas das operadoras de telecomunicações vêm atualmente de assinantes que pagam taxas mensais. Estas caíram nos últimos anos e ninguém espera que aumentem, mesmo com o 5G. Se a base de assinantes for a mesma, a receita cairá. As operadoras esperam encontrar novos assinantes na forma de setores verticais da indústria, como carros ou dispositivos da Internet das Coisas (IoT), mas mesmo aqui não há um fluxo claro de mercado e de receita. Sem crescimento de receita, é difícil justificar investimentos maciços em 5G. Nesta altura, 85% dos europeus (465 milhões) já dispõem de assinaturas de dados móveis.

Em Itália, por exemplo, as empresas de telecomunicações tiveram de gastar 6,5 mil milhões de euros, apenas no leilão de ondas de alta velocidade do novo 5G. Isso foi mais do dobro do que o governo italiano previra, criando um custo "ruinoso" para as empresas.

Quem ganha? Governos e empresas tecnológicas. Para os fabricantes (Ericsson, Nokia, Huawei, etc.) há um claro benefício: se o 5G for amplamente implantado, eles venderão mais equipamentos para os operadores. Para os governos, percebe-se ser um benefício político e económico alinharem com a mais recente tecnologia digital (e os ministros, e outros governantes, quase nunca entendem as questões envolvidas). O problema é que não é do interesse da maioria dizer algo negativo sobre o 5G, já que isso não traz nenhum benefício.

Também as empresas tecnológicas cuja atividade assenta sobre as telecomunicações – por exemplo empresas de blockchain (incluindo de NFTs), de streaming de entretenimento, de armazenamento e/ou serviços de cloud, de casino online e de apostas - também vêm grande benefício na implantação do 5G.

Isso significa que o *hype* pode ficar fora de controlo.

Com tudo isto a comunicação social convencional nos encoraja a estar excitados com a nova tecnologia 5G, e desvaloriza os receios e medos, apontando declarações da organização de supervisão para as telecomunicações Americana, a FCC, e de associações do ramo das telecomunicações, e escrevendo artigos de opinião jornalísticos - em que mais que jornalistas eles se mostram verdadeiros cientistas nas palavras - asseverando total confiança na tecnologia, e nos aconselhando a não estar preocupados. Muitas vezes se apoiam na guia do ICNIRP como base sólida de suas teses, o que contraria a posição de 2008 do professor Paolo Vecchia - presidente do ICNIRP de 2004 a 2012 -, onde afirma que as guias de exposição “não são prescrições mandatórias para a segurança.” “Não são a ‘última palavra no assunto”, e “não são muralhas defensivas para a indústria ou outros”. A que acresce o facto de que as suas orientações se concentram na saúde humana, e não têm aplicação ao resto da natureza.

Nos encorajam a receber a nova tecnologia de olhos fechados e corações bem abertos.

O resultado é um grande salto no vazio. No qual os fabricantes de hardware e software de telecomunicações, empresas de telecomunicações, empresas de componentes, outras empresas tecnológicas, e as estruturas governativas (nacionais e locais) preferem que avance sem impedimentos.

Não é o público em geral que pressiona para a rápida adoção da tecnologia 5G.

12 - Automatização de postos de trabalho e anonimização e precarização dos trabalhadores

O sonho do 5G, da Internet das Coisas e da Inteligência Artificial irá também acelerar a automatização dos locais de trabalho, e contribuir para um crescimento acentuado do nível de competitividade industrial, da redundância no mercado de trabalho e desemprego (estrutural) a nível mundial, assim como levar à procura de migrar esses desempregados para novas áreas, nas quais têm geralmente menos hipóteses de competir, em especial perante uma competitividade crescente nestas áreas, alimentada por esta e outras causas do aumento da procura de emprego nelas, ajudando também a baixar salários. Mas a automatização de processos e um aumento de empregos menos qualificados também podem levar a uma desaceleração do aumento da produtividade. Levando a automatização de postos de trabalho a um aumento de desigualdades económicas, de insegurança profissional e de pobreza.

O banco Morgan Stanley está a usar IA para substituir o trabalho dos seus advogados, tendo poupado mais de 10 milhões de dólares em honorários em 2021. E outros bancos, como Goldman Sachs e JP Morgan começam a lhes seguir as pisadas, procurando automatizar os seus processos.

A Amazon seguiu o exemplo de outras empresas, e está a automatizar o processo de recrutamento de novos empregados, estando também a dispensar centenas de recrutadores.

E a Altice indica que está já a desenvolver com um cliente uma solução de fábrica, suportada pela rede 5G, que permite aumentar a eficiência fabril. "Esta solução vem garantir uma tomada de decisão mais fácil, dando a conhecer a performance do processo produtivo, ajudando a simular novos cenários de produção com uma réplica 3D do chão de fábrica e facilitando o treino virtual dos colaboradores. Sendo o 5G uma rede mais robusta, vai permitir que toda a informação recolhida seja transmitida, processada e integrada em tempo real num gémeo digital, dotando a fábrica de uma operação verdadeiramente inteligente", refere.

A maior agência de seguros e resseguros do mundo, a Swiss Re, avalia esse risco e afirma que "a implantação da IA [Inteligência Artificial] terá um impacto significativo no conhecimento e empresas de capital humano, transformando os empregados numa força de trabalho 'melhorada'. Isto poderá levar a um aumento do desemprego, inicialmente nas profissões menos exigentes, e desencadear agitação social."

O investigador de Inteligência Artificial Luís Moniz Pereira da Universidade Nova avisou que "qualquer empresa, qualquer programador pode desenvolver ferramentas que podem causar danos muito grandes", salientando que o mundo também não está atento ao impacto social, quando grandes fatias de trabalho forem entregues a instrumentos de IA.

"Há uma falta de previsão em relação a consequências [da IA] e estou a pensar especificamente em consequências sobre o desemprego e o subemprego", observou o diretor do Centro de Inteligência Artificial na Universidade Nova de Lisboa e autor do livro Máquinas Éticas.

Os "governantes e outras entidades dizem: acabam uns empregos, mas criam-se outros, mas isso não está estudado" e "não está a ser feito um estudo sobre quais são [as consequências], em que quantidade e com que probabilidade", salientou.

No futuro próximo, "esse monopólio [das tarefas cognitivas] vai ser substituído por máquinas" e, mesmo que as pessoas tenham formação, o número de novos empregos será inferior aos que forem extintos.

A ideia de um processo empresarial mais rápido e eficiente, que não descansa nem necessita de ser pago um salário, nem subsidiado, que não tem direitos laborais e faz o trabalho de vários empregados é um sonho para empresários. Mas não para os empregados que precisam do seu salário...

Mas esta adoção desenfreada de Inteligência Artificial pelas empresas nos seus processos tem provocado na maioria dos casos dissabor ou indiferença ao nível da experiência laboral. Segundo um estudo do Massachusetts Institute of Technology (MIT) de 2025, apenas 5% dos projetos piloto empresariais sobre IA atingiu um rendimento assinalável. Com 95% a falharem.

Ainda assim a isto se junta o ritmo da investigação e da comercialização de ferramentas de Inteligência Artificial crescer ao passo da ganância e da voracidade humanas. O caso da

voz de Scarlett Johansson e a empresa OpenAI é um exemplo disto, onde, perante a recusa da atriz de ceder a sua voz para ser usada pelo ChatGPT, a empresa adicionou uma voz bastante semelhante à dela e se terá recusado a fornecer informações sobre o processo que levou ao caso.

Surgiu entretanto a agência de talentos de Inteligência Artificial inglesa Xicoia que apresentou uma atriz digital, criada com IA, que apelidou da nova Scarlett Johansson, chamada Tilly Norwood. Esta empresa especializa-se na criação de atores digitais.

Foi feita uma demonstração da capacidade de Tilly Norwood no Festival Cinematográfico de Zurich, onde clipes foram apresentados. O que suscitou o interesse de várias agências de talentos na empresa Xicoia.

Este desenvolvimento levou muitos atores e sindicatos da indústria cinematográfica a censurar o projeto da *start-up* inglesa, sugerindo que atores criados com IA representam um perigo existencial aos atores humanos e para o cinema.

A "filosofia da nossa época, o que interessa, é ganhar mais dinheiro, mais negócio, ganhar o mais possível e é a ganância" e a IA vai permitir o surgimento de novos protagonistas, com um impacto social grande, considerou Luís Moniz Pereira.

Por outro lado, disse, há muitos países que não têm ferramentas desenvolvidas e podemos assistir a "um novo colonialismo de informática e, especificamente, de Inteligência Artificial", com a redução de línguas locais ou idiomas menos falados.

"Eu temo que possa haver tragédias", por falta de regulação, avisou, salientando que o crescimento está a ser exponencial e os governos não estão atentos ao problema, nem preparados para lidar com ele.

Na Europa, foi já aprovada o pacote de regulamentação para o setor, mas esta legislação só tem efeito daqui a dois anos, o que o investigador entende ser um problema, a que se soma ausência de mecanismos de controlo.

Além disso, "quem é que vai monitorar a aplicação da legislação?" -- questionou, salientando que entregar essa responsabilidade a mecanismos privados poderá ser um problema.

Já o filósofo Günther Anders (12 de julho de 1902 – 17 de dezembro de 1992), na caracterização da segunda e terceira revoluções industriais, assistindo ao florescimento da robótica, genética, informática, telecomunicações e eletrónica, assinalava e preconizava com alarme a contínua limitação e perda de significado do ser humano em contexto laboral e social, provocados pelo avanço tecnologia e a mecanização dos processos de trabalho, que tornavam progressivamente o ser humano obsoleto e redundante. A tecnologia começava a limitar de forma evidente a contribuição do homem no processo de trabalho, a diminuir a abrangência da sua função e a desvalorizá-lo, pondo-o efetivamente, de uma forma natural, ao serviço do instrumento da destruição da sua vida e do seu papel social. Mesmo

mentalmente - Anders assinalava -, com a circunscrição do trabalho humano a tarefas menos abrangentes, mais repetitivas, menos significativas, a capacidade de pensar e a imaginação do ser humano sofreram um empobrecimento, pela sua redução a uma peça na máquina de produção industrial, que condiciona a apatia, e torna a sua vida mais isolada, e também mais vulnerável, em um mundo crescentemente adaptado para máquinas.

E as pessoas tenderão cada vez mais a ter sobre si próprias, e os outros, expectativas irrealistas de perfeccionismo, como se de máquina especializadas se tratassem, desumanizando os outros e a si próprias.

Valdemar Setzer, professor do departamento de Ciência da Computação da Universidade de São Paulo, no Brasil, preocupa-se com uma perda de mão de obra. “Os robôs deveriam substituir o trabalho humano apenas em duas condições: na medida em que o trabalho degrada o ser humano e na medida em que se dê um trabalho mais digno para a pessoa substituída”, avalia. Para ele, há risco de as pessoas tratarem cada vez mais colegas como máquinas.

Kate Darling, pesquisadora do Massachusetts Institute of Technology (MIT) especialista nas relações humanas, afirma que “a automação pode até ter substituído os humanos em algumas áreas, mas a tecnologia atual ainda não é suficiente para o trabalho totalmente sem humanos.”

Mas a tecnologia aproxima-se cada vez mais desse ideal empresarial: de um mundo (laboral) feito especialmente para máquinas e de uma força laboral exígua.

Assim como haverá uma especialização e uma diversificação cada vez maior das tecnologias e das profissões que operarão sobre as máquinas, assim como uma exigência crescente de capacidade de trabalho e uma precarização das condições de trabalho.

E o que está na voga atualmente é a chamada *gig economy* da Uber, Cabify, Lyft. Estas empresas fazem parte de um mercado que move milhares de milhões por todo o mundo. Só nos Estados Unidos estima-se que valha mais de 5 milhares de milhões de dólares. E em 2025 mais de 540 milhões de pessoas a nível mundial deverão procurar trabalho por estas plataformas online.

Existe muita excitação sobre esta nova forma de trabalho e a procura de a adaptar às outras áreas laborais.

Isto no entanto não impede que os trabalhadores destas empresas sejam empregados como “parceiros”, recebendo uma verba potencial variável pelo seu trabalho regulada pela empresa, e sem os direitos do normal trabalhador, como seguro de trabalho, subsídio de férias e de parentalidade, ou sequer respeito. O que conduz a um tipo de trabalho precário pouco regulamentado, roçando a ilegalidade. Por esta razão e a lisura em geral em termos legais que este mercado tem, estas empresas fazem competição desleal e estão a destruir os tipos de serviço a que vêm oferecer uma alternativa, como o do táxi.

Isto contrasta com a situação interna intrigante com que estas empresas operam. A Uber e outras empresas declaram prejuízo, mas trabalham com milhares de milhões de euros e pagam milhões aos seus gestores executivos.

Uma realidade que também é importante salientar na operação destas plataformas online é que apesar de parecer que funcionam de forma mágica por Inteligência Artificial, a verdade é que empregam mão de obra humana que é remetida para o anonimato e muitas vezes em condições também ela de exploração e precariedade. Por vezes subcontratada de serviços como o Amazon Mechanical Turk, da Amazon cujo presidente executivo é o indivíduo mais rico do mundo, Jeff Bezos.

Este estado de coisas no sector tecnológico salienta uma verdade profunda, normalmente incompreendida e de contornos trágicos: a realidade abstrata (do digital) não é a mesma da realidade física, material. Um indivíduo no mundo real pode-se reduzir a uma variável num programa de computador, e este programa pode criar, manipular e eliminar múltiplas destas variáveis sem grande trabalho ou consequência, mas no mundo real estas variáveis são vidas humanas. Esta abstração, própria da tecnologia, conduz a uma progressiva desumanização dos seres humanos, reduzidos a aspetos que lhe são atribuídos.

O que será das pessoas?

Ou se adaptarão ou ficarão para trás. E mesmo aquelas que se adaptem, têm de competir por oportunidades que vão progressivamente escasseando e se tornando previsivelmente mais precárias.

Como disse Einstein, “Tornou-se perturbadoramente aparente que a nossa tecnologia superou a nossa humanidade.”

13 - Uma síntese da história da tecnologia 5G

O termo Internet das Coisas surgiu nos anos 90, numa apresentação de Kevin Ashton à empresa multinacional Procter & Gamble, onde a procurava convencer a usar tecnologia RFID.

Nos princípios de 2000, investigadores chegaram à conclusão que a tecnologia 3G e 4G não chegaria para suportar redes de milhares de milhões de aparelhos interconectados pelo mundo fora. A tecnologia 4G era demasiado lenta para comunicação em tempo real.

Em abril de 2008, a NASA fez uma parceria com Geoff Brown e Machine-to-Machine Intelligence (M2Mi) Corp para desenvolver a quinta geração de telecomunicações, embora focada em comunicação com nanosatélites²¹.

21 - satélites artificiais com peso e massa muito reduzidos

Também em 2008, o programa sul-coreano de investigação e desenvolvimento de 5G móvel foi formado.

A partir daqui, ao longo dos anos, diferentes entidades públicas e privadas se associaram à investigação sobre a quinta geração de telecomunicações: a Universidade Nova Iorque, a Universidade de Surrey, Huawei, Samsung, Telefonica Europe, Fujitsu Laboratories Europe, Rohde & Schwarz, Aircom International, a União Europeia (e os projetos METIS e iJOIN), Samsung Electronics, Índia, Israel, Nippon Telegraph and Telephone, Qualcomm, entre outros.

Também há que falar do envolvimento íntimo na elaboração de standards de segurança associados à tecnologia 5G por parte do FBI, do GCHQ²² britânico e outras agências de espionagem e organizações policiais, que estão a pressionar no sentido que seja facilitada a coleção da informação dos consumidores, na utilização do 5G, tanto quanto possível tecnicamente.

Em 2012, o Radiocommunication Bureau da International Telecommunication Union²³ criou o conceito de IMT-2020, para desenvolver a sua visão para as telecomunicações móveis internacionais para 2020 e além. O desenvolvimento das tecnologias 3G e 4G foi de acordo com IMT-2000 and IMT-Advanced, respectivamente.

“O *standard* IMT-2020 está determinado para ser a rede de comunicação global para as próximas décadas e está em linha para estar implementado até 2020”, segundo François Rancy, director do Radiocommunication Bureau. “O próximo passo é um consenso no que serão as especificações detalhadas para IMT-2020, o paradigma que alicerçará as próxima gerações de banda móvel e conectividade IoT”.

Na comunicação de 6 de maio de 2015 do Parlamento Europeu, que estabelece uma Estratégia para o Mercado Único Digital para a Europa, a Comissão sustentou que a revisão do quadro regulamentar das telecomunicações incidiria sobre as medidas que visam promover o investimento nas redes de banda larga de elevado débito, que adotam uma abordagem mais coerente à escala do mercado interno no respeitante à política e à gestão do espectro de radiofrequências, que criam condições para a realização de um verdadeiro mercado interno, abordando a questão da fragmentação regulamentar, que garantem uma defesa dos consumidores eficaz, condições de concorrência equitativas para todos os intervenientes no mercado e a aplicação coerente das regras, além de estabelecer um quadro regulamentar institucional mais eficaz.

Em 2015, a organização 3GPP²⁴ começou a trabalhar na geração seguinte de tecnologia celular, ou 5G, com o objetivo de submeter uma tecnologia candidata ao processo associado ao IMT-2020.

22 - GCHQ é a sigla representativa da agência de inteligência britânica Government Communications Headquarters.

23 - a agência especializada das Nações Unidas para tecnologias de informação e comunicação

24 - 3GPP (3rd Generation Partnership Project) é a designação dada à colaborações de um conjunto de organizações responsáveis pelo desenvolvimento e manutenção de tecnologias de telecomunicações móveis e standards associados, incluindo 5G.

Na World Radio Conference de 2015, o foco principal esteve em procurar encontrar maior largura de banda para serviços de 4G, começando-se já a preparar para a necessidade de espectro associada ao 5G.

Em 14 de setembro de 2016, a Comissão Europeia lançou a iniciativa “5G Action Plan”, como forma de acelerar a instalação de 5G na União Europeia. Esta medida não-legislativa apresenta um calendário europeu comum para o desenvolvimento de infraestruturas e serviços 5G de forma coordenada entre os estados-membros até 2020, para a colaboração entre os estados-membros e membros da indústria de telecomunicações para identificar e alocar espectro eletromagnético para o 5G, para a organização de testes da tecnologia na União Europeia em 2018, para promover standards de 5G comuns e globais, e para encorajar a elaboração e adoção a nível nacional de planos para a implementação da tecnologia 5G nos estados-membros. A Comissão Europeia estabeleceu nesta iniciativa o objetivo de, até 2020, em cada estado membro, uma cidade principal ter oferta comercial 5G. A Comissão Europeia também estabeleceu, aqui, três objetivos para 2025:

- todos os proponentes socioeconómicos, como escolas, universidades, hospitais, centros de investigação, estações, serviços públicos e empresas tecnológicas devem ter acesso a conectividade extremamente alta, na ordem de 1 Gigabit/s de ligação;
- todos os lares europeus, urbanos ou rurais, devem ter acesso a conectividade com uma capacidade de download de 100 megabit/s, que pode ser atualizada para 1 Gigabit/s;
- todas as áreas urbanas, assim como estradas e caminhos-de-ferro importantes devem ter conectividade 5G ininterrupta.

O Observatório Europeu 5G formado pela Comissão Europeia, em 2018, informa sobre o avanço destes objetivos, e de outros objetivos estabelecidos posteriormente pela União Europeia, assim como sobre o avanço da tecnologia 5G em outros grandes mercados, como o americano, o chinês, o japonês e o sul-coreano.

Em 1 de junho de 2017, o Parlamento Europeu aprovou a resolução “Internet connectivity for growth, competitiveness and cohesion: European gigabit society and 5G”. Esta elogia a estratégia da Comissão Europeia e apoia os objetivos, por ela, propostos. Urgindo à elaboração de um cronograma explícito sobre a instalação da tecnologia 5G e uma estratégia de financiamento do 5G ambiciosa, incluindo fundos europeus. Assim como apela a um ambiente regulatório favorável ao investimento, favorecendo a competição justa, uma estratégia sobre o espectro europeu coerente, com uma melhoria da coordenação na alocação das bandas eletromagnéticas, e exige a aceleração dos esforços europeus de standardização sobre a tecnologia 5G.

Em fins de 2017 ocorreu a entrega inicial de especificações para 5G NR NSA (Non-Stand-Alone, ou, em português, dependente das tecnologias de telecomunicações prévias [4G e 3G]), pela 3GPP, evoluindo o trabalho na direção da criação de um conjunto completo de standards para a tecnologia 5G (incluindo 5G NR SA [Stand-Alone]) subsequentemente. Isto permitiu aos vendedores de chips progredir rapidamente com o desenho de componentes e implementações iniciais de redes 5G em 2019.

Em 1 de março de 2018, um acordo sobre o espectro destinado ao 5G foi atingido a nível da União Europeia, entre o Parlamento Europeu e equipas de negociação do Conselho Europeu. A 14 de novembro de 2018 o Parlamento Europeu aprovou o acordo em plenário e o Conselho Europeu adotou o Electronic Communications Code em 4 de dezembro de 2018.

No texto da diretiva da União Europeia 2018/1972 do Parlamento Europeu e do Conselho de 11 de dezembro de 2018 que estabelece o Código Europeu das Comunicações Eletrónicas pode-se ler:

“A convergência dos setores das telecomunicações, dos meios de comunicação social e das tecnologias da informação implica que todas as redes e todos os serviços de comunicações eletrónicas deverão ser, na medida do possível, regidos por um único código europeu das comunicações eletrónicas, estabelecido por meio de uma única diretiva, com exceção das matérias que possam ser melhor tratadas por via de regras diretamente aplicáveis, estabelecidas por meio de regulamentos.”

Na União Europeia, a 12 de março de 2019 o Parlamento Europeu aprovou em plenário uma resolução pedindo ação a nível da União Europeia sobre riscos à segurança ligados à crescente presença tecnológica da China dentro da união. Nela, membros do Parlamento Europeu pedem à Comissão e aos estados-membros para providenciar orientação em como lidar com riscos informáticos e vulnerabilidades quando procurando equipamento 5G e estabelecer uma estratégia para reduzir a dependência da Europa em tecnologia de cibersegurança estrangeira. Adicionalmente, a resolução pede à Comissão para incumbir a ENISA (Agência de Cibersegurança da União Europeia) de trabalhar num esquema de certificação assegurando que a instalação de 5G na União Europeia atinge os padrões de segurança mais elevados.

Na World Radio Conference de 2019, de 28 de outubro a 22 de novembro, chegou-se à conclusão que seria necessário significativamente mais espectro eletromagnético para o serviço 5G. Para isso poder-se-ia diminuir o tamanho da área de operação das antenas, mas ainda assim seria necessário espectro adicional. Capacidade adicional foi identificada para possível uso nas bandas 24.25-27.5 GHz, 37-43.5 GHz, 45.5-47 GHz, 47.2-48.2 e 66-71 GHz. Este espectro adicional viria a ser referenciado como 5G mmWave ou high-band (5G ultrarrápido). Também o espectro alocado para o 5G deveria ser consensual a nível global, de forma a facilitar o desenvolvimento tecnológico.

Para diminuir os riscos de interferência maliciosa nas instalações de 5G e nas aplicações web na União Europeia, a Comissão publicou, a 29 de janeiro de 2020, a Toolbox (“caixa de ferramentas”) 5G – um conjunto de medidas de mitigação dos riscos associados à tecnologia 5G trabalhado por instâncias nacionais e supranacionais (Grupo de Cooperação NIS e Agência de Cibersegurança Europeia) - respeitante à gestão desta tecnologia pelos países da União Europeia, em resposta às exortações do Conselho Europeu a uma abordagem conjunta na segurança das redes 5G, e seguindo as recomendações da própria comissão. A sua implementação é responsabilidade dos países sob a visão atenta da Comissão Europeia.

Em 3 de julho de 2020 foram oficialmente declaradas como terminadas as especificações para todo um sistema inicial de telecomunicações 5G, pela organização 3GPP (responsável pelo seu desenvolvimento). Sendo que trabalho continua a ser realizado em diversos campos ligados à tecnologia 5G, incluindo gasto e eficiência energéticos, comunicação com veículos, cidades inteligentes, incorporação de Inteligência Artificial e Machine Learning, posicionamento de terminais e localização, segurança, streaming. Também continuam a ser investigadas melhorias e inovações no funcionamento de telecomunicações em FR1 e FR2.

Em outubro de 2020, o Conselho Europeu pediu à Comissão Europeia para apoiar a aceleração da instalação de infraestruturas de rede seguras de muita alta capacidade, tais como de 5G, por toda a União Europeia.

No início de 2021, a Comissão Europeia publicou uma comunicação sobre as “Orientações para a Digitalização até 2030: a via europeia para a Década Digital”, na qual era dado um grande destaque ao papel da rede de quinta geração (o 5G). Foi estipulado que todos os lares deveriam ter conectividade de 1 Gigabit, e todas as áreas populadas deveriam ter cobertura 5G até 2030, entre outros objetivos para a conectividade.

A 3 de fevereiro de 2021 a Comissão Europeia pediu à ENISA para preparar um esquema de certificação sobre cibersegurança da União Europeia para redes 5G.

A 25 de março de 2021, os estados-membros, em cooperação próxima com a Comissão Europeia, chegaram a um acordo sobre a Connectivity Toolbox. A Connectivity Toolbox consiste em um conjunto de práticas que são consideradas como as mais eficientes a permitir e encorajar operadoras de telecomunicações a instalar redes de muita alta capacidade e 5G.

Em junho de 2021, 25 dos 27 países da União Europeia já tinham disponíveis serviços comerciais de 5G. Os únicos dois países que não tinha eram Portugal e Lituânia. Note-se que, no caso da Lituânia, os atrasos no desenvolvimento da rede 5G deveram-se às dúvidas suscitadas pelo parlamento nacional sobre a segurança das infraestruturas desenvolvidas pela Huawei, sendo certo que, entretanto, já foram instaladas em 2021 e encontram-se em operação mais de uma dezena de estações que suportam a tecnologia 5G.

A 17 de dezembro de 2021, a União Europeia pôs em funcionamento o primeiro programa de larga escala intitulado “6G Research and Innovation Work Programme”, com um financiamento público de 240 milhões de euros, para financiar investigação e testagem dos sistemas 5G e 6G, incluindo com indústrias verticais.

13.1 - A implantação da tecnologia 5G em Portugal

A tecnologia 5G, segundo o então Secretário de Estado para a Transição Digital, André de Aragão Azevedo, “está muito mais vocacionada para determinados setores específicos, para vias de comunicação, para infraestruturas críticas, onde aí, sim, a rapidez da

comunicação, os grandes volumes de dados, são de facto muito relevantes do ponto de vista do impacto e transformação dos negócios”, salientou.

Também por isto a Altice pressionou a ANACOM para acelerar o plano de implementação do 5G, advertindo a possibilidade de Portugal ficar atrasado em relação ao resto da Europa na adoção da tecnologia.

A ANACOM anunciou a 23 de outubro de 2019 que iria realizar um leilão - "recorde" a nível europeu na quantidade de faixa eletromagnética leiloado - para atribuir faixas eletromagnéticas para o funcionamento dos serviços comerciais de 5G em 2020, de abril a junho. O valor inicial do conjunto dos lotes de banda eletromagnética em leilão iria ser de 237,9 milhões de euros. Onde em vez dos normais blocos de 20 MHz de banda, iria procurar vender conjuntos de 10 MHz, com o fundamento de permitir que surjam mais serviços comerciais de 5G, localizados nas faixas de 700 MHz, 900 MHz, 1.8 GHz, 2.16 GHz, 2.6 GHz e 3.6 GHz.

Neste leilão virtual, as empresas de telecomunicações foram aconselhadas pelo regulador, ANACOM, a partilhar o investimento, de forma a ficar mais barato, levantando questões sobre se o preço das faixas iria aumentar. Perante isto, representantes das operadoras Altice, NOS e Vodafone afirmaram que não admitiam pagar, em conjunto, mais do que 100 milhões de euros. E a ANACOM via com bons olhos a entrada de novos operadores no sector das telecomunicações em Portugal - uma sugestão que desagradou às empresas de telecomunicações já implantadas no mercado nacional.

A estas verbas é acrescido uma renda anual paga pelas operadoras de telecomunicações ao Estado. As operadoras afirmaram estar dispostas a pagar 48 milhões de euro anualmente pelo aluguer das frequências móveis.

As operadoras, especialmente em Portugal, dão os primeiros passos na nova geração de rede móvel num formato non-standalone. Ou seja, este primeiro 5G, apesar de reduzir a latência nas comunicações — isto é, o tempo que a informação leva a chegar ao destino —, será um 5G assente na atual rede 4G, ainda com núcleo (core) de quarta geração, e não um “5G puro”, com rádios e um núcleo 5G.

Isto aconteceu numa altura em que, noutros países, as frequências altas dos 26 GHz já foram atribuídas a empresas e o 5G mmWave já começava a ser desenvolvido. A ANACOM não escondia isso, mas recordava que, na União Europeia, apenas a Itália tinha atribuído espetro na faixa dos 26 GHz até à altura do anúncio do leilão.

Assim, é certo que, nesta primeira fase, Portugal, como a maioria dos países que implementa a tecnologia, terá inicialmente um serviço de 5G limitado, que servirá de transição do 4G para a total oferta de serviços de telecomunicações esperados do 5G.

Há que acrescentar que esta etapa na implementação do 5G em Portugal serviu também para a ANACOM incentivar a expansão da rede 4G, nomeadamente às escolas e à linha ferroviária do norte do país.

Haviam as metas de até dezembro de 2020 em Portugal “pelo menos uma cidade situada em territórios de baixa densidade” (existem no país 165 municípios que cabem nesta definição) e “uma cidade do litoral, com mais de 50 mil habitantes” estarem cobertas com rede 5G. Sendo que os centros de saúde, universidades e PME (pequenas e médias empresas) também podiam pedir cobertura específica de 5G.

Até 2023 as metas no regulamento definido pela Anacom e a Estratégia Nacional para o 5G, estabelecida pelo governo, decretavam que os operadores, no âmbito do 5G, tinham de garantir uma "cobertura de 75 % da população de cada uma das freguesias consideradas de baixa densidade e de cada uma das freguesias das Regiões Autónomas da Madeira e dos Açores".

Um ano depois tinha de estar assegurada a "cobertura de 70% da população de cada uma das freguesias que não são consideradas de baixa densidade, mas que integram municípios com freguesias de baixa densidade".

Até 2025, tinha de haver uma "cobertura de 95% da população total do país", bem como uma cobertura de rede na esmagadora maioria das autoestradas nacionais, itinerários principais, itinerários ferroviários e redes de metropolitano de Lisboa, do Porto e do Sul do Tejo.

Somavam-se, ainda, obrigações para levar o 5G a centros de saúde e hospitais públicos, universidades, aeroportos, parques empresariais, além de portos e instalações militares.

Mas os objetivos até 2022 foram descartados por conta do arrastamento da crise sanitária causada pelo SARS-CoV-2 e do adiamento para 2021 do leilão de frequências para o 5G. Acresce-se também os efeitos do impacto da litigância entre operadores e ANACOM que atrasaram os procedimentos.

O leilão de frequências para o 5G arrastou-se, em parte devido às diatribes entre a ANACOM e as principais operadoras de telecomunicações nacionais, sobre a forma como ocorria e a duração do processo, acabando por encerrar a fase de licitação no dia 27 de outubro de 2021, com o Estado a embolsar cerca de 566,8 milhões de euros com o processo. Discriminadamente, a NOS foi a que investiu mais dinheiro neste leilão, num total de 165 milhões de euros, seguindo-se a Vodafone com 133 milhões, a Meo com 125,2 milhões, a Nowo com 70 milhões, a DixaRobil (ligada à Digi) com 67,3 milhões e a Dense Air com 5,7 milhões.

Dia 15 de dezembro de 2021 foi aprovado o último título DUF (Direito de Utilização de Frequências) pela ANACOM a empresas de telecomunicações que participaram no leilão, neste dia à Meo. Tendo sido emitidos os restantes títulos DUF à NOS e à Dense Air a 26 de novembro, à Vodafone a 29 de novembro, e à DixaRobil Telecom e à Nowo ambos a 30 de novembro.

A partir deste momento as operadoras de telecomunicações estão autorizadas, mediante o regulamento estipulado no leilão, a disponibilizar a sua oferta de serviços comerciais 5G.

Proximamente também deverá ganhar força a discussão em torno do lançamento do 5G ultrarrápido, que faz uso de frequências na faixa das micro-ondas de 26 GHz. A ANACOM já teve em curso uma consulta pública para aferir o interesse das operadoras, que decorreu durante o mês de janeiro de 2022.

Em fevereiro de 2022, depois de ter lançado os serviços de 5G no início de janeiro, a operadora Meo diz agora que o seu serviço comercial 5G está disponível em todas as capitais de distrito, chegando a cerca de metade da população no território nacional.

Mas com a inflação e as disrupções na cadeia de distribuição os planos do 5G em Portugal podem mudar, com operadoras como a Altice Portugal, NOS e Vodafone a prepararem-se para pedir ao Governo mais tempo para cumprirem os objetivos de cobertura, que teriam de ser cumpridos até 2025. Os problemas nas cadeias de abastecimento (como a escassez de chips), a pandemia, a inflação e a subida de preços em todas as áreas económicas levam a que quando as empresas de telecomunicações encomendam componentes e equipamentos os custos são mais elevados e demoram a chegar. A Vodafone supostamente já contactou o governo.

Por outro lado, fonte oficial da ANACOM revela que desconhece as intenções das operadoras de telecomunicações para a extensão do prazo, acrescentando que não recebeu qualquer pedido relativo a esta situação.

Em março de 2021, a UE estabeleceu um novo objetivo de alcançar a cobertura 5G em todo o espaço comunitário até 2030. Contudo, esse desígnio não foi incluindo nas metas portuguesas.

O Tribunal de Contas Europeu lembrou também que "ainda não foi transposto o Código Europeu das Comunicações Eletrónicas", uma diretiva que apoia na definição de ações e prazos para o 5G e que já deveria estar acomodada na legislação portuguesa, desde dezembro de 2020. A mesma fonte do TCE salienta que a Comissão Europeia poderá "vir a recorrer ao Tribunal Europeu de Justiça [contra Portugal]", pelo atraso.

No entanto essa transposição o Código Europeu das Comunicações Eletrónicas já está a fazer o seu percurso legal pelas instâncias políticas nacionais sobre a forma da Proposta de Lei 83/XIV/2, publicada a 2021-04-09.

13.2 – Cronologia do avanço da instalação do 5G em Portugal

A ANACOM tem a sua origem no Instituto das Comunicações de Portugal (ICP), criado em 1981, passando a instituto público com autonomia administrativa e financeira em 1989. Viu a sua designação mudada para ICP - Autoridade Nacional de Comunicações (ICP-ANACOM) em 2002. Com a nova mudança de designação e a aprovação dos estatutos atuais da ANACOM pelo Decreto-Lei n.º 39/2015, de 16 de março de 2015, e na Lei das

Comunicações Eletrónicas, passou a caber à instituição «assegurar a gestão eficiente do espectro radioelétrico, envolvendo a planificação, a atribuição dos recursos espectrais, a sua supervisão e a coordenação entre as radiocomunicações civis, militares e paramilitares». O atual presidente, João Cadete de Matos, foi empossado em 2017.

Em 2 de abril de 2019, por comunicado de imprensa, a NOS anunciou ter-se juntado ao projeto de Matosinhos como primeira Zona Livre Tecnológica (ZLT) em Portugal, numa parceria com a CeiiA (Centro de Engenharia e Desenvolvimento). Será neste concelho da área metropolitana do Porto que serão testadas as soluções, pioneiras a nível nacional, incluindo para a tecnologia 5G.

Em junho de 2019, a NOS demonstrou com uma simulação, em ambiente real, em Matosinhos, as potencialidades da quinta geração de comunicações móveis, aplicada à vigilância de praia e zonas costeiras, através da transmissão de vídeo de alta definição 4K 360°. A demonstração realizou-se com a colaboração do CeiiA.

Em 11 de outubro de 2019, Aveiro também avançou para a adoção da tecnologia 5G, lançando a iniciativa Aveiro 5G Challenges, em parceria com a Altice Labs, com o objetivo de premiar monetariamente novas soluções e produtos sustentados tecnologicamente pela tecnologia 5G. No laboratório vivo da cidade de Aveiro, statups, scaleups e centros de I&D puderam desenvolver e escalar comercialmente as suas soluções, através de acompanhamento técnico e de sessões de mentoria. Houve duas edições deste projeto conjunto.

A Altice pressionou a ANACOM para acelerar o plano de legalização do 5G em Portugal, advertindo a possibilidade de Portugal ficar atrasado em relação ao resto da Europa na adoção da tecnologia.

A ANACOM anunciou a 23 de outubro de 2019 que iria realizar um leilão - "recorde" a nível europeu na quantidade de faixa eletromagnética leiloado - para atribuir faixas eletromagnéticas para o funcionamento dos serviços comerciais de 5G em 2020, de abril a junho. O valor inicial do conjunto dos lotes de banda eletromagnética em leilão iria ser de 237,9 milhões de euros. Onde em vez dos normais blocos de 20 MHz de banda, iria procurar vender conjuntos de 10 MHz, com o fundamento de permitir que surjam mais serviços comerciais de 5G, localizados nas faixas de 700 MHz, 900 MHz, 1.8 GHz, 2.16 GHz, 2.6 GHz e 3.6 GHz.

Neste leilão virtual, as empresas de telecomunicações foram aconselhadas pelo regulador, ANACOM, a partilhar o investimento, de forma a ficar mais barato, levantando questões sobre se o preço das faixas iria aumentar. Perante isto, representantes das operadoras Altice, NOS e Vodafone afirmaram que não admitiam pagar, em conjunto, mais do que 100 milhões de euros. E a ANACOM via com bons olhos a entrada de novos operadores no sector das telecomunicações em Portugal - uma sugestão que desagradou às empresas de telecomunicações já implantadas no mercado nacional.

A estas verbas é acrescido uma renda anual paga pelas operadoras de telecomunicações ao Estado. As operadoras afirmaram estar dispostas a pagar 48 milhões de euro anualmente pelas frequências móveis.

Também em 23 de outubro de 2019, também por comunicado de imprensa, a NOS anunciou ter coberto totalmente a cidade de Matosinhos com a quinta geração de comunicações móveis, em parceria com a Huawei. A rede 5G da NOS estava integralmente operacional e disponível, em regime de piloto, à autarquia, empresas e polos de investigação, para o desenvolvimento de *use cases* alavancados nesta tecnologia.

Ao dotar a cidade de Matosinhos com uma rede 5G, a NOS posicionou-se na linha da frente na implementação desta nova tecnologia e assumiu um papel de liderança na inovação associada às cidades inteligentes e ao desenvolvimento do novo paradigma de sociedade.

Esta infraestrutura inicial 5G de Matosinhos era composta por uma rede com cerca de 20 estações rádio que cobriam integralmente a cidade de Matosinhos, bem como a totalidade da Zona Livre Tecnológica compreendida entre o Parque da Cidade do Porto, o Porto de Leixões, a Freguesia de Sr^a da Hora e a zona comercial do NorteShopping.

A rede 5G da NOS utilizou espectro solicitado à ANACOM para efeitos de ensaio, na banda dos 3,5 GHz, acessível a todos os cidadãos através de terminais 5G.

Já em fevereiro de 2020, o partido PAN (Pessoas-Animais-Natureza) apresentou uma recomendação pela urgente realização de uma campanha informativa sobre o 5G pelo concelho de Matosinhos, aprovada por unanimidade.

“É urgente que o executivo promova ações várias junto dos munícipes, como palestras, conferências e debates por toda a cidade, e que, de forma sucinta e compreensível, permitam o entendimento das reais diferenças e implicações da implementação da rede 5G e, sobretudo, da sobreposição das redes já existentes. Só desta forma as pessoas poderão ter uma posição devidamente informada nesta matéria”, defendeu Albano Lemos Pires, então deputado municipal do PAN.

Mas tais sessões nunca vieram a ocorrer.

Com a crise sanitária em Portugal associada ao SARS-CoV-2 (também conhecido como coronavírus e COVID-19) a consulta pública sobre o projeto de regulamento do leilão para a atribuição de direitos de utilização de frequências para a instalação de serviço comercial 5G teve o período de consulta pública estendido até 1 de abril de 2020. Posteriormente foi suspenso, e adiado até depois do estado de emergência, para uma altura em que estivessem reunidas condições para a sua realização.

Em março de 2020, o CDS-PP anunciou ter proposto à Comissão Parlamentar de Economia e Inovação a realização de uma conferência sobre o 5G e “os desafios de Portugal no futuro digital”, de acordo com o então deputado João Gonçalves Pereira. Os centristas queriam convidar “todos os ‘stakeholders’ [intervenientes] e demais interessados a dar o seu

contributo”, mas subinham que “o programa da conferência deve resultar das sugestões e consenso dos diferentes grupos parlamentares”. Gonçalves Pereira defendeu igualmente que, “para que Portugal acompanhe esta transformação inexorável, é necessário que legisladores, reguladores, cidadãos, empresas e instituições estejam devidamente esclarecidos quanto às implicações e benefícios decorrentes da implementação do 5G”.

“Tendo em conta que Portugal esteve, no passado, na vanguarda do teste e da implementação deste tipo de tecnologias, que introduziu como prioridade na sua agenda a transição e transformação digitais, e as questões levantadas por outros grupos parlamentares relativamente ao futuro do 5G, o grupo parlamentar do CDS-PP considera oportuna e necessária a promoção, pela Assembleia da República, do esclarecimento dos cidadãos, das empresas e das instituições”, salientou.

Mas esta sugestão não teve frutos.

O grupo parlamentar do PAN enviou no dia 7 de abril de 2020 ao Ministro de Estado da Economia e da Transição Digital um inquérito onde afirma que é "fundamental que, de uma forma clara e concreta, se identifiquem os principais riscos ambientais e de saúde pública decorrentes da implementação de uma rede 5G" em Portugal. No texto são endereçadas ao Governo questões sobre riscos ambientais, riscos de saúde pública e de cibersegurança, inquirindo também sobre as conclusões do grupo de trabalho criado pelo Governo para avaliar a segurança digital das redes 5G, e solicitando acesso ao relatório resultante deste trabalho. E na ausência de uma resposta objetiva e clara, o PAN enviou no final de maio novamente questões sobre estes temas para o Ministério da Saúde, o Ministério do Ambiente e Ação Climática, o Ministério das Infraestruturas e Habitação e a Presidência do Conselho de Ministros.

A Resolução do Conselho de Ministros publicada no Diário da República no dia 21 de abril de 2020, sob o título "Aprova o Plano de Ação para a Transição Digital" afirma a transição digital como "uma prioridade para Portugal", argumentando que "na atual era da quarta revolução industrial, caracterizada por exponencial digitalização da sociedade e da economia, torna-se imperativa a transição de Portugal para um país mais digital e, consequentemente, mais competitivo e mais fortalecido a nível internacional." O documento oferece uma visão sobre a globalidade da questão da digitalização afirmando a "necessidade de aproveitar o potencial transformador do digital para a promoção de uma nova era, tem-se verificado um forte investimento a nível europeu no domínio digital". Define a meta de "convergência com a Europa no domínio digital", onde “Portugal tem também percorrido a sua jornada digital, reforçada como um dos principais desígnios identificados no Programa do XXII Governo Constitucional enquanto prioridade estratégica e vetor essencial ao crescimento económico do país.” E com base nesta visão estratégica do Governo, as "novas tecnologias digitais, como os sistemas de inteligência artificial, a tecnologia 5G, a computação em nuvem e de proximidade e a Internet das Coisas, constituem-se, no seu conjunto, como um dos principais alicerces da transição energética da economia, em particular dos setores industriais estratégicos para Portugal e do seu tecido empresarial". E "para tanto, urge incentivar a adoção, por parte das empresas e do Estado de ferramentas e instrumentos mais modernos". Ainda assim avisa que "sendo a digitalização um conceito

volátil e em constante evolução, também este plano de ação deve ser um documento «vivo», alvo de inclusão de novas medidas ou atualização de medidas existentes, e que, mantendo o alinhamento com a estratégia e a visão do Governo neste domínio, reflitam o dinamismo das prioridades e preocupações da economia e da sociedade."

No dia 29 de abril de 2020, o secretário de Estado Adjunto e das Comunicações português, Alberto Souto de Miranda, declarou publicamente que voltou a haver condições para retomar o processo da implementação da tecnologia de telecomunicações 5G em Portugal, com a saída do país do estado de emergência (decretado inicialmente em 18 de março de 2020).

Em linha com a Resolução do Conselho de Ministros acima sintetizada e as afirmações do secretário de Estado das Comunicações, foi noticiado que o Governo estava a reavaliar a estratégia nacional de implementação do 5G, de forma "a adotar novas metas, mais adequadas às circunstâncias que vivemos" de crise pandémica. Passaria por um novo plano para a migração da Televisão Digital Terrestre (TDT) e por uma gestão cuidadosa da Telescola, não tendo sido adiantado na altura nenhum *timing* para o novo arranque do processo de migração da TDT, interrompido em março com a pandemia.

A migração da TDT – segundo o calendário pré-Covid da ANACOM – estava prevista terminar em finais de junho, embora a Altice, operadora que tem a concessão da rede e é responsável pela mudança dos emissores, tivesse sempre apontado para julho de 2020 a conclusão deste processo necessário para a libertação da faixa dos 700 MHz para a sua utilização pela tecnologia 5G.

Uma fonte oficial dentro do Ministério das Infraestruturas e da Habitação, onde está integrada a Secretaria de Estado das Comunicações, afirma que "a redefinição de regras [para o arranque do 5G] pode ser feita em confinamento. O próprio leilão também, já que, em circunstâncias normais, já seria digital". "É prematuro estar hoje a antecipar calendário. Essa avaliação está em curso", comunicou o Ministério, quando questionado sobre uma nova data para o arranque do processo sobre o 5G.

A ANACOM veio anunciar à imprensa que "já não estando em vigor o estado de emergência, encontrando-se o país em fase de desconfinamento, (...) entende que estão criadas as condições para retomar" o procedimento de consulta pública do projeto de regulamento do leilão para a atribuição de direitos de utilização de frequências para o 5G e outras faixas relevantes (700 MHz, 900 MHz, 1800 MHz, 2,1 GHz, 2,6 GHz e 3,6 GHz) e do procedimento de audiência prévia e de consulta pública sobre o sentido provável de decisão relativa à alteração do direito de utilização de frequências atribuído à Dense Air Portugal, e, em ambos os casos, os prazos terminariam a 3 de julho de 2020.

A ANACOM comunicou também que o leilão de frequências deveria ser um instrumento para "garantir a coesão económica e social do país, indo ao encontro das expectativas das populações e do sector económico nacional, bem como acautelar os objetivos nacionais e europeus definidos para a banda larga móvel".

“Torna-se público, nos termos e para os efeitos previstos no n.º 1 do artigo 98.º do Código do Procedimento Administrativo, que o Conselho de Administração da Autoridade Nacional de Comunicações (ANACOM), no exercício do poder regulamentar, previsto na alínea a) do n.º 2 do artigo 9.º, no artigo 10.º e na alínea b) do n.º 1 do artigo 26.º, todos dos Estatutos, aprovados pelo Decreto-Lei n.º 39/2015, de 16 de março, e das competências que lhe estão cometidas, nos termos do n.º 1 e 5 do artigo 15.º, n.º 3 do artigo 19.º, n.os 1, 3, 5, 7 e 8 do artigo 30.º e no artigo 31.º, todos da Lei n.º 5/2004, de 10 de fevereiro (Lei das Comunicações Eletrónicas - LCE), na redação atualmente em vigor, decidiu, em 31 de outubro de 2019, dar início ao procedimento de elaboração do regulamento do leilão para atribuição de direitos de utilização de frequências nas faixas dos 700 MHz, 900 MHz, 1800 MHz, 2,1 GHz, 2,6 GHz e 3,6 GHz.”

Entretanto o presidente do conselho de administração da Autoridade Nacional de Comunicações (ANACOM), João Cadete de Matos, foi à Assembleia da República no dia 9 de junho de 2020, a uma audição da comissão parlamentar de Economia, Inovação, Obras Públicas e Habitação falar sobre os planos para a quinta geração da rede móvel (5G) em Portugal, numa altura que os procedimentos suspensos desde março 2020 - por causa da pandemia de Covid-19 - foram retomados. Para os deputados estava em causa a necessidade de uma discussão parlamentar sobre o 5G, alicerce da estratégia de desenvolvimento tecnológico e económico nacionais, alinhada com diretrizes de Bruxelas e com objetivos e metas concretas para 2020. O representante da ANACOM assegurou que o leilão da quinta geração móvel (5G) iria decorrer até ao final do ano de 2020, apesar de estar com um atraso de três meses face ao calendário inicial, por causa da crise de saúde pública.

Apesar da data concreta estar então dependente da conclusão do processo de migração da televisão digital terrestre (TDT) para novos canais (que a Altice previa que se concluisse até novembro de 2020), bem como da publicação do regulamento do leilão (cujo projeto ainda estava em fase de consulta pública), o procedimento “há-de ser com certeza este ano”, afirmou na altura Cadete de Matos.

Só se “houvesse uma situação anómala” é que não aconteceria, disse o regulador, apesar de reconhecer que os operadores voltaram a dar “sinais” de que não estavam com muita pressa, porque estavam com menores capacidades para investir devido à crise económica, decorrente da pandemia.

De acordo com informações recolhidas, a instalação da rede 5G começava já a se generalizar por todo o país.

Com o SARS-CoV-2 surgiu pressão à digitalização apressada das relações interpessoais e do trabalho, com os incentivos ao distanciamento social e isolamento, passando, na dimensão do possível, de forma progressiva para a esfera do virtual. E com uma crise económica em desenvolvimento, assim como uma crise energética e de cadeias logísticas, de contínuo impacto na economia portuguesa, europeia e mundial, era de esperar que os decisores políticos e sociais, portugueses e internacionais, dessem significativamente maior primazia a preocupações de cariz económico e financeiro - o economicismo -, deixando para segundo

plano questões de saúde e ecologia, continuando a acelerar a digitalização da economia e a implementação dos serviços comerciais de 5G.

A própria ANACOM declarou, por comunicado de imprensa, que "a implementação do 5G afigura-se determinante para mitigar as deficiências ao nível das coberturas e das capacidades disponibilizadas pelas redes móveis existentes e garantir a coesão económica e social do país, indo ao encontro das expectativas das populações e do sector económico nacional, bem como acautelar os objetivos nacionais e europeus definidos para a banda larga móvel".

Mas isto estava em direta contradição com as declarações proferidas na altura pelo anterior presidente da Altice Portugal (detentora da empresa MEO), Alexandre Fonseca, que afirmou que o período de confinamento - com os portugueses a conseguirem passar a trabalhar remotamente pela Internet sem falhas significativas a registar, nem no 4G, nem na fibra ótica - veio mostrar que "as redes actuais ainda estão em linha" com as necessidades e expectativas dos consumidores e empresas, e por isso é necessário olhar "com prudência" para os investimentos que estão associados à quinta geração móvel (5G). E asseverou que era preciso introduzir "equilíbrio" e "racionalidade" na equação do 5G. Reiterando que ainda havia potencial por explorar nas redes 4G.

Alexandre Fonseca também assumiu que a nova geração de rede móvel era importante para permitir, "a médio prazo", aplicações que não eram possíveis então. Mas não seria tão importante para os consumidores em geral, uma vez que ainda nem sequer tinha sido esgotada a largura de banda do 4G.

Alexandre Fonseca admitiu também que embora a Altice fizesse serviço público, não era uma empresa pública: "Temos de ser realistas: não temos obrigação contratual. É investimento 100% privado. É um investimento nosso, de empresa privada, que se destina a alargar as nossas redes, há investimentos que, por muito que queiramos fazer, não podemos, porque não teremos retorno".

A empresa Ericsson, segundo o seu líder de serviços digitais - Nuno Roso - dizia que do ponto de vista tecnológico estava tudo preparado para lançar a 5G no mercado português: "Estamos preparados para avançar com implementação do 5G amanhã se for necessário".

A consulta pública do projeto de regulamento do leilão para a atribuição de direitos de utilização de frequências para o 5G e outras faixas relevantes recebeu cerca de 500 contributos até ao seu término, no qual participaram organismos governamentais, os dois Governos regionais, reguladores, instituições públicas, autarquias locais, prestadores de serviços de comunicações eletrónicas, fabricantes e o público em geral.

E, como previsto, a ANACOM procedeu à atualização do calendário indicativo para a realização do leilão, vindo anunciar que o leilão se iniciaria em outubro de 2020 e encerraria em dezembro do mesmo ano. Isto significaria que a conclusão dos procedimentos de direitos de utilização de frequências (DUF) só aconteceria em janeiro ou fevereiro de 2021, atrasando a entrada em funcionamento da tecnologia 5G para 2021.

"Uma visão ponderada sobre o 5G e tecnologias relacionadas", texto de Miguel Vilhena



António Costa Silva, consultor do Governo, apresentou na reunião do Conselho de Ministros um trabalho intitulado Plano de Recuperação Económica e Social de Portugal, defendendo a utilização da rede 5G para reforçar a coesão territorial e evitar que o país viva “a várias velocidades”. Costa Silva acrescentou, além disso, que a transição digital é “um dos instrumentos essenciais de estratégia de desenvolvimento do país”, salientando que é preciso “fazer muito mais” na introdução das tecnologias digitais nos processos produtivos e modelos organizacionais.

“As novas tecnologias digitais, como os sistemas de inteligência artificial, a tecnologia 5G, a computação em nuvem e de proximidade e a Internet das coisas, constituem, em conjunto, um dos principais alicerces da transição energética da economia, em particular dos setores industriais estratégicos para Portugal e do seu tecido empresarial. Como tal, a transição digital deve ser assumida como catalisador da transformação industrial em curso”. Isto é declarado no Plano de Recuperação Económica e Social.

De acordo com o relatório da Public First encomendado pela Google, anunciado em 2023, a IA generativa (capaz de gerar texto, imagens e vídeo) “poderá aumentar a dimensão da economia portuguesa em 15.000 milhões de euros (ou o equivalente a 8% do Valor Acrescentado Bruto ou 6% do Produto Interno Bruto) e poupar, em média, mais de 80 horas por ano a cada trabalhador – o equivalente a duas semanas de trabalho”.

E como pôr em prática essa transição digital e, consequentemente, a transformação industrial e social? Costa Silva destacava a importância de alargar a todo o país a fibra ótica — é um “projeto estruturante para o futuro de Portugal”, disse — e de apostar na rede 5G.

“Um elemento propulsor desta transformação é o alargamento da fibra ótica para cobrir todo o país, o que é muito importante para não termos um país a várias velocidades, ao mesmo tempo que reforça a coesão territorial e a integração do interior na economia nacional e global, promovendo plataformas digitais para vender produtos, bens e serviços online. O outro elemento propulsor, e estratégico para o futuro, é a utilização da nova geração de tecnologias móveis, a rede 5G, para alavancar a conectividade do país, inserindo-o nas redes globais”, lê-se no documento que foi apresentado ao Executivo de António Costa.

Costa Silva arrematava dizendo: “É importante o país reforçar e consolidar todas as infraestruturas tecnológicas e digitais, aumentar o poder das redes, e reforçar as tecnologias de informação e comunicação e as competências de gestão”.

Também Samuel Ferreira, 5G Solutions Architect da Huawei Portugal, não tinha dúvidas de que a quinta geração da rede móvel “é de facto importante e que será uma mais valia para aumentar a competitividade das empresas”, no contexto de transformação e transição digital que Portugal e o mundo atravessam.

António Martins da Costa, então presidente da Câmara de Comércio Americana em Portuga, foi um dos promotores, com a Accenture, da conferência “5G, Cibersegurança e Transformação Digital”, onde afirmou que “no contexto de grande transformação digital que o Mundo vive nos últimos anos, já verificámos relativamente a outras tecnologias que ser ‘early adopter’ pode trazer vantagens competitivas importantes.”

As operadoras de telecomunicações seguiam também aumentando a instalação nacional de fibra ótica, e estabelecendo parcerias, nomeadamente com a Huawei Portugal, com universidades em domínios como o Big Data e Analíticas, Ciência dos Dados, Inteligência Artificial e Sistemas Cognitivos, e com instituições de saúde, com a oferta de material informático.

O então Secretário de Estado Adjunto e das Comunicações, Alberto Souto de Miranda, em julho de 2020, revelou ao Parlamento que o projeto do leilão do 5G da ANACOM não estava alinhado com a estratégia do Governo, numa audição da comissão de Economia, Inovação, Obras Públicas e Habitação, a pedido do Bloco de Esquerda. Perante um cenário de uma maior desarticulação, o Secretário indicou que o Governo “terá de avaliar a situação”, tendo em vista a adoção de medidas com “outra força legislativa”, caso contrário, havia o “risco de os procedimentos serem anulados”.

“A situação não é nada tranquilizadora”, explicou Alberto Souto de Miranda. O Secretário afirmou que, embora o país já tivesse atrasos antes da pandemia de COVID-19, o mesmo não se passava em matéria de tecnologia. “Estamos bem preparados para o 5G”, indicou acrescentando que o que era necessário era alcançar consenso no projeto de leilão, e que “não está excluída a hipótese de fazer uma reavaliação de todo o processo”.

Alberto Souto de Miranda esperava que João Cadete de Matos, presidente da ANACOM, revisse o projeto. Questionado sobre se o processo do 5G não iria avançar, assim, nos moldes propostos pela ANACOM, o governante foi assertivo: “Do ponto de vista do governo não. Como é evidente, um regulador tem que cumprir as leis do país. E o que se espera de uma entidade responsável é que adapte o regulamento no sentido de tornar o mesmo congruente com a resolução do Conselho de Ministros”, defendeu.

Souto de Miranda deixou ainda o aviso: “Não me passa pela cabeça que a ANACOM não venha a adaptar o regulamento ao que foi aprovado. Seria uma violação grave. Espero que a ANACOM reflita nisto que acabei de dizer. Era bom que cada um entendesse o seu papel”.

E as críticas não ficaram por aqui. O responsável aproveitou para dizer que "o governo é que define a política de comunicações. Não é a ANACOM. Isto é clarinho como a água, e se não é claro para todas as pessoas deveria ser".

Sendo que estas declarações acabam por contextualizar as críticas feitas às entidades reguladoras na economia portuguesa - entre elas à ANACOM - na reportagem da Rádio Renascença, produzida com o apoio da Fundação Gulbenkian, intitulada "Os polícias dos mercados" com o subtítulo "Das portas giratórias às contas desfalcadas", apontando que "as entidades reguladoras em Portugal são independentes só de nome". "De que a lei lhes promete autonomia financeira, mas o ministro das Finanças cativa-lhes milhões de euros por ano e o Governo é livre de nomear e exonerar os seus dirigentes". Acusando-os na globalidade de "promiscuidade e os conflitos de interesses" que "continuam a ser uma realidade no setor financeiro".

Em relação ao tema da Huawei e da cibersegurança, o secretário de estado Souto de Miranda falou sobre a criação de um sistema de certificação de equipamentos concebido para verificar a legitimidade da tecnologia, assim como a implementação de avaliações contínuas, com auditorias às tecnologias instaladas.

O secretário de estado enfatizou ainda a diversificação de fornecedores, lembrando que "é um tema muito importante", uma vez que "que há países que estão numa linha mais dura, talvez por força das relações privilegiadas" que têm com outras nações.

E com toda esta verborreia de preocupações e considerações económicas e industriais, com a pressão sobre a ANACOM para se alinhar com os interesses do governo, nem uma palavra para os temas da saúde das populações, ou da ecologia, no território português ou para o desemprego perspetivado decorrente do impulso dado à automatização das indústrias.

A Autoridade da Concorrência, na figura da sua presidente, Margarida Matos Rosa, afirmou o desejo de agitar o "status quo" do setor das telecomunicações. Há, no entender da presidente da AdC, que garantir que o leilão permita "realmente" a entrada de novos operadores no mercado das operadoras.

O projeto de alteração do Regulamento do Leilão foi aprovado em 31 de maio de 2021, e esteve em consulta por um período de 5 dias úteis, o qual terminou no dia 9 de junho. A alteração ao regulamento do leilão foi publicada no Diário da República, no dia 30 de junho, vigorando as alterações introduzidas desde o dia 5 de julho.

A alteração do regulamento do leilão visou aumentar o número diário de rondas da fase de licitação principal. Esta alteração permitiria imprimir maior celeridade ao leilão, sem afetar as estratégias dos licitantes, tornando viável a realização de 12 rondas diárias de licitação.

A Altice e a NOS criticaram veementemente a alteração dos moldes do leilão ainda a decorrer, e a Vodafone ameaçou seguir para tribunal, para parar a mudança. Descreveram a mudança do regulamento como antiético e amador, e como péssimo para o país.

A partir de 27 de setembro, quando entraram em vigor as novas regras, os valores monetários oferecidos por dia aumentaram mais de 4 milhões, chegando mesmo a superar os 5 milhões de aumento diário.

O primeiro ministro português - António Costa – em 20 outubro de 2021 lançou um ataque sem precedentes à ANACOM pela perpetuação do leilão no tempo, dizendo que “o modelo de leilão que a ANACOM inventou é, obviamente, o pior modelo de leilão possível, nunca mais termina e está a provocar um atraso imenso no desenvolvimento do 5G em Portugal”.

O chefe do Governo foi ainda mais longe, criticando o atual modelo de regulação do setor das comunicações: “Quem construiu essa doutrina absolutamente extraordinária de que é preciso limitar os poderes dos governos para dar poder às entidades reguladoras, deve bem refletir sobre este exemplo do leilão do 5G, para ver se é este o bom modelo de governação económica do futuro”.

Depois do primeiro-ministro criticar a ANACOM, os valores diários subiram mais de 6 milhões. As licitações mínimas são determinadas pelas operadoras. São eles que ao longo do leilão vão formando os preços.

O leilão de frequências para o 5G arrastou-se apesar das diatribes entre a ANACOM e as principais operadoras de telecomunicações, sobre a forma como ocorria e a duração do processo, acabando por encerrar a fase de licitação no dia 27 de outubro de 2021, com o Estado a embolsar cerca de 566,8 milhões de euros com o processo. Discriminadamente, a NOS foi a que investiu mais dinheiro neste leilão, num total de 165 milhões de euros, seguindo-se a Vodafone com 133 milhões, a Meo com 125,2 milhões, a Nowo com 70 milhões, a DixaRobil (ligada à Digi) com 67,3 milhões e a Dense Air com 5,7 milhões.

O Ministério das Infraestruturas comunicou que “será agora necessário que a ANACOM conclua o processo, nos termos do regulamento, o qual culminará com a atribuição dos direitos de utilização aos licitantes”, ficando os operadores, depois disso, “sujeitos ao cumprimento das obrigações estabelecidas no regulamento do leilão, designadamente obrigações de cobertura”.

Dia 15 de dezembro de 2021 foi aprovado o último título DUF (Direito de Utilização de Frequências) pela ANACOM a empresas de telecomunicações que participaram no leilão, neste dia, à Meo. Tendo sido emitidos os restantes títulos DUF à NOS e à Dense Air a 26 de novembro, à Vodafone a 29 de novembro, e à DixaRobil Telecom e à Nowo ambos a 30 de novembro.

A partir deste momento as operadoras de telecomunicações estão autorizadas, mediante o regulamento estipulado no leilão, a disponibilizar a sua oferta de serviços comerciais 5G.

Proximamente também deverá ganhar força a discussão em torno do lançamento do 5G ultrarrápido, que faz uso de frequências muito elevadas na faixa dos 26 GHz. A ANACOM já

teve em curso uma consulta pública para aferir o interesse das operadoras de telecomunicações, que decorreu durante o mês de janeiro de 2022.

“A ANACOM decidiu auscultar o mercado para aferir do interesse na disponibilização de espetro na faixa dos 26 GHz, uma das que integra o conjunto de faixas pioneiras/prioritárias para o desenvolvimento do 5G”, indicou a ANACOM numa nota. Em concreto, a dos 26 GHz, “por ter uma cobertura geográfica mais reduzida que as restantes faixas de frequências, mas uma muito mais elevada capacidade de transmissão de dados, pode vir a ser utilizada em pontos específicos e localizados”, explica o regulador.

Quando fez a consulta pública antes do primeiro leilão do 5G, a ANACOM notou o “interesse relevante do mercado nesta faixa, numa perspetiva de implementação futura do 5G”. No entanto, esse interesse não era “acompanhado por uma perspetiva definida sobre a utilidade a curto prazo desta faixa e do modo como esta devia ser disponibilizada pelo regulador”.

Um possível leilão da faixa dos 26 GHz só deverá acontecer depois de 2024.

Em fevereiro de 2022, depois de ter lançado os serviços de 5G no início de janeiro, a operadora Meo disse que o seu serviço comercial 5G estava disponível em todas as capitais de distrito, chegando a cerca de metade da população no território nacional.

Mas com a inflação e as disrupções na cadeia de distribuição de componentes, os planos da instalação de 5G em Portugal podem mudar, com operadoras como a Altice Portugal, NOS e Vodafone a prepararem-se para pedir ao Governo mais tempo para cumprirem os objetivos de cobertura, que teriam de ser cumpridos até 2025. Os problemas nas cadeias de abastecimento (como a escassez de chips), a pandemia, a inflação e a subida de preços em todas as áreas económicas levam a que quando as empresas de telecomunicações encomendam componentes e equipamentos, os custos são mais elevados e demoram a chegar. A Vodafone supostamente já contactou o governo.

Por outro lado, fonte oficial da ANACOM revelou que desconhecia as intenções das operadoras de telecomunicações para a extensão do prazo, acrescentando que não recebeu qualquer pedido relativo a esta situação.

Em março de 2021, a União Europeia estabeleceu um novo objetivo de alcançar a cobertura 5G em todo o espaço comunitário até 2030. Contudo, esse desígnio não foi incluindo nas metas públicas portuguesas. O Tribunal de Contas Europeu observou mesmo que apenas metade dos 27 estados-membros incluiu o novo objetivo nas estratégias nacionais para o 5G.

O Tribunal de Contas Europeu lembrou também que "ainda não foi transposto o Código Europeu das Comunicações Eletrónicas", uma diretiva que apoia na definição de ações e prazos para o 5G e que já deveria estar acomodada na legislação portuguesa, desde dezembro de 2020. Neste ponto, Portugal não é caso único - há 23 países que ainda não adotaram a diretiva, o que levou o auditor a afirmar que, "ao atual ritmo de execução, é muito provável

que os objetivos da UE para a atual década não sejam atingidos", no que respeita às telecomunicações.

Quanto ao atraso de Portugal nesta transposição, a mesma fonte do TCE salientou que a Comissão Europeia poderia "vir a recorrer ao Tribunal Europeu de Justiça [contra Portugal]".

No entanto essa transposição do Código Europeu das Comunicações Eletrónicas já está a fazer o seu percurso legal pelas instâncias políticas nacionais portuguesas, sobre a forma da Proposta de Lei 83/XIV/2, publicada a 2021-04-09.

Porquê tanta pressa, ansiedade e secretismo sobre a implementação da tecnologia 5G?

14 - A questão do lixo tecnológico

Também é importante falar da quantidade de lixo tecnológico.

O relatório das Nações Unidas sobre lixo tecnológico conclui que a quantidade deste tipo de detrito tem vindo a aumentar - a maioria dele, por indivíduo, proveniente na Europa -, com 53.6 milhões de toneladas produzidas em 2019 a nível mundial, das quais 82% não foi reciclado, tendo sido queimado ou depositado. Sendo importante notar que este tipo de lixo liberta gases nocivos incluindo CO₂, e substâncias tóxicas para os solos, incluindo mercúrio, o que causa perigos ambientais e de saúde pública, especialmente em áreas urbanas tecnologicamente evoluídas e densamente povoadas, como Matosinhos, Porto ou Lisboa.

Em média cada homem, mulher e criança à volta do mundo produziu 7.3 Kg de lixo tecnológico em 2019. E até países com um sistema de gestão de resíduos tecnológicos apresentam resultados relativamente modestos de recolha e reciclagem deste tipo de lixo.

O subsecretário geral das Nações Unidas David M. Malone, sobre isto, declarou que "Substancialmente maiores esforços são urgentemente necessários para garantir mais inteligente e mais sustentável produção, consumo, e descarte de equipamentos elétricos e eletrónicos. Este relatório contribui fortemente para o sentido de urgência em inverter este perigoso padrão global."

E este tipo de problema só terá tendência a aumentar com uma nova geração de telecomunicações (5G) mais exigente tecnicamente, fazendo uso de diferentes tecnologias, e mais densificada, com a Internet das Coisas e as cidades inteligentes. Isto tendo em conta os modelos de obsolescência planeada praticados pelas empresas do ramo das indústrias tecnológicas e de substituição precoce aplicados pelas empresas de telecomunicações.

Este relatório das Nações Unidas aponta para uma previsão de crescimento do despejo de aparelhos para 74 milhões de toneladas métricas em 2030, acreditando que será alimentado este ritmo por maior consumo de artigos elétricos e eletrónicos, ciclos de vida mais curtos e

opções de reparação limitadas. E isto, se nada for feito em contrário, estimulará o progressivo esgotamento de recursos e novas vagas de poluição diretas (sob a forma de resíduos) e indiretas (da extração de matérias primas e produção industrial).

E com o Sars-CoV-2 este problema agravou-se, com as pessoas em isolamento em casa, desfazendo-se de seus utensílios e a fazer compras, e com menos pessoas a recolher e a reciclar o lixo.

Enquanto os danos causado ao ambiente pela deposição deste tipo de resíduos são incalculáveis, o relatório da UN avisa que: “A forma na qual produzimos, consumimos e nos desfazemos estes resíduos tecnológicos é insustentável.”

Muita da invasão tecnologicamente recente das nossas vidas tem sido sustentada pelo mito de que é sinónima com emancipação e progresso, mas que está em oposição às realidades do aumento das desigualdades sociais, da destruição da natureza e do desperdício de recursos naturais que tem promovido, fazendo perigar de facto o planeta, a civilização, as nações, e as nossas próprias vidas.

Mais recentemente, as iniciativas a nível da União Europeia sobre a obrigatoriedade de todo o equipamento eletrónico como smartphones, tablets, máquinas fotográficas e consolas vendidos na UE incluírem uma porta USB-C até ao Outono de 2024, assim como o “direito a reparar”, que, apesar de parecerem muito próximas no calendário legislativo europeu, ainda não estão aprovadas pelo Parlamento Europeu nem pelo Conselho Europeu, prometem ajudar a reduzir a quantidade de lixo eletrónico no futuro, ao encontro dos objetivos europeus de economia circular e neutralidade carbónica para 2050.

E estes efeitos da política da União Europeia podem bem se estender para lá dos estados-membros, pelo “Efeito de Bruxelas”. Este é o nome dado, pela professora de direito da Universidade de Columbia, nos Estados Unidos, Anu Bradford, ao fenómeno da influência legislativa da União Europeia na política mundial. Onde nos Estados Unidos tem havido movimento no sentido generalizar o direito a reparar produtos eletrónicos, no Reino Unido foi já passado a lei, e também na Índia está a avançar semelhante medida legislativa.

E a Austrália tem “cafés de reparação” gratuitos, onde técnicos se voluntariam para partilhar conhecimentos de graça.

Mas, ainda assim, isto é muito pouco para reduzir a produção e a quantidade de lixo eletrónico a nível mundial.

15 - Conclusões

Nas palavras da doutora Fiorella Belpoggi, do Instituto Ramazzini, de Bolonha, "O que eu não entendo é que, por exemplo, a indústria química tem de demonstrar a segurança de um

composto antes de o pôr no mercado, mas a indústria da tecnologia não uma exigência idêntica, e disseminam os seus produtos sem qualquer estudo do seu impacto na saúde pública." Sobre a discrepância, a investigadora confessa que "o valor económico da indústria de telecomunicações atualmente é enorme." E conclui dizendo que "eu não posso afirmar que as ondas milimétricas são perigosas, mas ninguém pode afirmar que elas não o são."

Também no relatório de 2016, a EUROPAEM afirma que “novas tecnologias sem fios e aplicações têm sido introduzidas sem qualquer certeza sobre os seus efeitos na saúde, levantando novos desafios para a medicina e para a sociedade”.

Mas não há vontade de precisar os efeitos na saúde das radiações micro-ondas ou aceitar resultados comprometedores, em especial das usadas nas telecomunicações móveis, incluindo na tecnologia 5G, até porque conclusões científicas irrefutáveis sobre os efeitos nocivos tornariam as empresas de telecomunicações vulneráveis a litigação, e impactariam adversamente os mercados de telecomunicações e financeiros.

Isto é tão mais preocupante quando “o 5G alterará não só o paradigma global das interações interpessoais, mas também as interações com máquinas e inter-máquinas, amplificados pelo crescimento do IoT e das tecnologias de processamento de borda. Ao tornar as interações em tempo real uma realidade acessível e disponível, abrirá caminho a que a prestação de serviços remotos seja global, feita em larga escala e dê origem à criação e proliferação de novos serviços globais e relações pessoais e empresariais hoje impensáveis ou impraticáveis. Neste contexto, os volumes de dados gerados por estas interações possibilitarão novos níveis de sofisticação de Inteligência Artificial, pelo que os graus de automatismo e autossuficiência de equipamentos, estruturas e organizações (ex: indústria, logística) serão fortemente alavancados. O crescimento exponencial destas interações, dados e automatismos em tempo real abrirá um novo universo de oportunidades, porquanto esbaterá algumas das fronteiras e limitações hoje existentes no comércio global. Trará também uma concorrência mais global, digital e eficiente.”, de acordo com António Martins da Costa, presidente da Câmara de Comércio Americana em Portugal.

Pelo seu reconhecido tremendo potencial, não deveria a sua implementação ser mais prudente e gradual a nível global?

Porquê esta pressa em implementá-la em tempo recorde sem grandes estudos nem precauções?

Porque não esperar por estudos e consenso científicos suficientes sobre os efeitos das radiações eletromagnéticas para desenhar a tecnologia do 5G e a instalação da mesma, de forma minimizar os efeitos na saúde e no ambiente desta tecnologia?

Será agora, numa altura de investimentos na ordem dos biliões de euros na tecnologia 5G, com lucros previsto na ordem dos triliões, com múltiplas tecnologias em desenvolvimento para lucrar financeiramente com o 5G, com quase uma década de investigação e planeamento do 5G, com a credibilidade e as carreiras de muita gente pelo menos em parte associada à progressão da tecnologia, que irá haver vontade na comunidade

científica, nos governos e na indústria das telecomunicações de descortinar realmente os efeitos das radiações eletromagnéticas no ambiente e seres vivos?

Havendo no entanto a certeza que a falta de estudo dos efeitos das tecnologias a implementar, e já implementadas, ajudarão ao crescimento de doenças e mortes inexplicáveis, pela ausência de conhecimento ou segurança científica.

Tudo isto discutido aqui, com a pouca definição e profundidade oferecidas pela informação pública sobre a tecnologia 5G, e a pressa de a implementar, traz pouco esclarecimento, receio, aversão e polarização ao assunto, tornando este um campo fértil para todo o tipo de especulações e posições sobre esta tecnologia.

Isto devia tornar necessário haver pelo menos testes independentes sobre o 5G e as tecnologias associadas, que fossem capazes de esclarecer a discussão que rodeia este assunto, e nos mostrar de facto, cientificamente, as necessidades à sua operação e consequências associadas, e informar os decisores políticos, que estão fortemente balanceados em favor da implementação massiva desta tecnologia.

16 - Apelo à consciência

Com a consciência de que todo o trabalho tem uma dimensão política, pela forma como se enquadra na sociedade, apelo à consciência de todas as pessoas, em especial às que se perfilam para fazer parte da nova revolução tecnológica que se avizinha, para refletir sobre o que querem para a sociedade, sobre o seu trabalho, e sobre o que estão preparados a investir de si para que essa visão aconteça. Porque cada pessoa tem as suas ideias, e quem age, age pelos seus interesses pessoais, e não devemos esperar que outros implementem a nossa visão para a realidade.

Assim, devemos agir, não por medo, mas por consciência, e com isto apoiar as recomendações de 250 cientistas e médicos que assinaram o 5G Appeal, que invoca uma moratória imediata na instalação de 5G, e exigem financiamento governamental para a investigação necessária a encontrar limites seguros de exposição, e advogar - como já aconteceu em Bruxelas (Bélgica), Florença e Roma (Itália), Genebra, Vaud, Jura e Neuchâtel (Suíça), Totnes, Hove, Glastonbury, Frome e Shepton Mallet (Reino Unido), na Holanda e na Rússia²⁵ - um período de moratória sobre a introdução da tecnologia de telecomunicações 5G, até que os riscos associados sejam determinados por investigação científica independente, e possam ser ponderados conscientemente por comissões independentes especializadas na área, para a decisão de adoção, ou não, da tecnologia 5G, como vai sendo proposta e implementada à revelia de considerações de segurança pública. E não apenas vendo ser tratado este assunto meramente do ponto de vista económico, financeiro e político, com a decisão dependente de

25 - Um número crescente de cidades está a parar a implementação da tecnologia 5G. Para uma lista atualizada das cidades que estão a suspender a instalação do 5G vá a https://electromogportugal.weebly.com/uploads/1/2/3/3/123313372/lista_de_cidades_e_paises_que_baniram_o_5g.pdf

burocratas sem formação no campo das radiações eletromagnéticas e profissionais ligados às empresas envolvidas economicamente na exploração do 5G e essas empresas.

Na Suíça foi mesmo banida a instalação da tecnologia 5G em 2020, com a exigência de estudos sobre os efeitos de saúde da tecnologia 5G. Até produzidos esses estudos, a proibição não será levantada. Isto vem na sequência do parecer da agência ambiental suíça, de nome Bafu, assumindo incapacidade de criar uma regulação adequada para a tecnologia 5G sem mais testes sobre o impacto da radiação associada à tecnologia, e de uma declaração pública da Associação Médica Suíça avisando precaução sobre o 5G, argumentando no sentido de que os mais exigentes princípios legais fossem aplicados, em função de questões não esclarecidas sobre o potencial da tecnologia 5G para causar danos no sistema nervoso, e mesmo cânceros.

Bafu revelou mesmo que não estava ao corrente de nenhum standard internacional que pudesse ser usado para testar recomendações sobre a tecnologia 5G.

Sem um critério definido, os cantões têm poucas opções, para lá de licenciar infraestruturas 5G de acordo com as guias existentes sobre exposição a radiação, que precedem o uso do 5G exceto numa minoria dos casos.

Vários cantões impuseram entretanto a sua própria moratória por causa de incerteza sobre riscos de saúde.

Entretanto a Swisscom avisou que o processo de avaliação da agência Bafu não pararia a instalação da infraestrutura 5G, mesmo que significasse que não poderia ser usada na sua capacidade total.

Em face de controvérsia sobre a forma diversa como eram aprovadas as instalações de antenas celulares nos diferentes cantões suíços, algumas delas com um escrutínio quase inexistente, a partir de 2021 cada antena deverá passar por um processo adequado de licença de construção, em discussão pelos cantões que deverá também envolver o governo federal e as operadoras de telecomunicações móveis. A questão central é como a nova tecnologia 5G deve ser avaliada, segundo Stephan Attiger, presidente da Conferência Suíça de Diretores de Construção, Planeamento e Meio Ambiente: “A questão chave é quando uma mudança é significativa e quando é insignificante.»

Em junho de 2022, pela primeira vez foi revelado um relatório federal suíço sobre a exposição de antenas de telemóveis e transmissores de rádio. Foi observado que radiação não-ionizante sobrecarrega a população apenas ligeiramente. No entanto, são necessárias mais medições.

A expansão da rede móvel 5G é polarizadora na Suíça: segundo uma pesquisa, 42,5% da população apoia a rápida expansão proposta pelo Conselho Federal. 41,7% dos entrevistados são contra. O governo federal já criou uma plataforma de informação. Estão envolvidos a Secretaria Federal de Meio Ambiente (FOEN), a Secretaria Federal de Comunicações (OFCOM) e a Secretaria Federal de Saúde Pública (BAG).

Devemos dar voz e poder a especialistas creditados e a investigação independente credível na área, como a realizada pela BioInitiative 2012, que advoga padrões legais de exposição a radiação eletromagnética de baixa intensidade baseados em estudos de exposição biológica pública.

E com este objetivo devemos procurar sensibilizar, e tornar as pessoas conscientes sobre o 5G, e criar pressão civil sobre as autoridades que regulamentam o mercado das telecomunicações de forma a incutir uma atitude esclarecida, razoável, prudente e saudável em relação a tecnologias experimentais. Porque mais que uma grandíssima oportunidade de negócio e especulação financeira, é o futuro, a saúde, a segurança, o bem estar de todos, e o ambiente, que estão em jogo.

A tecnologia tem a capacidade de manifestar o pior na civilização: cobiça, ganância, imprudência, doença, medo, raiva, incivilidade, crise de confiança, solidão, alienação, polarização, fraude, populismo, violência, caos, distração e maior incapacidade de focar nos problemas reais. E isto afeta toda a gente dentro da sociedade tecnológica, caso esteja diretamente exposta à tecnologia ou não. E isto traz o perigo existencial de uma erosão completa dos pilares da sociedade e da própria civilização moderna.

Nas palavras de Justin Rosenstein, programador de software e empresário americano que trabalhou na Google e no Facebook, e foi publicado na revista Time:

“Enquanto a nossa economia funcionar dessa forma e empresas continuam não-reguladas, elas vão continuar a destruir árvores, a matar baleias, a minerar a Terra, e a continuar a tirar petróleo do chão, mesmo que saibamos que está a destruir o planeta e nós sabemos que irá deixar um mundo pior para futuras gerações.

Este é pensamento a curto-prazo, baseado nesta religião de lucro a todo o custo, como se de alguma forma, magicamente, cada empresa agindo nos seus interesses egoístas irá produzir o melhor resultado.

Isto tem afetado o ambiente por muito tempo.

O que é assustador, e esperemos seja a gota de água que nos irá acordar como civilização a quão errada esta teoria tem sido desde o princípio, é que nós agora somos as árvores, nós somos as baleias. A nossa atenção pode ser extraída. Nós somos mais lucrativos a uma empresa se nós gastarmos tempo fixados num ecrã, vendo um anúncio, que se nós gastarmos esse tempo vivendo a nossa vida de uma forma rica.

E assim nós estamos a ver os resultados disso. Nós vemos empresas usando inteligência artificial poderosa para nos compreender e descobrir como puxar a nossa atenção de encontro às coisas que eles querem que vejamos, em vez das coisas que são mais consistentes com os nossos objetivos, os nossos valores e as nossas vidas.”

Que mundo estamos a criar com o uso ignorante, desregulado, compulsivo e imprudente de tecnologias provavelmente tóxicas, invasivas, desumanas e evidentemente viciantes?

17 - Anexos

17.1 - Reflexão sobre a adequação do princípio da precaução

Como o filósofo francês contemporâneo Jean-Pierre Dupuy dissertou na sua tese, de 2005, intitulada “The Precautionary Principle and Enlightened Doomsaying: Rational Choice before the Apocalypse”, não podemos confiar no Princípio da Precaução para nos proteger, porque este foi desenhado para falhar, ou para previsivelmente ajudar a conduzir-nos à situação de desastre.

Na Declaração de Rio de Janeiro, decorrente da Conferência das Nações Unidas Sobre o Meio Ambiente e Desenvolvimento de 1992, o princípio da precaução é definido para a política internacional nestes moldes (na tradução para o português):

“De modo a proteger o meio ambiente, o princípio da precaução deve ser amplamente observado pelos Estados, de acordo com as suas capacidades. Quando houver ameaça de danos sérios ou irreversíveis, a ausência de absoluta certeza científica não deve ser utilizada como razão para postergar medidas eficazes e economicamente viáveis para prevenir a degradação ambiental.”

Este princípio está dependente, como mencionado acima, do enquadramento económica, e procura avaliar racionalmente riscos e fatores desconhecidos, estando fundamentada a precaução numa ambiguidade textual claramente aberta ao abuso, que não impede a continuação do modo de prevenção que existia anteriormente à introdução do princípio da precaução: ação reativa em resposta a desastres.

Um exemplo disto foi a suspensão da administração da vacina da farmacêutica AstraZeneca com base no “princípio de precaução em saúde pública”, em Portugal, em 2021, ocorrido depois de novos casos de efeitos secundários graves associados à toma desta vacina em Portugal, em linha com o previamente reportado, à altura, em vários outros países europeus.

O princípio da precaução não previne desastres, ou catástrofes, apenas permite mitigá-los, porque se estabelece como uma ferramenta subordinada a uma balança de custo-benefício de interesses públicos e privados, onde nada parece pesar o suficiente para prevenir, de facto, o desastre.

É preciso mais que o princípio da precaução. É preciso uma verdadeira mudança de vontades e prioridades em respeito à tecnologia, à nossa saúde e ao ambiente: uma visão consequencialista da ação humana. Neste caso respeitante à tecnologia dos campos eletromagnéticos, das telecomunicações e dos aparelhos relacionados. Que responsabilize entidades e pessoas pelas consequências dos seus atos, intencionais ou não, desde que previstas e não evitadas, com isto dando um peso mais significativo às possíveis consequências em decisões de interesse público.

17.2 - 5G e o Covid

Embora não seja um tema diretamente relacionado com a tecnologia 5G, estão a ser frequentemente associados o SARS-CoV-2 e a tecnologia 5G. Fazendo uso do raciocínio torna-se fácil refutar a ligação direta entre a doença e a nova tecnologia de telecomunicações, visto estar a ser noticiada a doença um pouco por todo o mundo, incluindo Portugal, que ainda não tem o serviço instalado e ativo.

Mas estes rumores e teorias espalham tão fácil e rapidamente porque há razões para isso.

Existe pouca clareza e muitas incógnitas à volta do SARS-CoV-2, sobre as suas origens, sobre o seu comportamento, sobre a sua propagação, a validade dos métodos de combate à doença e a informação veiculada sobre o tema. O que não é ajudado pela falta de transparência, lapsos e desinformação espalhada até por fontes governamentais e organizações internacionais, incluindo da área da saúde. Gerando isto previsivelmente desconfiança e paranóia.

Mas também, como este documento indica, existem também muitas dúvidas, deduções, informações contraditórias, ofuscação, desinformação, falta de vontade de lidar com e fuga ao assunto dos efeitos das radiações eletromagnéticas na saúde e no ambiente, em especial as associadas à tecnologia de telecomunicações móveis, por parte das autoridades de saúde e de ligadas à área, e até dos políticos. Existe um incómodo palpável ao lidar com o assunto, porque é um assunto técnico e complexo, e atualmente não oferece conclusões definitivas. E não havendo nenhuma autoridade reconhecida que perentoriamente afirme que não há efeitos da tecnologia associada ao 5G na saúde.

Em 2019, o grupo de jornalistas Investigate Europe entrevistou dezenas de cientistas especializados nos efeitos dos campos electro-magnéticos, e todas as autoridades internacionais relevantes. A conclusão deste trabalho é alarmante: falta muita informação, que deveria ser considerada antes de se avançar para esta revolução tecnológica.

A própria Agência Europeia do Ambiente (AEA) há muito que defende a precaução relativamente à exposição aos campos eletromagnéticos, assinalando que houve casos de não utilização do princípio da precaução no passado, que resultaram em danos muitas vezes irreversíveis para a saúde humana e para o ambiente. As acções adequadas, cautelares e proporcionadas tomadas agora para evitar ameaças plausíveis e potencialmente graves à saúde por parte dos CEM (campos eletromagnéticos) são susceptíveis de serem vistas como mais prudentes e sensatas de perspectivas futuras.

E o próprio Gabinete das Nações Unidas para a Redução de Riscos de Catástrofes declarou sobre o Covid-19, no seu relatório de apreciação global de 26 de abril de 2022, que “exposição a factores de risco (...) foram determinados como afetando significativamente taxas de mortalidade.”

Com tudo o que foi explorado neste documento não se assume como irrazoável considerar que a exposição a campos eletromagnéticos e à tecnologia 5G pode fragilizar o organismo, e o sistema imunitário, e torná-lo mais suscetível a doenças, assumindo um papel pernicioso durante a epidemia.

E também houve um artigo em 2020 que ligava a tecnologia 5G, células da pele e o SARS-CoV-2, que foi prontamente censurado e repudiado. O artigo defende a tese de que as ondas milimétricas do 5G no FR2 (Frequency Range 2) podiam ser absorvidas pelas células da pele atuando como antenas, e transmitidas para o interior do corpo, e causar a produção de coronavírus dentro de células. Este artigo assenta em parte, na tese defendida por outro artigo incluído neste documento, que discute a possibilidade de a radiação micro-ondas milimétrica poder ser absorvida pelos canais de suor atuando como antenas, e transmitindo essa radiação ao interior do corpo.

Perante tudo isto, o medo, a insegurança, a impotência, a fúria e o recurso à violência podem surgir em um encadeamento fácil e espontâneo, que já levou à destruição de material de telecomunicações, como antenas, e mesmo ao assédio a trabalhadores de operadoras de telecomunicações no estrangeiro. Mas isto não se justifica. É normal o medo e a procura de afastar esse medo, mas não devemos nos deixar levar pelo pânico e o fácil, que pode levar a desfechos que não se desejam quando se decide mais racionalmente, assim como oferecer argumentos oportunos aos interesses contrários aos nossos para, de forma inválida, apoucar as nossas preocupações (e a nós próprios), as censurarem e ignorarem.

Assim, individualmente, os melhores recursos perante os possíveis efeitos das radiações eletromagnéticas são a calma, a prudência, a vigilância e o rigor. Devemos fazer uso do nosso juízo crítico e autonomia quando sentimos realmente um efeito nocivo sobre a nossa saúde e comportamento. Devemos despistar a possibilidade do efeito nocebo e a possível histeria. Devemos tomar nota dos efeitos identificados, da sua evolução e do seu comportamento perante diferentes exposições. E se se confirmar no nosso entendimento a nossa hipótese inicial, devemos chamar a atenção pública para o tema, procurar se organizar com outros e agir positivamente (e não de forma destrutiva). Contactar os autoridades civis locais, associações de defesa da saúde e do ambiente, como a MOPPE, no caso das radiações eletromagnéticas, a Autoridade de Saúde Nacional, o Conselho de Autoridades de Saúde, a Ordem dos Médicos e ordens profissionais de saúde, o Conselho Nacional de Saúde Pública, a Direção Geral de Saúde, a ANACOM, o Ministério da Saúde, os partidos políticos, os representantes no parlamento português, o Presidente da República, e o Primeiro Ministro.

E não devemos esquecer a resposta dada por estes organismos e indivíduos às nossas preocupações e problemas, fazendo pesar sobre eles a responsabilidade social dos seus comportamentos e das situações que eles condicionaram. Devemos nos responsabilizar e responsabilizar individual e coletivamente os agentes sociais envolvidos nos problemas que enfrentamos, com efeito mais positivo ou mais negativo, com os mecanismos sociais ao nosso dispor permitidos pela Constituição Portuguesa, pela República Portuguesa e pela democracia instituída. Assim como no caso de sentimento de injustiça, pressionar a Justiça a agir.

No caso de uma agressão identificada à nossa saúde individual e coletiva, as nossas melhores armas são a racionalidade, a prudência e a ação positiva desasombradas.

17.3 - Boas práticas na navegação na Internet

Antes de partilhar alguma notícia, verificar a data, os factos, ou pelo menos ter em conta a credibilidade por nós associada à fonte de informação. A data de um artigo é muito importante em fenómenos em rápida evolução como uma pandemia, onde por vezes o que ontem era verdade, hoje poderá ser mentira.

Se um artigo de informação parecer criado para te emocionar, provavelmente é - sensacionalista.

Vota responsabilmente com os teus cliques. Procurando não perpetuar a manipulação emocional por lucro, nem a falsidade.

Procura estar exposto/a a diferentes pontos de vista, e procura refletir sobre eles e os compreender.

17.4 - Boas práticas no uso de tecnologia

Procurar fazer um uso consciente, refletido, regado e premeditado da tecnologia.

Um vício existe quando o comportamento associado é pernicioso à vida do indivíduo.

No caso de vício (comportamento habitual prejudicial à vida quotidiana) a uma tecnologia, procurar e fazer um esforço responsável para diminuir o tempo e a energia dedicada ao objeto do vício, progressivamente, sem desistir, não importa a dificuldade, nem o tempo que demore. Também é recomendado que procure um terapeuta que lide com vício, em especial com o tipo de vício que sofre.

Criar um espaço de tempo para nos concentrarmos em nós próprios e na nossa vida, sem qualquer recurso a tecnologia (desligar todas as notificações, desligar a internet, etc.).

Cultivar um distanciamento saudável à tecnologia. Por exemplo, numa saída em grupo, levar o mínimo de telemóveis necessário. Ou em um evento em grupo, guardar os telemóveis, como se guardam os casacos, e privilegiar a experiência do evento social.

Reduzir o número de notificações que recebemos nos aparelhos informáticos, às importantes para nós na medida do possível.

Retirar do quarto todos os aparelhos informáticos a uma dada hora todas as noites. Pelo menos meia hora antes do período de sono começar.

Não se deixar intimidar pelo aborrecimento. O período de aborrecimento contém um enorme potencial à invenção e à inovação (divagação mental). E são fundamentais as ações de introspeção, para processar informação, refletir, sintetizar e aprender, e devemos criar espaço para isto. Como disse Rollo May: “Tecnologia é o jeito de arranjar o mundo de tal forma que não o experimentamos.”

Criar um ambiente com intensidade luminosa constante em todo o campo visual, evitando que a luz incida diretamente no ecrã e nos olhos do utilizador, posicionar o nível superior do ecrã ao nível dos olhos (por forma a olhar para baixo), recorrer ao uso de lubrificantes oculares e fazer pausas frequentes (a regra 20-20-20 diz que em cada 20 minutos se deve fazer uma pausa de 20 segundos a olhar para uma distância de 20 pés/6 metros).

Dar um bom exemplo sobre o uso da tecnologia, apostando em uma abordagem refletida, consciente e responsável da tecnologia, procurando criar tempo de qualidade com as pessoas à nossa volta, e usar a tecnologia de uma forma ativa que complementa a nossa vida positivamente, e não reativa, como vício.

A atividade de *scrolling* (percorrer uma página a que vai sendo adicionado novos conteúdos à medida que o utilizador a percorre de cima a baixo) é exigente a nível da percepção e mental, cansando e desgastando o utilizador, para lá do grande consumo de tempo que é desenhado para condicionar. E isto deve ser tido em conta pelo utilizador na sua vida.

De acordo com a neurocientista Mary Helen Immordino-Yang, o bem-estar pessoal está ligado ao grau de agência que as pessoas sentem nas suas vidas, para fazer aquilo que lhes importa, incluindo com a tecnologia.

Nada de redes sociais até ao ensino secundário.

Discutir com sensibilidade com os filhos sobre um horário para o uso da tecnologia informática, por exemplo computadores, tablets, consolas, telemóveis (2 horas ou menos de utilização não parecem ter efeitos graves na saúde mental). E procurar cumprir e fazer cumprir o horário acordado.

Informar e discutir sobre filtros de imagem nas redes sociais (como o TikTok) - e resultados irrealistas que eles produzem - e algoritmos de apresentação de conteúdo que procuram prender a atenção do utilizador mostrando conteúdo sedutor.

Acompanhar os filhos menores no seu uso da tecnologia num papel pedagógico, compreensivo, exercendo uma boa influência, mas procurando não cair em autoritarismos, que criam clivagens, distância e segredos. Porque devemos procurar criar as condições para o pensamento crítico neles, de forma a tomarem boas decisões e serem pessoas equilibradas,

saudáveis e sensatas. Com uma figura paterna ou materna recetiva e compreensiva quando houver necessidade.

Outra excelente medida é, como defende o investigador Yuval Noah Harari, de tempos a tempos, quando a pessoa sente necessidade, realizar um jejum de informação. Onde não consumimos mais informação, apenas digerimos a informação e destoxificamos a nossa mente.

E devemos ter atenção especial à qualidade da informação que consumimos. Se nos focarmos no ódio, na ganância, no medo, teremos naturalmente mentes doentes, cujos pensamentos espelham esta informação que consumimos.

17.5 - Recomendação

Eu recomendo que não tomes a minha palavra como inquestionável, mas que faças a tua pesquisa e tires as tuas conclusões, podendo usar também as referências sugeridas abaixo.

E mantém-te informado sobre os desenvolvimentos da tecnologia 5G. Um bom ponto de partida para isso reside nestes websites:

- ◆ <https://www.pcmag.com/5g>
- ◆ <https://5gobservatory.eu/>
- ◆ <https://5gobservatory.eu/links/>
- ◆ <https://magdahavas.com/category/health-issues/>
- ◆ <https://electrosmogportugal.weebly.com/>

Embora nenhum destes websites sozinho é suficiente para acompanhar a progressão da tecnologia.

Sobre os perigos na Internet, existem estes recursos em português e para Portugal:

- ◆ <https://www.internetsegura.pt/>
- ◆ <https://www.miudossegurosna.net/>
- ◆ <https://www.seguranet.pt/>

Recomendo também que não uses o Google como motor de busca para fazer essa pesquisa. O Google viveu no passado recente um escândalo sobre vídeos que vieram a público com diretores da empresa a falarem sobre censura realizada pelo seu motor de busca de resultados de pesquisa, com vista a orientar os utilizadores de acordo com a noção ética e moral vigentes na Google, assim como a Google usa por defeito a informação que obtém da nossa navegação, incluindo no Youtube, para obter a lista de resultados que nos é apresentada. E a mesma censura pode ser observada no Youtube (website e empresa

pertencentes também à Google). Mas podemos limitar a coleção de dados e o uso que as aplicações da Google fazem dela na obtenção dos resultados que nos apresentam.

Um bom motor de busca é o DuckDuckGo (<https://duckduckgo.com/>), embora tenha declarado que passaria a censurar em 2022, nomeadamente a propaganda russa decorrente da guerra na Ucrânia. O browser do DuckDuckGo também é recomendado por mim devido à privacidade que oferece.

E o motor de busca Brave (<https://search.brave.com/>), que não faz censura e permite utilização anónima, mas que apresenta alguma limitação nos resultados apresentados.

18 – Descrição das adições de conteúdo ao documento

- 27/08/2022
 - Caso jurídico levantado à empresa Oracle nos Estados Unidos pela Irish Council for Civil Liberties, por suposta violação massiva de privacidade a nível internacional;
 - Revelações por um denunciante da inoperância e falta de ética dentro da empresa Twitter, que sugerem violações claras da privacidade dos seus utilizadores e tornam a empresa especialmente vulnerável a fugas de dados privados, hacking, manipulação e campanhas de desinformação;
 - Adição do anexo intitulado “Descrição das adições de conteúdo ao documento” a este documento, de forma a ser possível facilmente localizar nova informação.

- 15/09/22
 - Referência às propostas de lei para vigilância online de menores em vias de ser passadas a lei no estado da Califórnia, nos Estados Unidos da América;
 - Escalpelização de um artigo da Microsoft, de 2015, para vendedores, sobre a diminuição geral da atenção média da população canadiana, que apresenta ideias para explorar isto para ganho financeiro;
 - Adição do artigo e de informação sobre o recente ataque informático à TAP;
 - Adição de dois artigos sobre a evolução da lei dos metadados, que irá ser em princípio discutida no Parlamento, depois de interrompida com a pausa para férias;
 - Adição do tópico sobre o tema da utilização de técnicas de psicologia para permitir monetização antiética em videojogos, incluindo mecânica Gatcha, e de um vídeo simbólico sobre o tema, de uma apresentação de um desenvolvedor em uma convenção internacional sobre técnicas em que trabalhava para manipular jogadores;
 - Notícia sobre multa da Irlanda ao Instagram por violar a privacidade de menores;
 - Notícia sobre multas à Google e à empresa Meta por violações da privacidade na Coreia do Sul;
 - Notícia sobre a pressão das empresas Proton e DuckDuckGo sobre o congresso americano para que passe legislação anti-monopólio;

- Adição de artigo científico sobre o vício aos smartphones criar um desequilíbrio químico no cérebro;
 - Artigo sobre o império de vigilância tecnológica da Amazon, e adição de informação ao documento sobre ele.
 - Adição de informação e um artigo sobre uma app saudita, que permite reportar ações subversivas e ativistas às forças governamentais da Arábia Saudita;
 - Adição de artigo sobre a possibilidade da luz azul de smartphones e portáteis poder não afetar adversamente o sono em pequenas doses;
 - Adição de um artigo, primeiro numa série de exposições, sobre um serviço chamado Fog Reveal, que permite às forças policiais americanas aceder à localização de pessoas e aos lugares por onde passou, com dados obtidos de informação privada adquirida em apps vendidas nas lojas do Android e da Apple;
 - Artigo adicionado sobre o perigo de ferramentas de videovigilância de alunos, numa altura de ataque às liberdades pessoais à volta do mundo, incluindo a liberdade sexual e de aborto;
 - A exortação de psicólogos para as empresas de redes sociais e de serviços online para aumentarem a transparência dos seus algoritmos de forma a ajudar a prevenir e a mitigar problemas psicológicos dos usuários alimentados por estas tecnologias, e formas de diferentes tipos de agentes sociais ajudarem a minimizar a fomentação de problemas psicológicos por estes serviços.
- 25/09/22
 - A colaboração ilegal entre o Facebook e o FBI na vigia de potenciais comportamentos de insurreição de utilizadores depois da eleição presidencial americana de 2020;
 - Adição do endereço de Internet do Regulamento Geral sobre a Proteção de Dados às fontes;
 - Na União Europeia dados pessoais que podem revelar informações sensíveis sobre os cidadãos podem vir a ser considerados também como dados sensíveis, fortalecendo a privacidade sobre estas informações pessoais;
 - Investigadores afirmam que será impossível controlar Inteligência Artificial super-inteligente, à medida que supera a capacidade dos seus criadores humanos;
 - web3 tem sido usada como uma ferramenta para criar novos mercados e formas de comercialização, mas também pode ter utilizações idóneas não-comerciais;

- O governador da Califórnia, Gavin Newsom, aprovou a primeira legislação de cibersegurança de menores nas redes sociais nos Estados Unidos;
 - Adição às fontes de um vídeo sobre a criação de um mercado de exploração infantil de cariz sexual na rede social TikTok;
 - Adição às fontes de um artigo jornalístico que refere um estudo onde é afirmado que crianças estão a perder sono devido ao seu foco em notificações nos seus aparelhos eletrónicos, equiparando isto a uma noite de sono perdida por semana;
 - Adicionado às fontes um artigo sobre discos rígidos com dados sensíveis não-encryptados dos clientes da financeira multinacional Morgan Stanley terem sido leiloados online;
 - 1,5 milhões de passageiros da TAP tiveram as suas informações pessoais divulgadas na Internet, incluindo o Presidente da República, e os hackers afirmam ainda ter acesso remoto aos sistemas da companhia aérea;
 - A tentativa dos republicanos no estado americano do Texas de ditar a política de conteúdos das grandes redes sociais, procurando subtrair esse poder, e responsabilidade, das próprias empresas que gerem esses serviços;
 - As leis de retenção de dados pessoais na Alemanha, Luxemburgo e França são consideradas ilegais pelo Tribunal de Justiça Europeu, alegando que viola a legislação europeia guardar informação indiscriminadamente sobre cidadãos europeus sem justa causa;
 - Empresas do ramo dos transportes nos Estados Unidos estão a adicionar sistemas de videovigilância aos seus transportes, que lhes permite gravar conversas privadas;
 - As forças armadas americanas pagam por uma plataforma, Augury, que lhes permite acesso a 93% do tráfego de Internet mundial;
 - O exército americano mostra-se aborrecido pelo Facebook e Twitter removerem bots ligados a operações de propaganda e manipulação de massas;
 - A empresa Meta foi apanhada a vigiar páginas de hospitais nos Estados Unidos, e a compilar dados sobre consultas médicas, medicações e diagnósticos de forma secreta e ilegal.
- 28/08/22
 - Adição às fontes de uma notícia sobre uma possível multa à rede social TikTok por violar a privacidade de menores no Reino Unido;

- Adição às fontes de uma notícia sobre uma proposta de lei no estado de Nova Iorque para a proteção da privacidade online de crianças;
 - Adição da informação que a Intel e a empresa Classroom desenvolveram um software de inteligência artificial para reconhecer estados emocionais de estudantes;
 - Adição às fontes de um artigo de opinião que discute microtransações em videojogos, de uma candidata a PhD na Universidade de Princeton.
- 03/10/22
 - Adição da informação que a empresa TikTok também usa pixéis de rastreamento para coletar dados privados de forma ilegal na Internet;
 - Adição de um artigo sobre a necessidade de novos direitos humanos na tecnologia emergente Metaverso;
 - Adição da informação que o grupo de hackers ZINC, também conhecido como Lazarus, anda a infectar software legítimo de forma a atacar indivíduos e organizações específicas;
 - Adição do artigo que a indústria dos Bitcoins foi considerada, por investigadores da Universidade do Novo México, ser insustentável em termos ambientais, pela elevado consumo de eletricidade associado;
 - Facebook destrói redes de contas falsas russas e chinesas que procuravam manipular a opinião popular sobre a guerra na Ucrânia, as eleições americanas e o governo checo;
 - O governo britânico ignorou os pedidos de informação dos cidadãos sobre dados pessoais recolhidos, assim como a polícia de Kent e a empresa Virgin Media;
 - A empresa Meta foi acusada de vigiar a atividade online dos seus utilizadores com as suas plataformas Facebook, Facebook Messenger e Instagram.
 - 24/10/22
 - Adição de artigo sobre investigação científica que liga uso de redes sociais a depressão;
 - Adição de artigo sobre a divulgação do governo americano de um documento em que detalha cinco princípios que acredita que devem guiar o desenho, uso e utilização de sistemas autónomos de forma a proteger o público americano na era da Inteligência Artificial;

- Adição de informação e de um artigo jornalístico sobre a oposição à análise automática de mensagens online em busca de indícios de crime, que aponta o volume gigantesco de falsos positivos como um problema inultrapassável;
- Adição de artigo que detalha novas formas que a Rússia encontrou para espalhar desinformação, nomeadamente através de edição de vídeos russos, mensageiros como o Telegram e de bots;
- Adição de artigo sobre o software de ciberspionagem NSO ter sido usado para hackear jornalistas e ativistas no México;
- Adição de informação e de um artigo sobre um caso em que uma empresa foi condenada por despedir um trabalhador nos Países Baixos por não se deixar ser filmado durante o período de trabalho remoto;
- Adição de um artigo sobre tipos de apps que traficam dados pessoais, nomeadamente apps de meteorologia, redes sociais e de serviços de encontros amorosos;
- Adição de informação e de um artigo em como ignorar alguém com o uso do telemóvel pode levar a um ciclo de ressentimento e retaliação;
- Adição de mais um artigo sobre a aplicação Fog, que permite seguir os movimentos de indivíduos online, usado pela polícia americana. E que aborda os temas da vigilância digital e privacidade nos Estados Unidos;
- Adição de artigo sobre nova vulnerabilidade no software da Microsoft que pode ter exposto os dados pessoais de 65,000 empresas em 111 países;
- Adição de artigo sobre o excesso de lixo tecnológico, que deverá ver 5.3 milhares de milhões de telemóveis descartados durante o ano de 2022 a nível global;
- Adição de informação e de um artigo sobre como o modo incógnito do Google Chrome não protege significativamente a privacidade dos seus utilizadores;
- Adição de informação e um artigo sobre a Federal Trade Commission, que supervisiona as empresas online, estar-se a debruçar sobre os padrões negros usados nos negócios online;
- Adição de informação e do documento da FTC sobre padrões negros online, que os detalha e expande sobre eles;
- Adição de informação e de um artigo sobre a videovigilância, a propaganda e a censura na China;
- Adição de informação e de um artigo sobre o evento Network X em Amsterdão onde manifestam profunda preocupação para com a falta de segurança e a

crescente abstração dos serviços digitais atuais e a crescente proliferação e profissionalização dos hackers.

- 05/11/2022
 - Adição da notícia “Scientists Increasingly Can’t Explain How AI Works”, de que investigadores sobre Inteligência Artificial urgem os criadores de sistemas de AI a se focar em como e porquê produzem estes sistemas os resultados que produzem, em vez de na rapidez e exatidão dos resultados;
 - Adição da notícia “AI’s true goal may no longer be intelligence”, sobre o facto de que a discussão à volta da Inteligência Artificial está a deixar as questões profundas sobre inteligência, e inteligêncial geral, e se focar nas suas aplicações tecnológicas, que a fazem parecer inteligente;
 - Adição da notícia “America’s Ring doorbell camera obsession highlights the scourge of mass surveillance” sobre a invasão de privacidade e a insegurança decorrente da obsessão com câmaras de vídeo;
 - Adição do artigo “Facebook probably has your phone number, even if you never shared it. Now it has a secret tool to let you delete it.” sobre uma ferramenta que permite verificar a existência e eliminar informações de contacto pessoal da plataforma Facebook;
 - Adição do artigo “Truth Cops”, que detalham os planos do Department of Homeland Security de policiar a informação incorreta nas redes sociais, assim como outros esforços do governo americano de gerir o discurso online;
 - Adição do artigo “Exclusive: State Dept. gives law enforcement, intelligence agencies unrestricted access to Americans’ personal data”, assim como informação do mesmo ao documento, sobre a violação de privacidade perpetrada pelo governo americano de dar informação contidas nas aplicações para passaporte às agências de inteligência e forças policiais americanas, sem qualquer supervisão ou processo legal;
 - Adição do artigo “UK government set to extract hospital data to Palantir system without patient consent” e informação sobre ele, sobre a intenção do governo britânico de infundir dados médicos privados dos cidadãos britânico detido pelo NHS (serviço de saúde público) na sua plataforma de dados criada com a empresa privada Palantir, sem garantir o anonimato dos pacientes;
 - Adição do artigo “Matter could be better”, e de informação sobre ele, sobre o novo paradigma de comunicação associado a casas inteligentes, que enfraquece a privacidade dos consumidores e torna-os significativamente mais vulneráveis

ataques informáticos maliciosos, ao permitir aparelhos inteligentes ligarem-se diretamente à Internet de forma autónoma;

- Adição do artigo “TikTok is "unacceptable security risk" and should be removed from app stores, says FCC” e de informação ao artigo, sobre o pedido da FCC americana à Apple e à Google para removerem a aplicação TikTok das suas lojas digitais, por ser um perigo à privacidade dos cidadãos americanos, ao acumular uma grande quantidade de dados privados e possibilitar o acesso destes ao estado chinês;
- Adição do artigo “TikTok’s updated data privacy policy does little to settle nerves” sobre como o TikTok permite a empregados seus de países terceiros aceder à informação privada de cidadãos europeus;
- Adição do artigo “To Fight Misinformation, We Need to Teach That Science Is Dynamic” sobre a necessidade de divulgar a forma como a ciência é criada, esclarecendo incertezas e combatendo a desinformação.

- 30/12/22

- Adição do artigo “A leaked Amazon memo may help explain why the tech giant is pushing out so many recruiters” e de informação nele contida, sobre a Amazon está a testar uma solução de Inteligência Artificial para o recrutamento de pessoal, enquanto conduz a dispensa de centenas de recrutadores;
- Adição do artigo “An AI Algorithm is Raising Rents on Hundreds of Thousands of People Across the Country” e informação contida ao documento, sobre software de Inteligência Artificial usada para gerir investimentos imobiliários e gerir o valor das rendas;
- Adição do artigo “Robot Landlords Are Buying Up Houses” ao documento, sobre o uso de Inteligência Artificial para gerir imóveis;
- Adição do artigo “He Used AI to Publish a Children’s Book in a Weekend. Artists Are Not Happy About It” e de informação ao documento, sobre um oportunista que usou vários programas de Inteligência Artificial para criar um livro infantil num fim de semana e pôs-lo à venda na Amazon;
- Adição do artigo “The College Essay Is Dead” e de informação dele ao documento, sobre como programas de inteligência artificial já são usados para produzir trabalhos académicos;

- Adição do artigo “OpenAI upgrades GPT-3, stunning with rhyming poetry and lyrics” e de informação nele contida, sobre o uso de um programa de Inteligência Artificial para criar poesia e letras para música;
 - Adição do artigo “AI unmask anonymous chess players, posing privacy risks” e de informação nele contida ao documento, sobre um programa de Inteligência Artificial que consegue pelo estilo de jogo de xadrez identificar o jogador, um avanço na Inteligência Artificial que pode ajudar a identificar pessoas por outros padrões de comportamento;
 - Adição do artigo “AI image generation tech can now create life-wrecking deepfakes with ease” ao documento, sobre a facilidade e a qualidade de fakes com base em fotos ou imagens pessoais com o recurso a Inteligência Artificial;
 - Adição do artigo “AI-Created Comic Could Be Deemed Ineligible for Copyright Protection” e de informação dele ao documento, sobre o facto do Gabinete de Direitos de Autor americano estar em processo para tornar não-ilegível trabalhos artísticos baseados em Inteligência Artificial de direitos de autor;
 - Adição do artigo “ChatGPT. O prodígio da Inteligência Artificial é ‘empolgante’, mas é preciso ter cuidado com ‘efeitos secundários’”, e de informação nele contida ao documento.
- 21/02/23
 - Adição do artigo “Bard is going to destroy online search” e informação sobre como a inteligência artificial tenderá a mudar as pesquisas online e até a curiosidade humana;
 - Adição do artigo Noam Chomsky on ChatGPT: It’s “Basically High-Tech Plagiarism” and “a Way of Avoiding Learning”, sobre as afirmações do pensador Noam Chomsky sobre usos de programas de Inteligência Artificial;
 - Adição do artigo “Saudi Arabia jails two Wikipedia staff in ‘bid to control content’” e de informação sobre ele, em como o regime opressivo da Arábia Saudita condenou 2 funcionários da Wikipedia, como forma de procurar controlar o conteúdo do serviço de informação;
 - Adição do artigo “How the governance of and through digital contact tracing technologies shapes geographies of power” e de informação sobre ele, de como a tecnologia empregue durante a pandemia mundial afetou a governação política, a democracia e o papel das empresas tecnológicas, em especial na Áustria e na Noruega;

- Adição do artigo “Police seize on COVID-19 tech to expand global surveillance”, e de informação sobre ele, de como a tecnologia de contact-tracing desenvolvida para a pandemia de Covid-19 está em uso em países como a China, Israel e a Austrália para vigiar cidadãos e limitar as suas liberdades, para fins não relacionados com a pandemia;
 - Adição do artigo “Facebook addiction increases depression severity among people who are already depressed”, sobre um estudo longitudinal que apresenta resultados que apoiam a ideia de que o vício ao Facebook aumenta a severidade da depressão em pessoas já diagnosticadas com depressão;
 - Adição do artigo “Apple Says Your iPhone's Usage Data is Anonymous, but New Tests Say That's Not True” e de informação sobre ele, sobre o facto da Apple recolher informação que identifica e seguir os utilizadores dos iPhones, embora publicamente afirme que não o faz;
 - Adição do artigo “TikTok admits to spying on U.S. users as effort to ban the app heats up” e de informação dele, sobre os resultados de uma investigação interna no TikTok que revelaram que dados pessoais de duas contas de jornalistas americanos foram acedidos por quatro empregados chineses, posteriormente, alegadamente despedidos.
- 30/04/23
 - Adição do artigo “A.I. Will Not Displace Everyone, Everywhere, All at Once. It Will Rapidly Transform the Labor Market, Exacerbating Inequality, Insecurity, and Poverty” e informação sobre ele no documento, sobre como a automatização leva à migração de trabalhadores para empregos menos qualificados, ajudando a baixar salários, e como a automatização de postos de trabalho e a multiplicação de empregos menos qualificados leva a uma diminuição do aumento de produtividade.
 - 04/05/23
 - Adição do artigo “ChaosGPT And Why We Need AI Regulation” sobre uma variante do Auto-GPT que procura causar caos e destruição reais, e informação sobre ela ao artigo;
 - Adição do website do ChaosGPT ao documento;
 - Adição do endereço de um vídeo sobre o ChaosGPT ao documento.

- 22/09/23
 - Adição do vídeo “Top 10 Viral Challenges That Got People Killed” à bibliografia e alguma informação sobre ele ao artigo;
 - Adição do artigo “If You’ve Got a New Car, It’s a Data Privacy Nightmare” e informação contida nele ao documento.
- 01/10/23
 - Adição do vídeo do Youtube intitulado “The Death Of NFT Collections & Trading”, do criador de conteúdo YongYea, às referências, sobre a história e declínio da tecnologia NFT.
- 23/10/23
 - Adição da fonte e informação do artigo “A “Laudate Deum” e a Inteligência Artificial” sobre como o uso massivo de Inteligência Artificial pode aumentar significativamente o uso de energia elétrica;
 - Adição da fonte do artigo científico no qual se baseia a artigo referido anteriormente, “The growing energy footprint of artificial intelligence”.
- 31/10/23
 - Adição do artigo «Inteligência Artificial generativa pode ter impacto de 15.000 M€ em Portugal» ao documento e informação sobre ele;
 - Adição do artigo «Notários portugueses foram alvo de um ataque informático que terá recorrido a inteligência artificial» ao documento e informação sobre ele;
 - Adição do artigo «Há três esquemas online que estão a roubar milhões aos portugueses. Saiba como atuam os burlões e como se proteger» às fontes (referências);
 - Adição do artigo «Federal Court Rules Work Generated by Artificial Intelligence Alone Is Not Eligible for Copyright Protection» ao documento e informação sobre ele;
 - Adição do artigo «What do the latest US and China rulings on AI authorship mean for luxury?» ao documento e informação sobre ele;
 - Adição do artigo «Gere texto, imagens, códigos e muito mais com a IA do Google Cloud» às referências.

- 02/11/23
 - Adição do artigo «Estudo revela que equipamentos inteligentes espiam-nos em casa: “As pessoas não têm ideia”» à bibliografia;
 - Adição de informação do artigo «Guterres defende acesso dos países em desenvolvimento à Inteligência Artificial» ao documento e dele à bibliografia;
 - Adição de informação do artigo «Vai nascer um clube privado de líderes em ciência de dados em Portugal» ao documento e dele à bibliografia;
 - Adição do artigo «We built a ‘brain’ from tiny silver wires. It learns in real time, more efficiently than computer-based AI» à bibliografia.
- 03/11/23
 - Adição do estudo «Study: Deep neural networks don’t see the world the way we do» ao documento e de informação sobre ele;
 - Adição do artigo «Democracia portuguesa cai a pique em índice de avaliação dos cidadãos» ao documento e de informação sobre ele;
 - Adição do artigo «Parlamento aprova texto dos metadados que prevê conservação generalizada até seis meses» ao documento e de informação sobre ele.
- 22/02/24
 - Adição do artigo “As fotos vão para a tua família.” Chantagem e manipulação de imagens por Inteligência Artificial” que versa sobre a utilização de ferramentas de Inteligência Artificial para forjar fotos e outros registos pessoais com vista à chantagem, e adição de informação do artigo ao documento;
 - Adição do artigo “China uses AI to generate propaganda on YouTube, report finds” e de informação sobre ele ao documento, nomeadamente sobre a existência de várias contas de Youtube que usam Inteligência Artificial para passar propaganda do regime político chinês;
 - Adição dos artigos “China announces rules to reduce spending on videojogos” e “China considers revising gaming rules after tech giants lose billions” sobre a aventura de criar legislação efetiva para gerir o mercado dos videojogos online, a histeria dos investidores à volta da proibição de práticas predatórias generalizadas sobre os utilizadores – que tem o potencial para afetar adversamente de forma significativa os seus ganhos – e a sensibilidade do governo chinês a estes interesses;

- Adição do artigo “Microsoft and ZeniMax union reach “first of its kind” agreement over usage of AI tools in gamedev” e informação sobre o acordo pioneiro entre a Microsoft e a união de trabalhadores de empresa de videojogos ZeniMax sobre a implementação de ferramentas de Inteligência Artificial na empresa;
 - Adição da referência ao documentário The Gig Is Up e de informação contida no mesmo ao documento, abordando os temas da *gig economy* (da Uber, por exemplo) e o trabalho tecnológico precário por detrás da magia associada à Inteligência Artificial e às apps (do Amazon Mechanical Turk, por exemplo) no ponto de vista dos trabalhadores, do jornalismo e da comunidade científica.
- 01/05/24
 - Adição de informação sobre o esforço das empresas de tecnológicas para colonizar a atenção dos seus consumidores, tentando monopolizá-la em, por exemplo, os videojogos no modelo “live service”;
 - Informação sobre o surgimento e o sucesso dos programas que procuram simular uma relação pessoal com o seu utilizador, mencionando a política de privacidade questionável associada a estes serviços e o treino pelo utilizador do programa para o manipular de forma inadvertida;
 - Menção de que a Inteligência Artificial tem sido usada de forma massiva para fazer o trabalho criativo para pessoas sem grande capacidade artística, como os gestores das empresas, tornando o trabalho dos artistas redundante e fazendo perigar a sua segurança económica, em vez de oferecer aos artistas formas de tornar o seu trabalho menos aborrecido;
 - Inclusão da música Reaktion da banda RezoDrone que retrata bem a ilusão e a toxicidade da relação humana com a tecnologia.
 - 14/05/24
 - Inclusão do vídeo The Dark Future of Relationships – e de informação sobre ele – que aborda o tema da utilização da Inteligência Artificial para explorar para ganho financeiro o isolamento e a solidão das populações, que pode acabar por ter um efeito pernicioso ao aumentar a abstração das relações e aprofundar as carências sociais e afetivas dos seus consumidores.

- 20/07/24
 - Adição do artigo «Scarlett Johansson acusa OpenAI de imitar a sua voz. “Sky” retirada do ChatGPT» e informação sobre ele para o documento sobre o comportamento implacável da OpenAI se apropriando sem respeito da voz da atriz;
 - Adição do artigo «Perito português em inteligência artificial alerta para riscos da nova tecnologia» sobre perigos apontados ao desenvolvimento sem supervisão governamental da Inteligência Artificial e adição de informação dele ao documento;
 - Adição do vídeo «Will AI kill all of us? | Yuval Noah Harari and Lex Fridman» e informação sobre ele ao documento.
- 21/07/24
 - Adição do vídeo «What well-being is (and isn't), according to neuroscience | Mary Helen Immordino-Yang» e informação sobre ao documento.
- 23/07/24
 - Adição do artigo «Paolla Oliveira faz denúncia após ser vítima de montagem com inteligência artificial...» e de informação sobre ao documento.
- 25/07/24
 - Adição do artigo «Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI» sobre a legislação da União Europeia sobre Inteligência Artificial que entrará em vigor 2026, salvo exceções, assim como foi acrescentada informação sobre ele ao documento;
 - Adição do artigo «AI systems could be on the verge of collapsing into nonsense, scientists warn» sobre o risco da informação retornada pelas aplicações de Inteligência Artificial ser utilizada para novo processamento podendo em pouco tempo levar a que os resultados destas aplicações se tornem disparatados, e adição de informação sobre o artigo ao documento;
 - Adição da página «Lei n.º 18/2024, de 5 de fevereiro» sobre a nova lei portuguesa sobre os metadados, e de alguma informação sobre ela ao artigo;
 - Adição da informação que um possível leilão para o 5G sobre a faixa dos 26 GHz só deverá ocorrer depois de 2024.

- 14/08/24
 - Adição do artigo «IA invade publicações científicas e, para pesquisador, situação deve piorar» e de informação sobre ele ao documento.
- 26/08/24
 - Menção que a acção de scrolling é exigente mentalmente e torna-se cansativa, consumindo também normalmente mais tempo que o que o inicialmente pretendido pelo indivíduo.
- 21/09/24
 - Adição de informação sobre o artigo «É fake que IA "saiu do controle" no Japão; entenda» sobre como um programa de Inteligência Artificial contornou parâmetros definidos por experimentadores e agiu contrariamente as suas intenções;
 - Adição de menção à intenção expressa do governo português de usar ferramentas de Inteligência Artificial para monitorizar os contribuintes portugueses.
- 20/02/25
 - Adição do artigo «Geração Z está perdendo uma habilidade que temos há 5,5 mil anos: 40% estão perdendo a fluência na comunicação» ao texto do documento e à bibliografia, sobre os efeitos da tecnologia sobre as faculdades de pensar e escrita.
- 05/03/25
 - Adição do vídeo «They're Making Technology Worse - (On Purpose)» ao documento e de informação sobre ele, sobre o fenómeno de enshittification que, na procura de lucros maiores pelas empresas, está a tornar a generalidade de produtos e serviços piores para os consumidores
- 21/08/25
 - Adição de fonte e informação sobre o conjunto de leis conhecido como “Online Safety Act” em implementação em 2025 pelo governo do Reino Unido, que obriga os cidadãos britânicos a enviarem a sua identificação para usarem a Internet;

- Adição de informação sobre um caso em que a polícia visitou um cidadão por causa de uma mensagem postada nas redes sociais no Reino Unido;
 - Adição de fontes e informação sobre a lei em discussão “Chat Control” no parlamento europeu, sobre a intenção de espionagem de mensagens privadas e ficheiros de todos os cidadãos europeus excepto sobre a classe política;
 - Adição de fonte e de informação sobre a implementação australiana de um sistema de controlo de acesso à Internet semelhante ao inglês, no qual será preciso, a partir de dezembro de 2025, identificação do utilizador por câmara e a cedência dos dados da sua localização;
 - Adição de informação e fontes sobre o comportamento ditatorial de processadores de pagamento como Mastercard e Paypal, que têm se recusado a permitir a compra de materiais legais por declarem serem maus para a sua imagem empresarial, com isto directa ou indirectamente procurando condicionar os artigos disponibilizados na Internet, nos mercados;
 - Adição de informação e fonte sobre a plataforma online Roblox, que apresenta múltiplas microtransações para a sua audiência de, tendencialmente, menores de idade e permite o contacto destes com predadores sexuais, com um caso documentado de rapto de uma criança por um predador sexual associado a contacto na plataforma Roblox, mas que no entanto continua, ao contrário de outras plataformas e vendedores de conteúdos online, a merecer o serviço de processadores de pagamentos como a Mastercard.
- 23/08/25
 - A referência e adição às fontes de informação sobre a necessidade massiva de água de *data centers* gigantesco para suportar o desenvolvimento da Inteligência Artificial e outras tecnologias por empresas privadas.
 - 24/08/25
 - Adição de informação e da fonte do vídeo “Yuval Noah Harari: Como proteger sua mente na era da informação lixo” sobre a Inteligência Artificial e a sua relação com o ser humano.
 - Adição de informação e da fonte do vídeo “A verificação da idade na Internet chegou aos EUA”, nomeadamente aos estados de Mississippi e de Texas;

- Adição do vídeo “This Is What a Digital Coup Looks Like | Carole Cadwalladr | TED” às fontes sobre a sua batalha judicial com o político Nigel Farage onde a sua privacidade digital foi totalmente devassada;
 - Adição do artigo sobre o Reino Unido “Police make 30 arrests a day for offensive online messages” e de informação sobre ele ao documento;
 - Adição às fontes do vídeo “How AI uses our drinking water - BBC World Service”;
 - Adição às fontes do vídeo “Why data centers are eating up enormous water resources | Transforming Business”.
- 25/09/2025
 - Adição às fontes do vídeo “Corremos um perigo real de perder nossas almas e nossa humanidade.” e de informação sobre ele ao documento, de como a virtualidade e a abstração da tecnologia que abusamos pode conduzir a indivíduos mais desumanizados;
 - Adição às fontes do artigo “Bollywood stars fight for personality rights amid deepfake surge” e de informação ao documento, sobre a razão dada a estrelas do cinema indiano nos tribunais sobre os seus direitos de imagem, incluindo contra forjações com Inteligência Artificial.
 - 27/09/2025
 - Adição às fontes do artigo “Meta analisa fragilidade dos jovens para exibir anúncios, diz denunciante” e de informação sobre este ao documento, sobre como a plataforma Facebook analisa o comportamento, neste caso de jovens, em especial procurando sinais de depressão e partilhava essa informação com anunciantes para vender produtos;
 - Adição às fontes do vídeo “AI’s first kill and why top experts predict our extinction.” sobre o comportamento amoral e cada vez mais difícil de controlar da Inteligência Artificial e o perigo existencial que representa para a Humanidade;
 - Adição às fontes do artigo “Bónus e salários de 100 milhões: Zuckerberg acusado de aliciar talentos da OpenAI com propostas milionárias” e de informação sobre ele ao documento.

- 28/09/2025
 - Adição da informação que as grandes empresas tecnológicas, como a Google, Microsoft e Adobe, estão a adicionar Inteligência Artificial às suas aplicações;
 - Adição da fonte do artigo “Adobe AI controversy: Why are creators ditching Adobe?” às fontes do documento.
- 02/10/2025
 - Adição do artigo “What the AI Actor Tilly Norwood Means for the Future of Film” às fontes e de informação sobre ele ao documento, sobre a polémica apresentação da primeira atriz criada com Inteligência Artificial.
- 03/10/2025
 - Adição do vídeo “Replacing Humans with AI is Going Horribly Wrong” e de informação sobre ele ao documento, que aborda o facto de 95% das aplicações piloto de Inteligência Artificial estudadas pelo MIT falhar em apresentar um aumento de rendimento assinalável, gerando indiferença e até arrependimento entre os profissionais sobre a sua adopção;
 - Adição do artigo “MIT report: 95% of generative AI pilots at companies are failing” com ligação ao relatório do MIT ao documento.
- 04/10/2025
 - Adição do artigo “Japan faces Asahi beer shortage after cyber-attack” e de informação sobre ele ao documento, sobre um grande ciberataque sofrido pela gigante japonesa de bebidas e comida Asahi que irá provocar escassez dos seus produtos no Japão.
- 10/10/25
 - Adição às fontes do artigo “New digital ID scheme to be rolled out across UK” e ao documento, sobre a implementação do governo britânico de uma identificação online dos seus cidadãos;
 - Adição às fontes do artigo “ID photos of 70,000 users may have been leaked, Discord says” e ao documento, sobre o ataque informático que a empresa de

comunicação online Discord sofreu que expôs as fotografias de identificação de 70 000 utilizadores assim como outros dados pessoais;

- Adição às fontes do artigo “It’s official! Germany “will not agree” to Chat Control – here's everything we know” e ao documento, sobre a oposição dos eurodeputados germânicos à proposta de lei conhecida como Chat Control que efetivamente leva ao seu chumbo;
- Adição às fontes do artigo “RUSSIA introduces DIGITAL ID under the State controlled MAX app.Zakharova about the missing children” e ao documento, sobre a introdução de identificação digital na Rússia.

- 13/10/2025

- Adição ao documento de informação sobre e às suas fontes do vídeo “HUGE Online Safety Act Data Breach”, sobre como o ataque informático ao Discord pode ter abrangido mais de 2 milhões de utilizadores, cuja identificação pode ter sido roubada.

19 - Referências

- 1) Humanity's broken risk perception is reversing global progress in a 'spiral of self-destruction', finds new UN report – United Nations Office for Disaster Risk Reduction, <https://www.undrr.org/news/humanitys-broken-risk-perception-reversing-global-progress-spiral-self-destruction-finds-new>
- 2) Humanity locked in a 'spiral of self-destruction' unless we change our perception of risk, UN says – Space.com, <https://www.space.com/un-humanity-spiral-self-destruction>
- 3) Mobile signal woes 'strengthens' business case for 5G - TechRadar, <https://www.techradar.com/news/mobile-signal-woes-strengthens-business-case-for-5g>
- 4) Rede 5G: Saiba o que vai mudar e a diferença entre o 4G e o 5G - Adslfibra, <https://adslfibra.pt/servicos/cobertura/5g>
- 5) 5G - NOS, <https://www.nos.pt/particulares/5g/Pages/5g.aspx>
- 6) Início – Portal 5G, <https://portal5g.pt/>
- 7) O que é o 5G? Quais as funcionalidades e casos de uso desta rede - Gemalto, <https://www.gemalto.com/brasil/telecom/inspire-se/5g>
- 8) How emergency services and disaster recovery will benefit from 5G - TechRadar, <https://www.techradar.com/news/how-emergency-services-and-disaster-recovery-will-benefit-from-5g>
- 9) How 5G is set to revolutionize healthcare - TechRadar, <https://www.techradar.com/news/how-5g-is-set-to-revolutionize-healthcare>
- 10) What does 5G means for autononous vehicles? - TechRadar, <https://www.techradar.com/news/what-does-5g-mean-for-autonomous-vehicles>
- 11) How is 5G set to change the classroom - TechRadar, <https://www.techradar.com/news/how-is-5g-set-to-change-the-classroom>
- 12) This is how 5G will take mobile gaming to the next level - TechRadar, <https://www.techradar.com/news/this-is-how-5g-will-take-mobile-gaming-to-the-next-level>
- 13) What does 5G mean for robotics? - TechRadar, <https://www.techradar.com/news/what-does-5g-mean-for-robotics>

- 14) Get ready for a 5G Internet of the Sky - TechRadar,
<https://www.techradar.com/news/get-ready-for-a-5g-internet-of-the-sky>
- 15) 5G RuralFirst looks at smart farming, spectrum sharing and broadcasting - TechRadar,
<https://www.techradar.com/news/5g-ruralfirst-looks-at-smart-farming-spectrum-sharing-and-broadcasting>
- 16) Transforming sports for spectators: the 5G effect - TechRadar,
<https://www.techradar.com/news/transforming-sports-for-spectators-the-5g-effect>
- 17) How will smartwatches and fitness trackers make use of 5G - TechRadar,
<https://www.techradar.com/news/how-will-smartwatches-and-fitness-trackers-make-use-of-5>
- 18) Will 5G solve signal issues at stadiums, festivals and venues? - TechRadar,
<https://www.techradar.com/news/will-5g-solve-signal-issues-at-stadiums-festivals-and-venues>
- 19) 5G and film: how will the tech change how we consume movies? - TechRadar,
<https://www.techradar.com/news/5g-and-film-how-will-the-tech-change-how-we-consume-movies>
- 20) How 5G could improve augmented reality - TechRadar,
<https://www.techradar.com/news/how-5g-could-improve-augmented-reality>
- 21) 5G and smart cities: everything you need to know - TechRadar,
<https://www.techradar.com/news/5g-and-smart-cities-everything-you-need-to-know>
- 22) How 5G could make your home smarter - TechRadar,
<https://www.techradar.com/news/how-5g-could-make-your-home-smarter>
- 23) 5G set to push mobile data use sky-high - TechRadar,
<https://www.techradar.com/news/5g-set-to-push-mobile-data-use-sky-high>
- 24) The future of cybersecurity in a 5G-connected world - TechRadar,
<https://www.techradar.com/news/the-future-of-cybersecurity-in-a-5g-connected-world>
- 25) 5G: How will businesses benefit? - TechRadar, <https://www.techradar.com/news/5g-how-will-businesses-benefit>
- 26) 5G's impact on the future of work - TechRadar, <https://www.techradar.com/news/5gs-impact-on-the-future-of-work>

- 27) AI won't steal your job, just make it meaningless - Iai, <https://iai.tv/articles/ai-wont-steal-your-job-just-make-it-meaningless-auid-2082>
- 28) A.I. Will Not Displace Everyone, Everywhere, All at Once. It Will Rapidly Transform the Labor Market, Exacerbating Inequality, Insecurity, and Poverty – Ubi Guide, <https://www.scottssantens.com/ai-will-rapidly-transform-the-labor-market-exacerbating-inequality-insecurity-and-poverty/>
- 29) AI Robot Lawyers Are Saving Morgan Stanley Millions In Soliciting Fees – Contx, <https://www.contxmedia.com/robot-lawyers-save-morgan-stanley-millions-soliciting-fees/>
- 30) A leaked Amazon memo may help explain why the tech giant is pushing out so many recruiters – Vox, <https://www.vox.com/recode/2022/11/23/23475697/amazon-layoffs-buyouts-recruiters-ai-hiring-software>
- 31) Philosopher of the apocalypse – Aeon, <https://aeon.co/essays/gunther-anders-a-forgotten-prophet-for-the-21st-century>
- 32) Uso de tecnologia em contexto laboral invade vida pessoal, consideram mais de metade dos trabalhadores – Visão, <https://visao.sapo.pt/atualidade/sociedade/2022-03-16-uso-de-tecnologia-em-contexto-laboral-invade-vida-pessoal-consideram-mais-de-metade-dos-trabalhadores/>
- 33) Direito a desligar: A empresa pode ligar-me? E quem paga despesas do teletrabalho? - Jornal de Notícias, <https://www.jn.pt/nacional/direito-a-desligar-a-empresa-pode-ligar-me-e-quem-paga-despesas-do-teletrabalho-14284846.html>
- 34) Teletrabalho. Envio de email sem exigir resposta imediata não viola direito a desligar – Diário de Notícias, <https://www.dn.pt/sociedade/teletrabalho-envio-de-email-sem-exigir-resposta-imediata-nao-viola-direito-a-desligar-14581267.html>
- 35) Xbox Cloud Gaming (Beta) with Xbox Game Pass – Xbox, <https://www.xbox.com/en-US/xbox-game-pass/cloud-gaming>
- 36) Playstation Now – Playstation, https://www.playstation.com/pt-pt/ps-now/?emcid=pa-co-422324&gclid=Cj0KCQiAraSPBhDuARIsAM3Js4ppJDzBQZPwRAYYZP21yR5p_ZEpb_nFWRZXW1nTBE5jctPPZRLAfIUUaAodbEALw_wcB&gclsrc=aw.ds
- 37) Blockchain – Builtin, <https://builtin.com/blockchain>
- 38) TRON introduces NFT standard TRC-721 – DappRadar, <https://dappradar.com/blog/tron-introduces-nft-standard-trc-721>

- 39) Axie Infinity – Axie Infinity, <https://axieinfinity.com/>
- 40) NFTs, explained – The Verge, <https://www.theverge.com/22310188/nft-explainer-what-is-blockchain-crypto-art-faq>
- 41) Line Goes Up – The Problem with NFTs – Youtube, https://www.youtube.com/watch?v=YQ_xWvX1n9g
- 42) NFTs, RA e Jogos de Casino: empresas portuguesas exploram tecnologias inovadoras no mundo do gaming – Diário de Notícias, <https://www.dnoticias.pt/2022/5/13/310811-nfts-ra-e-jogos-de-casino-empresas-portuguesas-exploram-tecnologias-inovadoras-no-mundo-do-gaming/>
- 43) Textbook publisher: NFTs will let us squeeze even more money out of students – The Verge, <https://www.theverge.com/2022/8/3/23290335/pearson-textbook-publisher-nft-blockchain-secondhand-ebook-sales>
- 44) The Death Of NFT Collections & Trading – Youtube, <https://www.youtube.com/watch?v=2JYlopnc3I8>
- 45) Is web3 a scam? | Jan Liphardt | TEDxBostonStudio – Youtube, https://www.youtube.com/watch?v=K2_EeEo7kwY
- 46) BMW starts selling heated seat subscriptions for \$18 a month – The Verge, <https://www.theverge.com/2022/7/12/23204950/bmw-subscriptions-microtransactions-heated-seats-feature>
- 47) 5 things about 5G more important than the speed - TechRadar, <https://www.techradar.com/news/5-things-about-5g-more-important-than-the-speed>
- 48) The future of cybersecurity in a 5G-connected world - TechRadar, <https://www.techradar.com/news/the-future-of-cybersecurity-in-a-5g-connected-world>
- 49) 5G – uma evolução que exige muita prudência - Técnico Lisboa, <https://tecnico.ulisboa.pt/pt/noticias/campus-e-comunidade/5g-uma-evolucao-que-exige-prudencia/>
- 50) 5G - Wikipedia, <https://en.wikipedia.org/wiki/5G>
- 51) 5G - Wikipedia, <https://pt.wikipedia.org/wiki/5G>
- 52) What is 5G - PCMag, <https://www.pcmag.com/article/345387/what-is-5g>

- 53) Overview of Risks Introduced by 5G Adoption in the United States - Cybersecurity and Infrastructure Security Agency,
https://www.dhs.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf
- 54) What Type of Wavelengths Do Cellphones Use? - Techwalla.com,
<https://www.techwalla.com/articles/what-type-of-wavelengths-do-cellphones-use>
- 55) Radiofrequency radiation - Australian Radiation Protection and Nuclear Safety Agency, <https://www.arpsa.gov.au/understanding-radiation/what-is-radiation/non-ionising-radiation/radiofrequency-radiation>
- 56) Radio Frequency - Wikipedia, https://en.wikipedia.org/wiki/Radio_frequency
- 57) Electromagnetic Radiation - Wikipedia,
https://en.wikipedia.org/wiki/Electromagnetic_radiation
- 58) Electromagnetic Spectrum - Wikipedia,
https://en.wikipedia.org/wiki/Electromagnetic_spectrum
- 59) Anatomy of an Electromagnetic Wave - NASA,
https://science.nasa.gov/ems/02_anatomy
- 60) Luz: ondas eletromagnéticas, espectro eletromagnético e fótons - Khan Academy,
<https://pt.khanacademy.org/science/physics/light-waves/introduction-to-light-waves/a/light-and-the-electromagnetic-spectrum>
- 61) Ondas Milimétricas - NUCTECH,
<http://www.nuctech.com/br/SitePages/ThNormalPage.aspx?nk=TECH&k=EEBCEI>
- 62) Please Lower Small Cell Antenna Heights in 5G - IEEE Xplore Digital Library,
<https://ieeexplore.ieee.org/document/7842150/>
- 63) Advanced Antenna Systems for 5G White Paper - 5G Americas,
https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Americas_Advanced-Antenna-Systems-for-5G-White-Paper.pdf
- 64) Vodafone to use manhole covers to improve 4G and 5G - TechRadar,
<https://www.techradar.com/news/vodafone-to-use-manhole-covers-to-improve-4g-and-5>
- 65) Massive MIMO and Beamforming: The Signal Processing Behind the 5G Buzzwords - Analog Dialogue, <https://www.analog.com/en/analog-dialogue/articles/massive-mimo-and-beamforming-the-signal-processing-behind-the-5g-buzzwords.html#>

- 66) 5G Radios are Packed with Advanced Antenna Technology - Commscope
<https://www.commscope.com/blog/2019/5g-radios-are-packed-with-advanced-antenna-technology/>
- 67) Active Antenna Versus Passive Antenna Design – RCR Wireless,
<https://www.rcrwireless.com/20210916/5g/active-antennas-are-essential-to-5g-deployments-analyst-angle>
- 68) MIMO - Wikipedia, <https://en.wikipedia.org/wiki/MIMO>
- 69) Beamforming - Wikipedia, <https://en.wikipedia.org/wiki/Beamforming>
- 70) Exemplos de instalações de células pequenas 5G - Associação de Surf e Atividades Marítimas do Algarve, <http://www.asmaa-algarve.org/en/5g/5g-articles/examples-of-5g-small-cell-installations>
- 71) 25 Cell Phone Towers Disguised to Look Like Something Else - Twisted Sifter,
<https://twistedsifter.com/2012/08/examples-of-cell-phone-tower-disguises/>
- 72) New trend of 2019 LED lighting: 5G smart street lights - uPowerTek,
<https://www.upowertek.com/2019/08/22/new-trend-of-2019-led-lighting-5g-smart-street-lights/>
- 73) Smart Street Lamps - Huawei, <https://www.huawei.com/minisite/iot/en/smart-lighting.html>
- 74) ALERTA: Postes de lâmpadas LED que são liderados por 5G enab estão surgindo em todo o país - Associação de Surf e Atividades Marítimas do Algarve, <http://www.asmaa-algarve.org/en/5g/5g-articles/alert-led-lampposts-that-are-5g-enabled-are-springing-up-all-over-portugal>
- 75) Luminárias vão ser substituídas por tecnologia LED em Albufeira - Associação de Surf e Atividades Marítimas do Algarve,
<http://www.asmaa-algarve.org/en/5g/5g-articles/luminarias-vao-ser-substituidas-por-tecnologia-led-em-albufeira>
- 76) EDP Distribuição instalada + - 600 mil luminárias LED até dezembro de 2019 em Portugal - Associação de Surf e Atividades Marítimas do Algarve, <http://www.asmaa-algarve.org/en/5g/5g-articles/edp-distribuicao-instalou-600-mil-luminarias-led-ate-dezembro-de-2019-em-portugal>
- 77) Luzes de rua inteligentes LED 5G - o que a indústria está dizendo - Associação de Surf e Atividades Marítimas do Algarve,

<http://www.asmaa-algarve.org/en/5g/5g-articles/led-5g-smart-street-lights-what-the-industry-is-saying>

78) EMF frequencies used for crowd control weapons form the foundation of 5G network – Nexus Newsfeed.com, <https://nexusnewsfeed.com/article/human-rights/emf-frequencies-used-for-crowd-control-weapons-form-the-foundation-of-5g-network/>

79) Active Denial System FAQs - Non-Lethal Weapons Program U.S. Department of Defense, <https://jnlwp.defense.gov/About/Frequently-Asked-Questions/Active-Denial-System-FAQs/>

80) Microwave ovens - EXPLAINTHATSTUFF!, <https://www.explainthatstuff.com/microwaveovens.html>

81) Microwave ovens - World Health Organization, https://www.who.int/peh-emf/publications/facts/info_microwaves/en/

82) Electromagnetic Spectrum - The Physics Hypertextbook, <https://physics.info/em-spectrum/>

83) Definition of frequency bands (VLF, ELF... etc.) - Renato Romero Home Page, <http://www.vlf.it/frequency/bands.html>

84) What is Light? - UC Davis lecture slides, https://web.archive.org/web/20131205005843/http://cbst.ucdavis.edu/education/courses/winter-2006-IST8A/ist8a_2006_01_09light.pdf

85) The Electromagnetic Spectrum - Natural Resources Canada, <https://www.nrcan.gc.ca/maps-tools-publications/satellite-imagery-air-photos/remote-sensing-tutorials/introduction/electromagnetic-spectrum/14623>

86) Radiação Ionizante - Direção Geral de Saúde, <https://www.dgs.pt/paginas-de-sistema/saude-de-a-a-z/radiacoes-nao-ionizantes.aspx>

87) Potential health effects of exposure to electromagnetic field - European Commission, https://ec.europa.eu/health/scientific_committees/opinions_layman/electromagnetic-fields2015/en/index.htm

88) ISO 7010 W0005 - International Standard Organization Online Browsing Platform, <https://www.iso.org/obp/ui#iso:grs:7010:W005>

- 89) Sinalização de Segurança - Autoridade para as Condições do Trabalho,
[https://www.act.gov.pt/\(pt-PT\)/CentroInformacao/SinalizacaoSeguranca/Paginas/default.aspx](https://www.act.gov.pt/(pt-PT)/CentroInformacao/SinalizacaoSeguranca/Paginas/default.aspx)
- 90) The Shocking Reason France Banned Wi-Fi in Schools! - First Cry Parenting -
<https://parenting.firstcry.com/articles/the-shocking-reason-france-banned-wi-fi-in-schools/>
- 91) Not all 5G smartphones are created equal - Android Authority,
<https://www.androidauthority.com/not-all-5g-smartphones-are-equal-960791/>
- 92) Image content influences men's semen quality - PubMed.gov,
<https://www.ncbi.nlm.nih.gov/pubmed/17148180>
- 93) Effect of cell phone usage on semen analysis in men attending infertility clinic: an observational study - PubMed.gov, <https://www.ncbi.nlm.nih.gov/pubmed/17482179>
- 94) Effects of radiofrequency electromagnetic waves (RF-EMW) from cellular phones on human ejaculated semen: an in vitro pilot study - ScienceDirect,
<https://www.sciencedirect.com/science/article/abs/pii/S0015028208033566>
- 95) Evaluation of the effect of using mobile phones on male fertility - PubMed.gov,
<https://www.ncbi.nlm.nih.gov/pubmed/17655195>
- 96) Documentário alerta para excesso de exposição das crianças e adolescentes a ecrãs e as suas arrepiantes consequências – Sapo,
<https://lifestyle.sapo.pt/familia/noticias-familia/artigos/documentario-alerta-para-excesso-de-exposicao-das-criancas-e-adolescentes-a-ecras-e-as-suas-arrepiantes-consequencias>
- 97) Tempo de Ecrã – IMDB, <https://www.imdb.com/title/tt6809010/>
- 98) Geração Z está perdendo uma habilidade que temos há 5,5 mil anos: 40% estão perdendo a fluência na comunicação – IGN Portugal,
<https://br.ign.com/tech/134273/news/geracao-z-esta-perdendo-uma-habilidade-que-temos-ha-55-mil-anos-40-estao-perdendo-a-fluencia-na-comu>;
- 99) Yuval Noah Harari: Como proteger sua mente na era da informação lixo – vídeo do canal Big Think, <https://www.youtube.com/watch?v=K1OvbwY6GPM>;
- 100) Facebook addiction increases depression severity among people who are already depressed – Psy Post, <https://www.psypost.org/2022/12/facebook-addiction-increases-depression-severity-among-people-who-are-already-depressed-64586>

101) Some screen use before <https://www.newscientist.com/article/2336627-some-screen-use-before-bedtime-might-be-ok-for-your-sleep-after-all/> bedtime might be OK for your sleep after all – New Scientist,

102) Kids are waking up in the night to check their notifications and are losing about 1 night's worth of sleep a week, study suggests – Business Insider, <https://www.businessinsider.com/social-media-costing-children-one-night-sleep-study-2022-9>

103) “Phone snubbing” your partner can lead to a vicious cycle of resentment and retaliation, study suggests – Psypost, <https://www.psypost.org/2022/10/phone-snubbing-your-partner-can-lead-to-a-vicious-cycle-of-resentment-and-retaliation-study-suggests-64016>

104) The Social Dilemma – IMDB, <https://www.imdb.com/title/tt11464826/>

105) "Corremos um perigo real de perder nossas almas e nossa humanidade." – vídeo do canal Triggernometry, disponível em <https://youtube.com/shorts/IOi3HgJGhtY>;

106) Google Engineers Joked About How Incognito Mode Isn't Very Incognito – The Byte, <https://futurism.com/the-byte/google-engineers-joked-incognito-mode>

107) Apple Says Your iPhone's Usage Data is Anonymous, but New Tests Say That's Not True – Gizmodo, <https://gizmodo.com/apple-iphone-privacy-dsid-analytics-personal-data-test-1849807619>

108) Estudo revela que equipamentos inteligentes espiam-nos em casa: “As pessoas não têm ideia” – Postal, <https://postal.pt/sociedade/estudo-revela-que-equipamentos-inteligentes-espiam-nos-em-casa-as-pessoas-nao-tem-ideia/>

109) Vai nascer um clube privado de líderes em ciência de dados em Portugal – Exame Informática, <https://visao.pt/exameinformatica/noticias-ei/mercados/2023-10-31-rippy-clube-ciencia-de-dados-em-portugal/>

110) Two Republican judges just let Texas seize control of Twitter and Facebook – Vox, <https://www.vox.com/policy-and-politics/2022/9/19/23361050/supreme-court-texas-twitter-facebook-youtube-social-media-fifth-circuit-netchoice-paxton>

111) Psychology experts urge social media giants to increase transparency around algorithms to protect users’ mental health – PsyPost, <https://www.psypost.org/2022/09/psychology-experts-urge-social-media-giants-to-increase-transparency-around-algorithms-to-protect-users-mental-health-63873>

112) Meta analisa fragilidade dos jovens para exibir anúncios, diz denunciante – Notícias ao Minuto, <https://www.noticiasao minuto.com/tech/2764984/meta-analisa-fragilidade-dos-jovens-para-exibir-anuncios-diz-denunciante>

113) Let's go whaling: Tricks for monetising mobile game players with free-to-play – Youtube, <https://www.youtube.com/watch?v=xNjI03CGkb4>

114) The House Never Loses: How Microtransactions Exploit Video Game Players – Aesthetics for Birds, <https://aestheticsforbirds.com/2021/02/12/the-house-never-loses-how-microtransactions-exploit-video-game-players/>

115) Diablo Immortal reports \$100 million in revenue after 2 months - Win, <https://win.gg/news/diablo-immortal-reports-100-million-in-revenue-after-2-months/>

116) China announces rules to reduce spending on videojogos – Reuters, <https://www.reuters.com/world/china/china-issues-draft-rules-online-game-management-2023-12-22/>

117) China considers revising gaming rules after tech giants lose billions – Aljazeera, <https://www.aljazeera.com/news/2023/12/23/china-considers-revising-gaming-rules-after-tech-giants-lose-billions>

118) The Personal Brand Is Dead – The Atlantic, <https://www.theatlantic.com/technology/archive/2022/06/gen-z-internet-anonymity-instagram-tumblr/661316/>

119) Why Suffering can Promote Strength and Health – Academy of Ideas, <https://academyofideas.com/2022/06/why-suffering-can-promote-strength-health/>

120) AI can tell your race from an X-ray image — and scientists can't figure out how – National Post, <https://nationalpost.com/health/health-and-wellness/ai-can-tell-your-race-from-an-x-ray-image-and-scientists-cant-figure-out-how>

121) Scientists Increasingly Can't Explain How AI Works – Vice, <https://www.vice.com/en/article/y3pezm/scientists-increasingly-cant-explain-how-ai-works>

122) Adobe AI controversy: Why are creators ditching Adobe? - Dataquest, <https://www.dqindia.com/news/adobe-ai-controversy-why-are-creators-ditching-adobe-9656646>

123) Will AI kill all of us? | Yuval Noah Harari and Lex Fridman – Lex Clips, https://www.youtube.com/watch?v=1Gaqs1aT_ok

124) AI's first kill and why top experts predict our extinction. - Digital Engine,
https://www.youtube.com/watch?v=BcQb_8hmxSI;

125) 'The Game is Over': Google's DeepMind says it is on verge of achieving human-level AI – The Independent, <https://www.independent.co.uk/tech/ai-deepmind-artificial-general-intelligence-b2080740.html>

126) DeepMind's new AI can perform over 600 tasks, from playing games to controlling robots – Techcrunch, <https://techcrunch.com/2022/05/13/deepminds-new-ai-can-perform-over-600-tasks-from-playing-games-to-controlling-robots/>

127) Researchers Say It'll Be Impossible to Control a Super-Intelligent AI – Science Alert, <https://www.sciencealert.com/researchers-say-itll-be-impossible-to-control-a-super-intelligent-ai>

128) AI's true goal may no longer be intelligence – ZDNET, <https://www.zdnet.com/article/ai-true-goal-may-no-longer-be-intelligence/>

129) Bónus e salários de 100 milhões: Zuckerberg acusado de aliciar talentos da OpenAI com propostas milionárias – Público, <https://www.publico.pt/2025/06/23/tecnologia/noticia/bonus-salarios-100-milhoes-zuckerberg-acusado-aliciar-talentos-open-ia-propostas-milionarias-2137527>

130) Facebook Gets Results? 2010 Vote Experiment Worked, Scientists Say – CNBC, <https://www.cnn.com/2012/09/13/facebook-gets-results-2010-vote-experiment-worked-scientists-say.html>

131) What We Can Learn from Facebook's Study on Emotions – Towards Data Science, <https://towardsdatascience.com/what-we-can-learn-from-facebooks-study-on-emotions-1ec866357c0>

132) O poder do reforço intermitente – Youtube, <https://www.youtube.com/watch?v=IUXE6dooSN0>

133) Dopamine, Smartphones & You: A battle for your time – Harvard University, <https://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/>

134) Social Media Use Linked to Developing Depression Regardless of Personality - University of Arkansas, <https://news.uark.edu/articles/62109/social-media-use-linked-to-developing-depression-regardless-of-personality>

- 135) Negative impact of social media affects girls and boys at different ages – study – University of Oxford, <https://www.ox.ac.uk/news/2022-03-28-negative-impact-social-media-affects-girls-and-boys-different-ages-study>
- 136) Windows of developmental sensitivity to social media – Nature Communications, <https://www.nature.com/articles/s41467-022-29296-3>
- 137) Smartphone addiction creates imbalance in brain, study suggests – Science Daily, <https://www.sciencedaily.com/releases/2017/11/171130090041.htm>
- 138) Attention Spans – Microsoft Insights, Motamem.org, <https://dl.motamem.org/microsoft-attention-spans-research-report.pdf>
- 139) TikTok is sued over deaths of two young girls in viral ‘blackout challenge’ - Los Angeles Times, <https://www.latimes.com/business/technology/story/2022-07-01/tiktok-sued-over-death-of-two-young-girls-in-viral-blackout-challenge>
- 140) Top 10 Viral Challenges That Got People Killed – Youtube, <https://www.youtube.com/watch?v=K1YCGYIY6jc>
- 141) TikTok is Poisoning Society – Youtube, <https://www.youtube.com/watch?v=qbv-VteX5H8>
- 142) Neurodevelopment, impulsivity, and adolescent gambling - PubMed.gov, <https://pubmed.ncbi.nlm.nih.gov/12635540/>
- 143) Revealed: UK children being ensnared by ‘far-right ecosystem’ online – The Guardian, <https://www.theguardian.com/politics/2022/aug/03/revealed-uk-children-ensnared-far-right-ecosystem-online>
- 144) Confinamento e teletrabalho: Síndrome Visual do Computador – Trofa Saúde, <https://www.trofasaude.pt/noticias-e-eventos/noticias/confinamento-e-teletrabalho-s%C3%ADndrome-visual-do-computador/>
- 145) Feds step up focus on companies’ use of dark patterns - Legal Dive, <https://www.legaldive.com/news/ftc-enforcement-dark-patterns-online-manipulation-ccpa-rosca-Husch-Blackwell/633962>
- 146) Bringing Dark Patterns to Light – FTC, https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%2009.14.2022%20-%20FINAL.pdf

147) President Biden wants to ban advertising targeted toward kids – Internet Archive (Engadget), <https://web.archive.org/web/20220302130245/https://www.engadget.com/biden-wants-to-ban-advertising-targeted-toward-kids-052140748.html>

148) Kids Online Safety Act Bill – Senator Blackburn, <https://www.blackburn.senate.gov/services/files/6ADC7E78-4965-4DA8-88AA-72862CB64AC9>

149) The Kids Online Safety Act Is a Heavy-Handed Plan to Force Platforms to Spy on Young People – Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2022/03/kids-online-safety-act-heavy-handed-plan-force-platforms-spy-young-people>

150) New California bill requires social media companies to prioritise children's mental health – Chemhelps, <https://chemhelps.com/new-california-bill-requires-social-media-companies-to-prioritise-childrens-mental-health/>

151) Governor Newsom Signs First-in-Nation Bill Protecting Children's Online Data and Privacy – Office of Governor Gavin Newsom, <https://www.gov.ca.gov/2022/09/15/governor-newsom-signs-first-in-nation-bill-protecting-childrens-online-data-and-privacy/>

152) NY's sweeping child privacy bill would force online security measures — but Big Tech battle brews - New York Post, <https://nypost.com/2022/09/25/ny-introduces-sweeping-child-privacy-bill-to-make-kids-safer-online/>

153) Congress quizzes Facebook whistleblower on potential Section 230 reforms - Internet Archive (Engadget), <https://web.archive.org/web/20220302075428/https://www.engadget.com/congress-quizzes-facebook-whistleblower-on-section-230-reforms-203605272.html>

154) Tech spent big on lobbying last year – Politico, <https://www.politico.com/newsletters/morning-tech/2022/01/24/tech-spent-big-on-lobbying-last-year-00001144>

155) Corporate lobbying could imperil sweeping data privacy bill - The Hill, <https://thehill.com/business-a-lobbying/3585322-corporate-lobbying-could-imperil-sweeping-data-privacy-bill/>

156) Proton and DuckDuckGo want Congress to approve tech antitrust reform 'as soon as possible' – The Verge, <https://www.theverge.com/2022/9/13/23351036/proton-mail-duckduckgo-mozilla-schumer-aico-antitrust-amazon-google>

157) U.S tech giants face tough new rules as EU countries, lawmakers clinch deal – Reuters, <https://www.reuters.com/world/europe/eu-countries-eu-lawmakers-clinch-deal-rules-rein-tech-giants-2022-03-24/>

158) New rules for U.S tech giants to come into force in October, EU's Vestager says – Reuters, <https://www.reuters.com/technology/rules-against-us-tech-giants-come-into-force-october-eus-vestager-says-2022-03-25/>

159) 5G Cell Towers: Why You See Them And How They Work - Lifewire, <https://www.lifewire.com/5g-cell-towers-4584192>

160) What are small cells in 5G technology – RF Page, <https://www.rfpage.com/what-are-small-cells-in-5g-technology/>

161) Mobile Phone Base Stations, How do mobile base stations work, Mobile Base Stations In Australia, Cell Tower, Mobile Phone Tower - Mobile Network Guide, https://mobilenetworkguide.com.au/mobile_base_stations.html

162) Analyst Angle: The rise and outlook of antennas in 5G - RCR Wireless News, <https://www.rcrwireless.com/20180624/wireless/analyst-angle-the-rise-and-outlook-of-antennas-in-5g>

163) A Possible Effect of Electromagnetic Radiation from Mobile Phone Base Stations on the Number of Breeding House Sparrows (*Passer domesticus*) (estudo de Joris Everaert e Dirk Bauwens 2007), <http://iddd.de/umtsno/lebewesen/EveraerBauwenssparrows.pdf>

164) Will 5G Affect Weather Forecasts? - BBC Click, https://www.youtube.com/watch?v=l_Ffl7pJxRI

165) 5G wireless networks threaten weather forecasts, NCAR expert tells Congress – UCAR, <https://news.ucar.edu/132801/5g-wireless-networks-threaten-weather-forecasts-ncar-expert-tells-congress>

166) Spectrum Needs for Observations in Earth and Space Sciences - US House of Representatives Committee on Science, Space and Technology, <https://science.house.gov/hearings/spectrum-needs-for-observations-in-earth-and-space-sciences>

167) 5G pode afetar as previsões meteorológicas! Saiba porquê... - pplware, <https://pplware.sapo.pt/internet/5g-pode-afetar-as-previsoes-meteorologicas-saiba-porque/>

168) Dirigentes de companhias aéreas dos EUA preocupados com interferências do 5G – Expresso, <https://expresso.pt/economia/2022-01-18-dirigentes-de-companhias-aereas-dos-eua-preocupados-com-interferencias-do-5g>

169) 'Make or break' moment for 5G - BBC News, <https://www.bbc.co.uk/news/technology-50208391>

170) **Session:** Joint Panel Discussion 1 The Wizard Behind the Curtain?—The Important, Diverse, and Often Hidden Role of Spectrum Allocation for Current and Future Environmental Satellites and Water, Weather, and Climate - AMS100

171) Critical weather data threatened by FCC ‘spectrum’ proposal, Commerce Dept. and NASA say - Washington Post, <https://www.washingtonpost.com/gdpr-consent/?destination=%2fweather%2f2019%2f03%2f08%2fcritical-weather-data-threatened-by-fcc-spectrum-proposal-say-department-commerce-nasa%2f%3f>

172) FCC to auction off wireless spectrum that could interfere with vital weather data, rejecting requests from U.S. House and science agencies - Washington Post, <https://www.washingtonpost.com/weather/2019/03/13/fcc-auction-off-wireless-spectrum-that-could-interfere-with-vital-weather-data-rejecting-requests-us-house-science-agencies/>

173) Electromagnetic hypersensitivity Wikipedia, https://en.wikipedia.org/wiki/Electromagnetic_hypersensitivity

174) O silêncio médico e os factos - MOPPE, <https://electrosmogportugal.weebly.com/blogue/o-silencio-medico-e-os-factos>

175) Dr. Sharon Goldberg Testifies at Michigan's 5G Small Cell Tower Legislation Hearing October 4, 2018, <https://www.youtube.com/watch?v=CK0AliMe-KA&feature=youtu.be>

176) Biological Effects of Low-intensity Radiofrequency Electromagnetic Radiation, https://www.weebly.com/uploads/1/2/3/3/123313372/acute_radiation_syndrome_conference_2017.pdf

177) Os efeitos imediatos da poluição electromagnética - MOPPE, <https://electrosmogportugal.weebly.com/blogue/os-efeitos-imediatos-da-poluicao-electromagnetica>

178) Live Blood & Electrosmog - Doutora Magda Havas, <https://www.youtube.com/watch?v=L7E36zGHxRw>

179) Dr. Magda Havas, PhD., <https://magdahavas.com/>

- 180) Dark Field Microscopy sees damage | TBYP 2017 Smart Meter documentary - Clarity, https://www.youtube.com/watch?v=4edIIisEj4w&feature=emb_title
- 181) Micro Wave Auditory Effect - Wikipedia, https://en.wikipedia.org/wiki/Microwave_auditory_effect
- 182) Human Skin as Arrays of Helical Antennas in the Millimeter and Submillimeter Wave Range – ResearchGate, https://www.researchgate.net/publication/51394628_Human_Skin_as_Arrays_of_Helical_Antennas_in_the_Millimeter_and_Submillimeter_Wave_Range
- 183) The human skin as a sub-THz receiver – Does 5G pose a danger to it or not? - Science Direct, <https://www.sciencedirect.com/science/article/abs/pii/S0013935118300331>
- 184) Specific Absorption Rate - Wikipedia, https://en.wikipedia.org/wiki/Specific_absorption_rate
- 185) Martin Pall's book on 5G is available online - EM Facts, <https://www.emfacts.com/2018/08/martin-palls-book-on-5g-is-available-online/>
- 186) "[Public Health](#)" (PDF) - European Commission
- 187) Dr George Carlo: The Wireless Industry is Committing Scientific Fraud - Electromagnetic Radiation Health Effects, https://www.youtube.com/watch?v=vsv0k5zvRXA&feature=emb_logo
- 188) At Senate Commerce Hearing, Blumenthal Raises Concerns on 5G Wireless Technology's Potential Health - Richard Blumenthal United States Senator for Connecticut [website pessoal], <https://www.blumenthal.senate.gov/newsroom/press/release/at-senate-commerce-hearing-blumenthal-raises-concerns-on-5g-wireless-technologys-potential-health-risks>
- 189) The Epidemiology of Cancer Among Police Officers - National Center for Biotechnology Information, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3655699/>
- 190) Speed Radar - Cop Radar, <https://copradar.com/chapts/chapt1/ch1d1.html>
- 191) Electromagnetic fields and public health - World Health Organization, <https://www.who.int/peh-emf/publications/facts/fs296/en/>
- 192) [US Senator Richard] Blumenthal Urges Cancer Study of 5G Technology - Associated Press, <https://apnews.com/c08591eb274a4095a4d0fba37a17a61d>

- 193) Effects of heat on embryos and foetuses (artigo de M. J. Edwards, R. D. Saunders & K. Shiota 2003) - Taylor & Francis Group,
<https://www.tandfonline.com/doi/pdf/10.1080/0265673021000039628>
- 194) Don't Want Hair Loss? Short-term Exposure to Cell Phone Radiation Can Cause DNA Damage in Hair-Root Cells - Activist Post, <https://www.activistpost.com/2020/05/dont-want-hair-loss-short-term-exposure-to-cell-phone-radiation-can-cause-dna-damage-in-hair-root-cells.html>
- 195) Single-strand DNA breaks in human hair root cells exposed to mobile phone radiation - Taylor & Francis Online,
<https://www.tandfonline.com/doi/abs/10.3109/09553002.2012.666005>
- 196) W. Ross Adey's research works | University of California, Riverside, CA(UCR) and other places ResearchGate,
https://www.researchgate.net/scientific-contributions/2089555399_W_Ross_Adey
- 197) Genetic susceptibility may modify the association between cell phone use and thyroid cancer: A population-based case-control study in Connecticut - Science Direct,
<https://www.sciencedirect.com/science/article/abs/pii/S0013935119308102>
- 198) Scientific American: "We Have No Reason To Believe 5G Is Safe" - Humans Are Free, <http://humansarefree.com/2019/11/scientific-american-we-have-no-reason.html>
- 199) We Have No Reason to Believe 5G Is Safe – Scientific American,
<https://blogs.scientificamerican.com/observations/we-have-no-reason-to-believe-5g-is-safe/>
- 200) What Are Free Radicals? - Live Science, <https://www.livescience.com/54901-free-radicals.html>
- 201) How does oxidative stress affect the body? - Medical News Today,
<https://www.medicalnewstoday.com/articles/324863>
- 202) Pineal melatonin level disruption in humans due to electromagnetic fields and ICNIRP limits – Pub Med, <https://pubmed.ncbi.nlm.nih.gov/23051584/>
- 203) Critical time delay of the pineal melatonin rhythm in humans due to weak electromagnetic exposure – Pub Med, <https://pubmed.ncbi.nlm.nih.gov/24772943/>
- 204) Evidence for an effect of ELF electromagnetic fields on human pineal gland function – Pub Med, <https://pubmed.ncbi.nlm.nih.gov/2096195/>
- 205) Pineal Gland – Britannica, <https://www.britannica.com/science/pineal-gland>

- 206) 5G Health Effects: Is This Wireless Technology Even Safe? - Dr. Axe,
<https://draxe.com/health/5g-health-effects/>
- 207) Systematic Derivation of Safety Limits for Time-Varying 5G Radiofrequency Exposure Based on Analytical Models and Thermal Dose, National Center for Biotechnology Information - <https://www.ncbi.nlm.nih.gov/pubmed/30247338>
- 208) How does a microwave oven heat up food even though it emits no thermal radiation? - Science Questions with Surprising Answers,
<https://wtamu.edu/~cbaird/sq/mobile/2013/05/16/how-does-a-microwave-oven-heat-up-food-even-though-it-emits-no-thermal-radiation/>
- 209) 2018 | 5G: Grande risco para a UE, EUA e Saúde internacional! de 8 tipos distintos de grandes danos causados por exposição a campos eletromagnéticos (EMF) e o mecanismo que os causam,
https://electrosmogportugal.weebly.com/uploads/1/2/3/3/123313372/resumo_martinpall-5g-grande_risco.pdf
- 210) The First Report of 5G Injury from Switzerland - Physicians for Safe Technology,
<https://mdsafetech.org/2019/07/20/the-first-report-of-5g-injury-from-switzerland/>
- 211) Scientists Warn of Health Effects: Washington DC Council 5G Small Cell Roundtable - Youtube, <https://www.youtube.com/watch?v=ljLynbr5iPc>
- 212) Part 1 - Impacts of Wireless Technology on Health - Frank Clegg intro and Dr. Riina Bray, <https://www.youtube.com/watch?v=F2urAWw7kx4>
- 213) EUROPAEM EMF Guideline 2016 for the prevention, diagnosis and treatment of EMF-related health problems and illnesses - De Gruyter,
https://www.degruyter.com/view/journals/reveh/31/3/article-p363.xml#ref_j_reveh-2016-0011_ref_019_w2aab3b8c20b1b7b1ab2ac19Aa
- 214) Cancer epidemiology update, following the 2011 IARC evaluation of radiofrequency electromagnetic fields (Monograph 102) – Science Direct,
<https://www.sciencedirect.com/science/article/abs/pii/S0013935118303475>
- 215) faq's - Radiações e Saúde - faqtos, <https://www.faqtos.pt/index.php?id=22&cat=13>
- 216) Magnetic Fields - Europa,
https://ec.europa.eu/health/scientific_committees/opinions_layman/en/electromagnetic-fields07/index.htm

217) The Feds Try To End the Debate Over 5G Health Concerns - Data Sheet - Fortune, <https://www.fortune.com/2019/08/09/the-feds-try-to-end-the-debate-over-5g-health-concerns-data-sheet/>

218) 5G Dangers: What the Experts Say About Health Risks - Tom's Guide, <https://www.tomsguide.com/special-report/5g-health-risk>

219) 5G phones and your health: What you need to know - CNET, <https://www.cnet.com/news/5g-phones-and-your-health-what-you-need-to-know/>

220) Ministério da Saúde anuncia “estudo aprofundado” sobre excessos de mortalidade – Público, <https://www.publico.pt/2022/08/12/sociedade/noticia/ministerio-saude-anuncia-estudo-aprofundado-excessos-mortalidade-2017091>

221) Forecast number of mobile users worldwide from 2020 to 2025 (in billions) – Statista, <https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/>

222) Swiss Re SONAR: New emerging risk insights – Environmental Health Trust, <https://ehtrust.org/wp-content/uploads/Swiss-Re-SONAR-Publication-2019-excerpt-1.pdf>

223) SONAR 2020: New emerging risk insights – Swiss Re Institute, <https://www.swissre.com/institute/research/sonar/sonar2020.html>

224) SONAR 2021: New emerging risk insights – Swiss Re Institute, <https://www.swissre.com/institute/research/sonar/sonar2021.html>

225) PORDATA – Estatísticas, gráficos e indicadores de Municípios, Portugal e Europa – PORDATA, <https://www.pordata.pt/>

226) ISPs can now collect and sell your data: What to know about Internet privacy rules – USA Today, <https://eu.usatoday.com/story/tech/news/2017/04/04/isps-can-now-collect-and-sell-your-data-what-know-internet-privacy/100015356/>

227) Will pay-for-privacy be the new normal? - Malwarebytes, <https://blog.malwarebytes.com/security-world/privacy-security-world/2019/02/will-pay-privacy-new-normal/>

228) AT&T is putting a price on privacy. That is outrageous – The Guardian, <https://www.theguardian.com/commentisfree/2015/feb/20/att-price-on-privacy>

229) When will Democrats deliver on their promise to restore net neutrality? - Fast Company, <https://www.fastcompany.com/90752261/when-will-democrats-restore-net-neutrality>

230) North Korea's Lazarus brings state-sponsored hacking approach to ransomware – Ars Technica, <https://arstechnica.com/information-technology/2020/07/north-korea-backed-hackers-dip-their-toes-into-the-ransomware-pool/>

231) Other articles by Alfonso Balmori - Cellular Phone Task Force
<https://www.cellphonetaskforce.org/other-articles-by-alfonso-balmori/>

232) Mobile Phone Mast Effects on Common Frog (Rana temporaria) Tadpoles: The City Turned into a Laboratory - Connecticut's Official State Website,
http://www.ct.gov/csc/lib/csc/pendingproceeds/docket_409/inlandwetland/409-iw_exh69-79.pdf#page=2

233) Statement on emerging health and environmental issues (2018) – European Commission,
<https://op.europa.eu/o/opportal-service/download-handler?identifier=37af1376-3978-11e9-8d04-01aa75ed71a1&format=pdf&language=en&productionSystem=cellar&part=>

234) Autarquia de Famalicão autoriza antena de telecomunicações ao lado da Escola D. Maria II – Eduprofs, <https://eduprofs.blogspot.com/2019/12/autarquia-de-famalicao-autoriza-antena.html>

235) 5G uses less power than 4G at peak bitrates, but more for basic tasks - VentureBeat,
<https://venturebeat.com/2019/09/11/5g-uses-less-power-than-4g-at-peak-bitrates-but-more-for-basic-tasks/>

236) Power Consumption: 5G Basestations Are Hungry, Hungry Hippos - Light Reading,
<https://www.lightreading.com/mobile/5g/power-consumption-5g-basestations-are-hungry-hungry-hippos/d/d-id/749979>

237) 5G Waveform Is A Battery Vampire - IEEE Spectrum,
<https://spectrum.ieee.org/telecom/wireless/5g-waveform-is-a-battery-vampire>

238) 5G May Drain Batteries, While Base Stations Will Require Three Times As Much Power - Slashdot, <https://hardware.slashdot.org/story/19/07/27/1924244/5g-may-drain-batteries-while-base-stations-will-require-three-times-as-much-power>

239) 5G base stations use a lot more energy than 4G base stations: MTN - Fierce Wireless,
<https://www.fiercewireless.com/tech/5g-base-stations-use-a-lot-more-energy-than-4g-base-stations-says-mtn>

240) 'Tsunami of data' could consume one fifth of global electricity by 2025 - The Guardian, <https://www.theguardian.com/environment/2017/dec/11/tsunami-of-data-could-consume-fifth-global-electricity-by-2025>

- 241) Technology: University of New Mexico researchers find Bitcoin mining is environmentally unsustainable – EurekAlert!,
<https://www.eurekalert.org/news-releases/966192>
- 242) 5G Heats Up Base Stations – Semiconductor Engineering,
<https://semiengineering.com/5g-heats-up-base-stations/>
- 243) Nokia touts 30% base station energy savings with 5G cooling tech - Fierce Wireless,
<https://www.fiercewireless.com/wireless/nokia-touts-30-base-station-energy-cost-savings-5g-cooling-tech>
- 244) Total Consumer Power Consumption Forecast - Research Gate,
https://www.researchgate.net/publication/320225452_Total_Consumer_Power_Consumption_Forecast
- 245) The Real Reason Your Power Bill Doubled (It's Not Inflation) – canal de Youtube de Vanessa Wingårdh, https://www.youtube.com/watch?v=hJ2tqs_vksc
- 246) How AI uses our drinking water - BBC World Service – vídeo do canal de Youtube BBC World Service, <https://www.youtube.com/watch?v=b0C56yqIkBk>
- 247) Why data centers are eating up enormous water resources | Transforming Business – vídeo do canal de Youtube DW News, https://www.youtube.com/watch?v=cl1ctf1_JxE
- 248) Oracle Accused of Invading Privacy with Tracking Technologies – Robinson + Cole,
<https://www.dataprivacyandsecurityinsider.com/2022/08/oracle-accused-of-invading-privacy-with-tracking-technologies/>
- 249) Oracle Sued By Privacy Advocates Over Data Collection Practices – CRN,
<https://www.crn.com/news/cloud/oracle-sued-by-privacy-advocates-over-data-collection-practices?itc=refresh>
- 250) Oracle faces class-action lawsuit for ‘tracking’ five billion people – Independent.ie,
<https://www.independent.ie/business/technology/oracle-faces-class-action-lawsuit-for-tracking-five-billion-people-41928438.html>
- 251) Class action against Oracle’s worldwide surveillance machine – Irish Council for Civil Liberties, <https://www.iccl.ie/news/class-action-against-oracle/>
- 252) Oracle Boasted That Its Software Was Used Against U.S. Protesters. Then It Took the Tech to China. - The Intercept, <https://theintercept.com/2021/05/25/oracle-social-media-surveillance-protests-endeca/>

253) Oracle admits to spying on Microsoft, Ellison takes responsibility – ITPro Today, <https://www.itprotoday.com/windows-8/oracle-admits-spying-microsoft-ellison-takes-responsibility>

254) A close look at how Oracle installs deceptive software with Java updates – ZDNET, <https://www.zdnet.com/article/a-close-look-at-how-oracle-installs-deceptive-software-with-java-updates/>

255) Did you know that Oracle owns the trademark to Javascript? - Dev, <https://dev.to/theoutlander/oracle-owns-the-trademark-to-javascript-1fil>

256) How TikTok Tracks You Across the Web, Even If You Don't Use the App – Consumer Reports, <https://www.consumerreports.org/electronics-computers/privacy/tiktok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813/>

257) What is a Tracking Pixel? - Cookie Script, <https://cookie-script.com/blog/tracking-pixel>

258) TikTok is "unacceptable security risk" and should be removed from app stores, says FCC – Malware Bytes Labs, <https://www.malwarebytes.com/blog/news/2022/07/tiktok-is-unacceptable-security-risk-and-should-be-removed-from-app-stores-says-fcc>

259) TikTok admits to spying on U.S. users as effort to ban the app heats up – Mashable, <https://mashable.com/article/tiktok-spying-internal-report-us-users>

260) Coalition Tells FTC to Curb Amazon 'Surveillance Empire' by Blocking Purchase of iRobot – Common Dreams, <https://www.commondreams.org/news/2022/09/09/coalition-tells-ftc-curb-amazon-surveillance-empire-blocking-purchase-irobot>

261) Grindr sold users' location data for years, may have outed Catholic priest: report - New York Post, <https://nypost.com/2022/05/02/grindr-sold-data-about-users-precise-locations-for-years-report/>

262) Advertising ID – Google, <https://support.google.com/googleplay/android-developer/answer/6048248?hl=en>

263) FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook – FTC, <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>

264) Twitter will pay a \$150 million fine over accusations it improperly sold user data – NPR, <https://www.npr.org/2022/05/25/1101275323/twitter-privacy-settlement-doj-ftc>

- 265) Ireland fines Instagram a record \$400 mln over children's data – Reuters, <https://www.reuters.com/technology/irish-regulator-fines-instagram-400-million-over-chidrens-data-2022-09-05/>
- 266) S.Korea fines Google, Meta billions of won for privacy violations – Reuters, <https://www.reuters.com/technology/skorea-fines-google-meta-over-accusations-privacy-law-violations-yonhap-2022-09-14/>
- 267) TikTok could face £27m fine for failing to protect children's privacy – The Guardian, <https://www.theguardian.com/technology/2022/sep/26/tiktok-fine-protect-children-privacy-uk-data-protection>
- 268) Meta faces mounting questions from Congress on health data privacy as hospitals remove Facebook tracker – STAT, <https://www.statnews.com/2022/09/19/facebook-meta-pixel-congress-health-data/>
- 269) Lawsuit accuses Meta of secretly tracking Facebook users' internet activity without consent – San Francisco Chronicle, <https://www.sfchronicle.com/bayarea/article/Lawsuit-accuses-Meta-of-secretly-tracking-17471245.php>
- 270) Texas sues Google for allegedly capturing biometric data of millions without consent – Reuters, <https://www.reuters.com/legal/texas-sues-google-allegedly-capturing-biometric-data-millions-without-consent-2022-10-20/>
- 271) Migration to the metaverse: We need guaranteed basic Immersive Rights – Delaware Digital News, <https://delawaredigitalnews.com/migration-to-the-metaverse-we-need-guaranteed-basic-immersive-rights>
- 272) Mozilla: Lack of Security Protections in Mental-Health Apps Is 'Creepy' – Threat Post, <https://threatpost.com/mozilla-security-health-apps-creepy/179463/>
- 273) Inside the harrowing world of online student surveillance – Fast Company, <https://www.fastcompany.com/90748240/gaggle-school-content-moderation-privacy>
- 274) Kids Are Back in Classrooms and Laptops Are Still Spying on Them – Wired, <https://www.wired.com/story/student-monitoring-software-privacy-in-schools/>
- 275) In-person teaching has resumed in the US – but electronic snooping hasn't stopped – The Guardian, <https://www.theguardian.com/commentisfree/2022/aug/06/school-surveillance-software-students-week-in-patriarchy>

- 276) Hidden Harms – Center for Democracy and Technology,
<https://cdt.org/wp-content/uploads/2022/08/Hidden-Harms-The-Misleading-Promise-of-Monitoring-Students-Online-Research-Summary-Final-Accessible.pdf>
- 277) The risks of student surveillance amid abortion bans and LGBTQ restrictions – The Guardian, <https://www.theguardian.com/education/2022/sep/08/abortion-bans-school-surveillance-lgbtq-restrictions>
- 278) Big Brother isn't just watching: workplace surveillance can track your every move – The Guardian, <https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology>
- 279) Subjecting workers to webcam monitoring violates privacy, Dutch court rules – The Verge, <https://www.theverge.com/2022/10/10/23396461/remote-worker-webcam-on-all-day-dutch-court-employee-rights-privacy>
- 280) Vodafone & Deutsche Telekom to introduce persistent user tracking – Simple Analytics Blog, <https://blog.simpleanalytics.com/vodafone-deutsche-telekom-to-introduce-persistent-user-tracking>
- 281) Rise of worker surveillance software – Digital Futures at Work Research Center, https://digit-research.org/blog_article/rise-of-worker-surveillance-software/
- 282) Video Doorbell Cameras Record Audio, Too – Consumer Reports, <https://www.consumerreports.org/video-doorbells/video-doorbell-cameras-record-audio-too-a4636115889/>
- 283) America's Ring doorbell camera obsession highlights the scourge of mass surveillance – NBC News, <https://www.nbcnews.com/think/opinion/amazons-ring-doorbell-videos-make-america-less-safe-crime-rcna55143>
- 284) If You've Got a New Car, It's a Data Privacy Nightmare – Gizmodo, <https://gizmodo.com/mozilla-new-cars-data-privacy-report-1850805416>
- 285) The Dark Future of Relationships – Youtube, <https://www.youtube.com/watch?v=gu1FS98pFrI>
- 286) Democracia portuguesa cai a pique em índice de avaliação dos cidadãos – Diário de Notícias, <https://www.dn.pt/politica/democracia-portuguesa-cai-a-pique-em-indice-de-avaliacao-dos-cidadaos-17268180.html>
- 287) Crime Ciberdependente – Apoio à Vítima, <https://www.apav.pt/cibercrime/>

- 288) 5G: Operadoras devem pensar "criticamente" segurança - TECHAOMINUTO, <https://www.noticiasominuto.com/tech/1348066/5g-operadoras-devem-pensar-criticamente-seguranca>
- 289) 5G: Estados-membros detetam riscos de espionagem e de ciberataques vindos de fora da Europa - Observador, <https://observador.pt/2019/10/09/5g-estados-membros-detetam-riscos-de-espionagem-e-de-ciberataques-vindos-de-fora-da-ue/>
- 290) How to Prepare for the Coming 5G Threats - SecurityIntelligence, <https://securityintelligence.com/how-to-prepare-for-the-coming-5g-security-threats/>
- 291) Security concerns in a 5G era: are networks ready for massive DDoS attacks? - SC Media, <https://www.scmagazineuk.com/security-concerns-5g-era-networks-ready-massive-ddos-attacks/article/1584554>
- 292) The Urgency of Network Security in the Shared LTE/5G Era – A10, <https://www.a10networks.com/blog/the-urgency-of-network-security-in-the-shared-lte-5g-era/>
- 293) "Pandemia está a originar o maior volume de ciberataques que já vimos" - Público, <https://www.publico.pt/2020/03/31/tecnologia/noticia/pandemia-originar-maior-volume-ciberataques-ja-vimos-1910028>
- 294) Com Portugal confinado, cibercrime cresce até 300% - Expresso, <https://expresso.pt/sociedade/2020-04-26-Com-Portugal-confinado-cibercrime-cresce-ate-300>
- 295) Vodafone: ataques informáticos aumentaram 81% só no ano passado – CNN Portugal, <https://cnnportugal.iol.pt/videos/vodafone-ataques-informaticos-aumentaram-81-so-no-ano-passado/6203cc9a0cf2c7ea0f18173a>
- 296) Security researcher discloses four IBM zero-days after company refused to patch - ZD Net, <https://www.zdnet.com/article/security-researcher-discloses-four-ibm-zero-days-after-company-refused-to-patch/>
- 297) Why The Largest Cyberattack In History Will Happen Within Six Months - Forbes, <https://www.forbes.com/sites/stephenmcbride1/2020/05/14/why-the-largest-cyberattack-in-history-will-happen-within-six-months/#49518c61577c>
- 298) “As responsabilidades das empresas. Um novo compromisso...” - Notícias Maia, <https://www.noticiasmaia.com/as-responsabilidades-das-empresas-um-novo-compromisso/>

299) A call to SMEs: Focus on cyber security or face more fallout from Covid-19 - Stuff, <https://www.stuff.co.nz/business/prosper/advice/121389256/a-call-to-smes-focus-on-cyber-security-or-face-more-fallout-from-covid19>

300) Aumentam os ataques cibernéticos a estruturas essenciais e até hospitais SIC Notícias, <https://sicnoticias.pt/pais/2020-04-17-Aumentam-os-ataques-ciberneticos-a-estruturas-essenciais-e-ate-hospitais>

301) How Coronavirus is Impacting Cyberspace - Ciso Mag, <https://www.cisomag.com/cyberthreats-due-to-coronavirus/>

302) EDP: só a arquitetura de rede impediu um apagão geral durante ataque de hackers - Exame Informática, <https://visao.sapo.pt/exameinformatica/noticias-ei/internet/2020-04-22-edp-so-a-arquitetura-de-rede-impediu-um-apagao-geral-durante-ataque-de-hackers/>

303) Cyberteam reivindicou ataque, mas Altice garante que não teve sucesso - Exame Informática, <https://visao.sapo.pt/exameinformatica/noticias-ei/internet/2020-04-16-cyberteam-reivindicou-ataque-mas-altice-garante-que-nao-teve-sucesso/>

304) Ciberataques à EDP e Altice expõem ofensiva global contra estruturas críticas - Público, <https://www.publico.pt/2020/04/28/tecnologia/noticia/ciberataques-edp-altice-expoem-ofensiva-global-estruturas-criticas-1914015>

305) CyberTeam. Quem são os piratas que hackearam a EDP e a Altice e ameaçam um mega ataque dia 25 de abril - Observador, <https://observador.pt/especiais/cyberteam-quem-sao-os-piratas-que-hackearam-a-edp-e-a-altice-e-ameacam-um-mega-ataque-dia-25-de-abril/>

306) Vodafone continua a recuperar de ataque informático – RTP Notícias, https://www.rtp.pt/noticias/economia/vodafone-continua-a-recuperar-de-ataque-informatico_n1383110

307) Ciberataque à Vodafone causa constrangimentos na rede multibanco – SIC Notícias, <https://sicnoticias.pt/pais/ciberataque-a-vodafone-causa-constrangimentos-na-rede-multibanco/>

308) Ciberataque à Vodafone: ainda há serviços afetados – SIC Notícias, <https://sicnoticias.pt/pais/ciberataque-a-vodafone-ainda-ha-servicos-afetados/>

309) Da energia à banca, onde chegou o ataque à Vodafone - Jornal de Negócios, <https://www.jornaldenegocios.pt/empresas/telecomunicacoes/detalhe/da-energia-a-banca-onde-chegou-o-ataque-a-vodafone>

310) Ataque informático. Vodafone notifica Comissão Nacional de Proteção de Dados de violação de dados pessoais - Observador,
<https://observador.pt/programas/noticiario/vodafone-notifica-cnpd-de-violacao-de-dados-pessoais/#>

311) Ataque à Vodafone. Espionagem industrial é uma das pistas - Sapo,
https://online.sapo.pt/artigo/761772/ataque-a-vodafone-espionagem-industrial-e-uma-das-pistas?-seccao=Portugal_i

312) Ciberataque à Vodafone: PJ segue pista de hacker russo – Jornal de Negócios,
<https://www.jornaldenegocios.pt/empresas/telecomunicacoes/detalhe/ciberataque-a-vodafone-pj-segue-pista-de-hacker-russo>

313) Clientes Vodafone queixam-se que estão a aparecer números gravados que não foram adicionados por eles – Cidade Hoje, <https://cidadehoje.pt/clientes-vodafone-queixam-se-que-estao-a-aparecer-numeros-gravados-que-nao-foram-adicionados-por-eles/>

314) Portugal está a ser “um alvo da moda” nos ciberataques, diz a Oni - Público,
<https://www.publico.pt/2022/02/11/economia/noticia/portugal-alvo-moda-ciberataques-oni-1995135>

315) Hackers publicam dados de clientes da TAP. Moradas, nomes e telefones entre informação divulgada - Público,
<https://www.publico.pt/2022/09/13/sociedade/noticia/hackers-publicam-dados-clientes-tap-moradas-nomes-telefones-informacao-divulgada-2020350>

316) Piratas publicam dados de 1,5 milhões de clientes e dizem ter acesso remoto a sistemas da TAP – Expresso, https://expresso.pt/life_style/ciencia/2022-09-19-Piratas-publicam-dados-de-15-milhoes-de-clientes-e-dizem-ter-acesso-remoto-a-sistemas-da-TAP-bb9f28ef

317) Menos de 1% das empresas portuguesas têm seguros de proteção contra ciberataques, diz consultora – Observador, <https://observador.pt/2022/02/11/menos-de-1-das-empresas-portuguesas-tem-seguros-de-protecao-contr-ciberataques-diz-consultora/>

318) Japan faces Asahi beer shortage after cyber-attack – MSN, <https://www.msn.com/en-us/money/companies/japan-faces-asahi-beer-shortage-after-cyber-attack/ar-AA1NLOqk>

319) Evolution of Hoaxcalls - radware,
<https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/hoaxcalls-evolution/>

320) This new variant of Mirai botnet malware is targeting network-attached storage devices - ZD Net, <https://www.zdnet.com/article/this-new-variant-of-mirai-botnet-malware-is-targeting-network-attached-storage-devices/>

321) Dark_nexus botnet outstrips other malware with new, potent features - ZD Net, <https://www.zdnet.com/article/new-dark-nexus-botnet-outstrips-others-with-original-advanced-capabilities/>

322) New Kaiji malware targets IoT devices via SSH brute-force attacks - ZD Net, <https://www.zdnet.com/article/new-kaiji-malware-targets-iot-devices-via-ssh-brute-force-attacks/>

323) Putin's Secret Intelligence Agency Hacked: Dangerous New 'Cyber Weapons' Now Exposed - Forbes, <https://www.forbes.com/sites/zakdoffman/2020/03/21/putins-secret-intelligence-agency-hacked-dangerous-new-cyber-weapons-target-your-devices/#3bd6c522778a>

324) The US Secret Service Issues Ransomware Warning – Cointelegraph, <https://cointelegraph.com/news/the-us-secret-service-issues-ransomware-warning>

325) US cyber-attack: Around 50 firms 'genuinely impacted' by massive breach – BBC, <https://www.bbc.com/news/world-us-canada-55386947>

326) Big tech companies including Intel, Nvidia, and Cisco were all infected during the SolarWinds hack – The Verge, <https://www.theverge.com/2020/12/21/22194183/intel-nvidia-cisco-government-infected-solarwinds-hack>

327) SolarWinds hack officially blamed on Russia: What you need to know – CNET, <https://www.cnet.com/news/solarwinds-hack-officially-blamed-on-russia-what-you-need-to-know/>

328) SolarWinds hackers accessed Microsoft source code, the company says – CNBC, <https://www.cnbc.com/2021/01/01/solarwinds-hackers-accessed-microsoft-source-code-the-company-says.html#close>

329) Microsoft breach may have affected 65,000 companies in 111 countries – Windows Central, <https://www.windowscentral.com/microsoft/microsoft-breach-may-have-affected-65000-people-in-111-countries>

330) More Than 80% of Cyberattacks Worldwide Happening in Russia or Ukraine – Nextgov, <https://www.nextgov.com/cybersecurity/2022/03/more-80-cyberattacks-worldwide-happening-russia-or-ukraine/362964/>

- 331) Security researchers from ESET reported that the Russia-linked APT group Sandworm continues to target Ukraine. - Security Affairs, <https://securityaffairs.co/wordpress/131523/apt/sandworm-attacks-against-ukraine.html>
- 332) White House Warns Companies to Encrypt Data in Case of Russian Cyberattack – Newsweek, <https://www.msn.com/en-us/news/technology/white-house-warns-companies-to-encrypt-data-in-case-of-russian-cyberattack/ar-AAVkpKQ>
- 333) 'Astonishing.' Morgan Stanley hard drives holding sensitive client data got auctioned off online – CNN, <https://edition.cnn.com/2022/09/20/business/morgan-stanley-fine-customer-data/index.html>
- 334) Direito a desligar: A empresa pode ligar-me? E quem paga despesas do teletrabalho? - Jornal de Notícias, <https://www.jn.pt/nacional/direito-a-desligar-a-empresa-pode-ligar-me-e-quem-paga-despesas-do-teletrabalho-14284846.html>
- 335) Direito a desligar do trabalho: o que diz a lei – Ekonomista, <https://www.ekonomista.pt/o-direito-a-desligar-do-trabalho/>
- 336) Uso de tecnologia em contexto laboral invade vida pessoal, consideram mais de metade dos trabalhadores – Visão, <https://visao.sapo.pt/atualidade/sociedade/2022-03-16-uso-de-tecnologia-em-contexto-laboral-invade-vida-pessoal-consideram-mais-de-metade-dos-trabalhadores/>
- 337) Teletrabalho. Envio de email sem exigir resposta imediata não viola direito a desligar - Diário de Notícias, <https://www.dn.pt/sociedade/teletrabalho-envio-de-email-sem-exigir-resposta-imediata-nao-viola-direito-a-desligar-14581267.html>
- 338) Microsoft and ZeniMax union reach "first of its kind" agreement over usage of AI tools in gamedev – Rock Paper Shotgun, <https://www.rockpapershotgun.com/microsoft-and-zenimax-union-reach-first-of-its-kind-agreement-over-usage-of-ai-tools-in-gamedev>
- 339) The Gig Is Up – IMDB, <https://www.imdb.com/title/tt14318912/>
- 340) Be aware of the household items hackers are targeting to learn information about you – Koaa News5, <https://www.koaa.com/news/on-your-side/be-aware-of-the-household-items-hackers-are-targeting-to-learn-information-about-you>
- 341) 'Look behind you'; Va. family says hackers used Ring cameras to taunt their children - ABC 13 News, <https://wset.com/news/local/look-behind-you-va-family-says-hackers-used-ring-cameras-to-taunt-their-children>

- 342) Singapore home cams hacked and stolen footage sold on pornographic sites – The Straits Times, <https://www.straitstimes.com/singapore/singapore-home-cams-hacked-and-stolen-footage-sold-on-pornographic-sites>
- 343) 'I'm in your baby's room': Nest cam hacks show risk of internet-connected devices – NBC News, <https://www.nbcnews.com/tech/tech-news/i-m-your-baby-s-room-nest-cam-hacks-show-n950876>
- 344) Vodafone mais uma vítima de ciberataque. Estarão os carros conectados seguros? - Away, <https://away.iol.pt/ciberseguranca/seguranca/vodafone-mais-uma-vitima-de-ciberataque-estaraos-carros-conectados-seguros/20220227/6202363b0cf2cc58e7e1ae92>
- 345) Cibertaque condiciona sistemas informáticos no Hospital Garcia de Orta – Sapo Tek, <https://tek.sapo.pt/noticias/internet/artigos/cibertaque-condiciona-sistemas-informaticos-no-hospital-garcia-de-orta>
- 346) Câmara Municipal da Moita alvo de ataque informático com ransomware – Pplware, <https://pplware.sapo.pt/informacao/camara-municipal-da-moita-alvo-de-ataque-informatico-com-ransomware/>
- 347) Tentativa de ataque informático na Unidade Local de Saúde do Litoral Alentejano – Saúde+, <https://www.saudemais.tv/noticia/38829-tentativa-de-ataque-informatico-na-unidade-local-de-saude-do-litoral-alentejano>
- 348) Coca-Cola investigating claims of hack after ransomware group hawks stolen data – The Record, <https://therecord.media/coca-cola-investigating-claims-of-hack-after-ransomware-group-hawks-stolen-data/>
- 349) Russian-speaking ransomware gang threatens to overthrow Costa Rica government after cyber attack – Euronews, <https://www.euronews.com/next/2022/05/17/russian-speaking-ransomware-gang-threatens-to-overthrow-costa-rica-government-after-cyber->
- 350) Fears grow for smaller nations after ransomware attack on Costa Rica escalates – Techcrunch, <https://techcrunch.com/2022/05/20/costa-rica-ransomware-attack/>
- 351) Seeing hack attacks on the rise, Israel orders telecoms to erect 'cyber Iron Dome' – The Times of Israel, <https://www.timesofisrael.com/seeing-hack-attacks-on-the-rise-israel-order-telecoms-to-erect-cyber-iron-dome/>
- 352) Why AI is the key to cutting-edge cybersecurity – World Economic Forum, <https://www.weforum.org/agenda/2022/07/why-ai-is-the-key-to-cutting-edge-cybersecurity/>

353) Notários portugueses foram alvo de um ataque informático que terá recorrido a inteligência artificial – CNN Portugal, <https://cnnportugal.iol.pt/burlas/phishing/ha-tres-esquemas-online-que-estao-a-roubar-milhoes-aos-portugueses-saiba-como-atuam-os-burloes-e-como-se-proteger/20230312/640225010cf2dce741adda74>

354) Ataques informáticos com resgate aumentaram 13% - Novo, <https://onovo.pt/tecnologia/ataques-informaticos-com-resgate-aumentaram-13-LH10533668>

355) "Hoje nenhuma instituição pode pensar que não vai ser atacada" por hackers – Sol, <https://sol.sapo.pt/artigo/769633/hoje-nenhuma-instituicao-pode-pensar-que-nao-vai-ser-atacada-por-hackers>

356) Há três esquemas online que estão a roubar milhões aos portugueses. Saiba como atuam os burlões e como se proteger – CNN Portugal, <https://cnnportugal.iol.pt/burlas/phishing/ha-tres-esquemas-online-que-estao-a-roubar-milhoes-aos-portugueses-saiba-como-atuam-os-burloes-e-como-se-proteger/20230312/640225010cf2dce741adda74>

357) The cloud and 5G security apocalypse is only a matter of time – Light Reading, <https://www.lightreading.com/security/the-cloud-and-5g-security-apocalypse-is-only-matter-of-time/d/d-id/781259>

358) New Warning For WhatsApp Users Over Account Suspension ‘Hack’ – Forbes, <https://www.forbes.com/sites/zakdoffman/2021/04/10/shock-new-warning-for-millions-of-whatsapp-users-on-apple-iphone-and-google-android-phones/?sh=18e96e657585>

359) Mobile IoT networks to be a 'core component' of 5G - TechRadar, <https://www.techradar.com/news/mobile-iot-networks-to-be-a-core-component-of-5g>

360) Qual o impacto do IoT no nosso dia a dia? - Olhar Digital, <https://olhardigital.com.br/pro/noticia/qual-o-impacto-do-iot-no-nosso-dia-a-dia/102236>

361) How Many IoT Devices Are There in 2022? [All You Need To Know] – Techjury, <https://techjury.net/blog/how-many-iot-devices-are-there/>

362) Evaluating the GCHQ Exceptional Access Proposal - Schneider on Security, https://www.schneier.com/blog/archives/2019/01/evaluating_the_.html

363) Principles for a More Informed Exceptional Access Debate - Lawfare, <https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate>

364) The Plan to Use Fitbit data to Stop Mass Shootings in the US Is One of the Scariest Proposals Yet - Gizmodo, <https://www.gizmodo.co.uk/2019/09/the-plan-to-use-fitbit-data-to-stop-mass-shootings-in-the-us-is-one-of-the-scariest-proposals-yet/>

365) U.N. Fact Finders Say Facebook Played a 'Determining' Role in Violence Against the Rohingya – Time, <https://time.com/5197039/un-facebook-myanmar-rohingya-violence/>

366) Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach - The Guardian, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

367) ‘I made Steve Bannon’s psychological warfare tool’: meet the data war whistleblower - The Guardian, <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

368) Regulamento Geral sobre a Proteção de Dados – União Europeia, <https://gdprinfo.eu/pt-pt>

369) New ruling: Your cookie data might be sensitive data – Simple Analytics, <https://www.simpleanalytics.com/blog/new-ruling-your-cookie-data-might-be-sensitive-data-here-is-why-that-matters>

370) The Truth About Data Mining: How Online Trackers Gather Your Info and What They See - Observer, <https://observer.com/2016/07/the-truth-about-data-mining-how-online-trackers-gather-your-info-and-what-they-see/>

371) I Visited 47 Sites. Hundreds of Trackers Followed Me. - New York Times, <https://www.nytimes.com/interactive/2019/08/23/opinion/data-internet-privacy-tracking.html>

372) Cookies: I looked at 50 well-known websites and most are gathering our data illegally - The Conversation, <https://theconversation.com/cookies-i-looked-at-50-well-known-websites-and-most-are-gathering-our-data-illegally-176203>

373) Some top 100,000 websites collect everything you type—before you hit submit – Ars Technica, <https://arstechnica.com/information-technology/2022/05/some-top-100000-websites-collect-everything-you-type-before-you-hit-submit/>

374) Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence – Arxiv, <https://arxiv.org/abs/2001.02479>

375) Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document – Vice, <https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes>

376) Facebook probably has your phone number, even if you never shared it. Now it has a secret tool to let you delete it. - Business Insider, <https://www.businessinsider.com/facebook-has-hidden-tool-to-delete-your-phone-number-email-2022-10>

377) Ex-Twitter exec blows the whistle, alleging reckless and negligent cybersecurity policies – CNN, <https://edition.cnn.com/2022/08/23/tech/twitter-whistleblower-peiter-zatko-security/index.html>

378) Twitter faces privacy scrutiny from EU watchdogs after Mudge report – TechCrunch, <https://techcrunch.com/2022/08/24/twitter-whistleblower-security-eu/>

379) Largest Study of Online Tracking Proves Google Really Is Watching Us All - MIT Technology Review, <https://www.technologyreview.com/2016/05/18/160139/largest-study-of-online-tracking-proves-google-really-is-watching-us-all/>

380) TikTok Can Circumvent Apple and Google Privacy Protections and Access Full User Data, 2 Studies Say (Exclusive) – Yahoo, <https://www.yahoo.com/entertainment/tiktok-circumvent-apple-google-privacy-140000271.html>

381) TikTok's updated data privacy policy does little to settle nerves – Quartz, <https://qz.com/tiktok-s-updated-data-privacy-policy-does-little-to-set-1849736467>

382) Avoid These 3 Types of App if You Care About Privacy – Make Use Of, <https://www.makeuseof.com/apps-avoid-privacy/>

383) Facebook spied on private messages of Americans who questioned 2020 election - New York Post, <https://nypost.com/2022/09/14/facebook-spied-on-private-messages-of-americans-who-questioned-2020-election/>

384) Truth Cops – The Intercept, <https://theintercept.com/2022/10/31/social-media-disinformation-dhs/>

385) Mass surveillance - Who is watching the watchers? - Google Books, https://books.google.pt/books?id=qhWkDAAAQBAJ&pg=PA12&lpg=PA12&dq=google+microsoft+intelligence+agencies&source=bl&ots=FeVTiau5mz&sig=ACfU3U0MbUutWvIdWhLNVrMYLwiAroxqw&hl=en&sa=X&ved=2ahUKEwj_uun5sLpAhXR8eAKHTiiDMMQ6AEwCHoECAoQAQ#v=onepage&q=google%20microsoft%20intelligence%20agencies&f=false

386) Intelligence Elites and Public Accountability: Relationships of Influence With Civil Society- Google Books, https://books.google.pt/books?id=zSFWDwAAQBAJ&pg=PT176&lpg=PT176&dq=google+microsoft+intelligence+agencies&source=bl&ots=X9nB_1BZq5&sig=ACfU3U0AZZouZh6BKA17WHVEkVrHVR9fpw&hl=en&sa=X&ved=2ahUKEwj_uun5sLpAhXR8eAKHTiiDMMQ6AEwBXoECAsQAQ#v=onepage&q=google%20microsoft%20intelligence%20agencies&f=false

387) The International Business Environment - Google Books, https://books.google.pt/books?id=IM4YBwAAQBAJ&pg=PA230&lpg=PA230&dq=google+microsoft+intelligence+agencies&source=bl&ots=4Yd0tko4N7&sig=ACfU3U1J9zEDrNBD87bWvJ3a5iD2digw9w&hl=en&sa=X&ved=2ahUKEwj_uun5sLpAhXR8eAKHTiiDMMQ6AEwBnoECACQAQ#v=onepage&q=google%20microsoft%20intelligence%20agencies&f=false

388) Journalist Who Helped Break Snowden's Story Reflects On His High-Stakes Reporting - WAMU, <https://wamu.org/story/20/05/20/journalist-who-helped-break-snowdens-story-reflects-on-his-high-stakes-reporting/>

389) Now More Than Ever You Need to Cover Phone And Laptop Cameras, Says Security Expert - Science Alert, <https://www.sciencealert.com/you-need-to-cover-phone-and-laptop-cameras-now-more-than-ever-says-security-expert>

390) Forget state surveillance. Our tracking devices are now doing the same job – The Guardian, <https://www.theguardian.com/commentisfree/2022/feb/19/forget-state-surveillance-our-tracking-devices-are-now-doing-the-same-job>

391) Maintaining confidentiality in 21st century: Mission (im)possible - 112 UA, <https://112.international/society/maintaining-confidentiality-in-21st-century-mission-impossible-51315.html>

392) Leaked Chinese government documents detail how tech is used to escalate the persecution of Uighurs - TechCrunch, <https://techcrunch.com/2019/11/24/leaked-chinese-government-documents-detail-how-tech-is-used-to-escalate-the-persecution-of-uighurs/>

393) 5G And The Internet Of Everything Is EVERYTHING THEY WANT! - WeAreChange, <https://www.youtube.com/watch?v=Ub-9CJc2Apchttps://www.youtube.com/watch?v=Ub-9CJc2Apc>

394) Is Your Phone Recording Your Conversations? The Answer Might Surprise You. - HuffPost, https://www.huffpost.com/entry/smartphone-devices-recording-privacy_1_5d570869e4b056fafd0bbc09

395) Thousand of Facebook internal documents, emails made public in leak - Business Insider, <https://www.businessinsider.com/facebook-internal-documents-executive-emails-published-six4three-court-leak-2019-11>

396) FBI greift massiv in 5G-Überwachungsstandards ein - radio FM4, <https://fm4.orf.at/stories/2989759/>

397) MI6, MI5 and GCHQ 'unlawfully collected private data' from telecoms firms, says ECJ official - The Telegraph, <https://www.telegraph.co.uk/technology/2020/01/16/mi6-mi5-gchq-unlawfully-collected-private-data-telecoms-firms/>

398) The 5g Controversy Exposed! - WeAreChange, <https://www.youtube.com/watch?v=H571y9xcLRU>

399) About 3GPP Home – 3GPP, <https://www.3gpp.org/about-3gpp/about-3gpp>

400) Release 13 - 3GPP, <https://www.3gpp.org/release-13>

401) Release 15 - 3GPP, <https://www.3gpp.org/release-15>

402) Release 16 – 3GPP, <https://www.3gpp.org/release-16>

403) Release 17 – 3GPP, <https://www.3gpp.org/release-17>

404) Release 18 – 3GPP, <https://www.3gpp.org/release18>

405) AT&T claims advanced 4G is '5G' - TechRadar, <https://www.techradar.com/news/atandt-claims-advanced-4g-is-5g>

406) AT&T announces it will build a fake 5G network - The Verge, <https://www.theverge.com/2017/4/25/15425414/att-5g-evolution-network-lte-advanced-misleading-marketing>

407) 5G vs 5GE vs 5GHz: What's the Difference? - PC Mag <https://www.pcmag.com/article/365754/5g-vs-5g-e-vs-5ghz-whats-the-differenc>

408) NOS obrigada a retirar campanha sobre 5G - Jornal de Notícias, <https://www.jn.pt/economia/nos-obrigado-a-retirar-de-campanha-sobre-5g-11502288.html>

409) Comparison of international policies on electromagnetic fields - Rijksinstituut voor Volksgezondheid en Milieu (Instituto Nacional de Saúde Pública e Meio Ambiente da Holanda), <https://www.rivm.nl/sites/default/files/2018-11/Comparison%20of%20international%20policies%20on%20electromagnetic%20fields%202018.pdf>

- 410) A conspiração que liga Covid e rede 5G - Diário de Notícias,
<https://www.dn.pt/dinheiro/a-conspiracao-que-liga-covid-e-rede-5g-12059916.html>
- 411) How ICNIRP, AGNIR, PHE and a 30 year old political decision created and then covered up a global public health scandal - Community Operating Systems,
<https://communityoperatingsystem.wordpress.com/2019/09/12/how-icnirp-agnir-phe-and-a-30-year-old-political-decision-created-and-then-covered-up-a-global-public-health-scandal/>
- 412) ICNIRP Guidelines - ICNIRP,
<https://web.archive.org/web/20140606044606/http://www.icnirp.org/documents/emfgdl.pdf>
- 413) Advisory Group on Non-Ionising Radiation - Gov.uk,
<https://www.gov.uk/government/groups/advisory-group-on-non-ionising-radiation-agnir>
- 414) Resolution of Notice of Inquiry, Second Report and Order, Notice of Proposed Rulemaking, and Memorandum Opinion and Order - FCC,
<https://docs.fcc.gov/public/attachments/FCC-19-126A1.pdf>
- 415) Resolution of Notice of Inquiry, Second Report and Order, Notice of Proposed Rulemaking, and Memorandum Opinion and Order – FCC - FCC,
https://docs.fcc.gov/public/attachments/FCC-19-126A1_Rcd.pdf
- 416) Is 5G Going to Kill Us All? - The New Republic,
<https://newrepublic.com/article/157603/5g-going-kill-us-all>
- 417) Exposure limits for radio-frequency fields (public) - World Health Organization
<http://apps.who.int/gho/data/node.main-eu.EMFLIMITSPUBLICRADIOFREQUENCY?lang=en>
- 418) Diário da República, 1.ª série - N.º 151 - 7 de agosto de 2017 - Assembleia da República, <https://dre.pt/application/conteudo/107963496>
- 419) Why you shouldn't get too excited about 5G yet – Business Insider,
<https://www.businessinsider.com/5g-high-speed-internet-cellular-network-issues-switch-2019-4>
- 420) How to Legally Track a Cell Phone – Lifewire, <https://www.lifewire.com/legally-track-cell-phone-4160372>
- 421) Can You Track Switched Off Phones? Apparently, NSA Can! - Techpp,
<https://techpp.com/2013/08/22/track-phone-turned-off/>

- 422) How GPS can track you, even when you turn it off – CNBC,
<https://www.cnn.com/2018/07/13/gps-can-spy-on-you-even-when-you-turn-it-off.html>
- 423) Your smartphone can be tracked even if GPS, location services are turned off – TechRepublic, <https://www.techrepublic.com/article/your-smartphone-can-be-tracked-even-if-gps-location-services-are-turned-off/>
- 424) How a handful of Apple and Google employees came together to help health officials trace coronavirus - CNBC, <https://www.cnn.com/2020/04/28/apple-iphone-contact-tracing-how-it-came-together.html>
- 425) Telemóveis de infetados podem ser "espécie de pulseira eletrónica" - Jornal de Notícias, <https://www.jn.pt/nacional/telemoveis-de-infetados-podem-ser-especie-de-pulseira-eletronica-12019200.html>
- 426) Coronavirus contact tracing poses serious threats to our privacy - The Conversation, <https://theconversation.com/coronavirus-contact-tracing-poses-serious-threats-to-our-privacy-137073>
- 427) 170 cybersecurity experts warn that British government's contact tracing app could be used to surveil people even after coronavirus has gone - Business Insider, <https://www.businessinsider.nl/cybersecurity-experts-uk-government-contact-tracing-surveillance-2020-4/>
- 428) Big Brother in the Age of Coronavirus: 100+ Groups Warn Against Exploiting Pandemic to Permanently Expand Surveillance State - Common Dreams News, <https://www.commondreams.org/news/2020/04/02/big-brother-age-coronavirus-100-groups-warn-against-exploiting-pandemic-permanently>
- 429) Eu prescindo da minha privacidade - Observador, <https://observador.pt/opiniao/eu-prescindo-da-minha-privacidade/>
- 430) Querem o meu telemóvel? Podem ficar com ele - Público, <https://www.publico.pt/2020/04/30/opiniao/opiniao/querem-telemovel-podem-ficar-1914485>
- 431) Bom dia! Esta é a primeira página do Jornal de Notícias desta terça-feira, 2 de junho de 2020. - Jornal de Notícias, <https://www.facebook.com/jornalnoticias/photos/a.315168737994/10160035060687995/?type=3>
- 432) Fomos enganados - Observador, <https://observador.pt/opiniao/fomos-enganados/>

433) We're losing the war against surveillance capitalism because we let Big Tech frame the debate – Salon, <https://www.salon.com/2020/06/20/were-losing-the-war-against-surveillance-capitalism-because-we-let-big-tech-frame-the-debate/>

434) How the governance of and through digital contact tracing technologies shapes geographies of power – Bristol University Press Digital, <https://bristoluniversitypressdigital.com/view/journals/pp/50/2/article-p181.xml>

435) Police seize on COVID-19 tech to expand global surveillance – Yahoo News, <https://news.yahoo.com/police-seize-covid-19-tech-052651411.html>

436) A proteção de dados na UE – Comissão Europeia, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt

437) Why we can't stop fighting about cancel culture – Vox, <https://www.vox.com/culture/2019/12/30/20879720/what-is-cancel-culture-explained-history-debate>

438) How Authoritarian Top Down Control Is Being Imposed on the World - Activist Post, <https://www.activistpost.com/2020/03/how-authoritarian-top-down-control-is-being-imposed-on-the-world.html>

439) Criminal identification bill in India raises fears of shadowing – Rfi, <https://www.rfi.fr/en/international/20220416-criminal-identification-bill-in-india-raises-fears-of-shadowing>

440) India Orders VPN Companies to Collect and Hand Over User Data – CNET, <https://www.cnet.com/news/privacy/india-orders-vpn-companies-to-collect-and-hand-over-user-data/>

441) The Chinese surveillance state proves that the idea of privacy is more “malleable” than you'd expect – MIT Technology Review, <https://www.technologyreview.com/2022/10/10/1060982/china-pandemic-cameras-surveillance-state-book/>

442) Saudi Arabians are using a widely available Google and Apple store app to report activists who speak out against the government. Some have received harsh sentences while others are self-censoring. - Insider, <https://www.businessinsider.com/saudi-arabia-mbs-human-rights-violations-apple-google-app-store-2022-9>

443) Saudi Arabia jails two Wikipedia staff in ‘bid to control content’ – The Guardian, <https://www.theguardian.com/technology/2023/jan/05/saudi-arabia-jails-two-wikipedia-staff-in-bid-to-control-content>

444) Exclusive: State Dept. gives law enforcement, intelligence agencies unrestricted access to Americans' personal data – Yahoo, <https://www.yahoo.com/news/exclusive-state-dept-gives-law-enforcement-intelligence-agencies-unrestricted-access-to-americans-personal-data-020409616.html>

445) Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police – Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police>

446) US Police Track Innocent People's Movements With Troubling New App – Consortiumnews.com, <https://consortiumnews.com/2022/10/21/us-police-track-innocent-peoples-movements-with-troubling-new-app/>

447) Revealed: US Military Bought Mass Monitoring Tool That Includes Internet Browsing, Email Data – Vice, <https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data>

448) Public Buses Across Country Quietly Adding Microphones to Record Passenger Conversations – Wired, <https://www.wired.com/2012/12/public-bus-audio-surveillance/>

449) UK government plans to remove key human rights protections – The Guardian, <https://www.theguardian.com/law/2020/sep/13/uk-government-plans-to-remove-key-human-rights-protections>

450) Human Rights Watch Response to UK Ministry of Justice Consultation . Human Rights Watch, <https://www.hrw.org/news/2022/03/09/human-rights-watch-response-uk-ministry-justice-consultation>

451) These MPs praised 'brave' Russian protesters – then voted to restrict protest in the UK – The Big Issue, <https://www.bigissue.com/news/activism/these-mps-praised-brave-russian-protesters-then-voted-to-restrict-protest-in-the-uk/>

452) Police use of facial recognition unlawfully breached privacy rights, says Court of Appeal ruling – Sky News, <https://news.sky.com/story/police-use-of-facial-recognition-unlawfully-breached-privacy-rights-says-court-of-appeal-ruling-12047012>

453) Facial recognition technology 'will turn our streets into police line-ups', campaigners say – Sky News, <https://news.sky.com/story/facial-recognition-technology-will-turn-our-streets-into-police-line-ups-campaigners-say-12572433>

454) UK: Dark day for civil liberties as 'deeply-authoritarian' Policing Bill passed by Lords – Amnesty International UK, <https://www.amnesty.org.uk/press-releases/uk-dark-day-civil-liberties-deeply-authoritarian-policing-bill-passed-lords>

455) Data sharing: MoD and Home Office ignored people's data requests – ICO – BCC,
<https://www.bbc.com/news/technology-63048984>

456) UK government set to extract hospital data to Palantir system without patient consent
– The Register, https://www.theregister.com/2022/11/04/uk_government_set_to_extract/

457) Online Safety Act – Gov.uk, <https://www.gov.uk/government/collections/online-safety-act>

458) Police make 30 arrests a day for offensive online messages – The Sunday Times,
<https://www.thetimes.com/uk/crime/article/police-make-30-arrests-a-day-for-offensive-online-messages-zbv886tqf>

459) New digital ID scheme to be rolled out across UK – Gov.uk,
<https://www.gov.uk/government/news/new-digital-id-scheme-to-be-rolled-out-across-uk>

460) RUSSIA introduces DIGITAL ID under the State controlled MAX app. Zakharova
about the missing children - Seemorerocks, <https://seemorerocks.substack.com/p/russia-introduces-digital-id-under>

461) This Is What a Digital Coup Looks Like | Carole Cadwalladr | TED – vídeo do canal
de Youtube TED, <https://www.youtube.com/watch?v=TZOoT8AbkNE>

462) New legal restrictions needed on police use of facial recognition: privacy watchdogs -
National Post, <https://nationalpost.com/pmnn/news-pmn/canada-news-pmn/new-legal-restrictions-needed-on-police-use-of-facial-recognition-privacy-watchdogs>

463) Australia just made the Internet MORE dangerous – canal de Youtube Hero Hei,
<https://www.youtube.com/watch?v=1TEY6saHvtg>

464) A verificação da idade na Internet chegou aos EUA - canal de Youtube Hero Hei,
https://youtu.be/jKPgAxsuSrk?si=kY_6J2uQl40hXSoH

465) ID photos of 70,000 users may have been leaked, Discord says – BBC,
<https://www.bbc.com/news/articles/c8jmzd972leo>

466) HUGE Online Safety Act Data Breach – vídeo do canal CYBER WAFFLE,
<https://www.youtube.com/watch?v=aqpRdDC-rmA>

467) Mass surveillance and attack on encryption: Civil society protests against EU chat
control plans – EU Reporter, <https://www.eureporter.co/business/2022/03/18/mass-surveillance-and-attack-on-encryption-civil-society-protests-against-eu-chat-control-plans/>

468) It's official! Germany "will not agree" to Chat Control – here's everything we know – Techradar, <https://www.techradar.com/computing/cyber-security/its-official-germany-will-not-agree-to-chat-control-heres-everything-we-know>

469) EFF Tells E.U. Commission: Don't Break Encryption – Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2022/03/eff-tells-eu-commission-dont-break-encryption>

470) European Parliament Says CSAM Detection Can Continue – For Now – ZwillGenBlog, <https://www.zwillgen.com/privacy/european-parliament-csam-detection-continue/>

471) EU plans to fight child sexual abuse online with new law obliging tech firms to report offences – Euronews, <https://www.euronews.com/next/2022/01/10/eu-plans-to-fight-child-sexual-abuse-online-with-new-law>

472) CSAM – 9TO5Mac, <https://9to5mac.com/guides/csam/>

473) Proposals for scanning encrypted messages should be cut from Online Safety Bill, say researchers – Computer Weekly, <https://www.computerweekly.com/news/252525778/Proposals-for-scanning-encrypted-messages-should-be-cut-from-Online-Safety-Bill-say-researchers>

474) Europe Is Building a Huge International Facial Recognition System – Wired, <https://www.wired.co.uk/article/europe-police-facial-recognition-prum>

475) Reforço do intercâmbio automatizado de dados no âmbito do quadro jurídico de Prüm – Comissão Europeia, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12563-Reforco-do-intercambio-automatizado-de-dados-no-ambito-do-quadro-juridico-de-Prum_pt

476) Boosting police cooperation across borders for enhanced security – European Commission, https://ec.europa.eu/home-affairs/news/boosting-police-cooperation-across-borders-enhanced-security-2021-12-08_en

477) Chat Control: UE prepara-se para “fazer scan” a todas as suas mensagens e e-mails – Pplware, <https://pplware.sapo.pt/internet/seguranca/chat-control-ue-prepara-se-para-fazer-scan-a-todas-as-suas-mensagens-e-e-mails/>

478) Fight Chat Control - Fight Chat Control, <https://fightchatcontrol.eu/>

479) Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das

comunicações eletrónicas (diretiva relativa à privacidade e às comunicações eletrónicas) – ANACOM, <https://www.anacom.pt/render.jsp?categoryId=332326>

480) Tribunal Constitucional chumba normas da “lei dos metadados” – Público, <https://www.publico.pt/2022/04/27/politica/noticia/tribunal-constitucional-chumba-normas-lei-metadados-2004030>

481) Metadados: Provedora leva lei ao Constitucional, mas por novos motivos – Público, <https://www.publico.pt/2019/09/04/politica/noticia/metadados-provedora-leva-lei-constitucional-motivos-diferentes-partidos-1885560>

482) Trabalhos parlamentares regressam com combate à inflação a marcar agenda – JM Madeira, https://www.jm-madeira.pt/nacional/ver/183803/Trabalhos_parlamentares_regressam_com_combate_a_inflacao_a_marcar_agenda

483) Marcelo recorre mais ao Constitucional para manter o Governo maioritário “na linha” – ZAP.aeiou, <https://zap.aeiou.pt/marcelo-constitucional-governo-497713>

484) Parlamento aprova texto dos metadados que prevê conservação generalizada até seis meses – TSF, <https://www.tsf.pt/portugal/politica/parlamento-aprova-texto-dos-metadados-que-preve-conservacao-generalizada-ate-seis-meses-17162207.html>

485) Lei n.º 18/2024, de 5 de fevereiro – Diário da República, <https://diariodarepublica.pt/dr/detalhe/lei/18-2024-840278734>

486) German data retention rules not compatible with EU law, says top court – DW, <https://www.dw.com/en/german-data-retention-rules-not-compatible-with-eu-law-says-top-court/a-63178438>

487) Democratic deficit – EUR Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:democratic_deficit

488) The EU's democratic problem – and what can be done about it – The Loop, <https://theloop.ecpr.eu/the-eus-democratic-problem-and-what-can-be-done-about-it/>

489) Pegasus spyware owner NSO sues Israeli newspaper – DW, <https://www.dw.com/en/pegasus-spyware-owner-nso-sues-israeli-newspaper/a-60937566>

490) How a Saudi woman's iPhone revealed hacking around the world – Reuters, <https://www.reuters.com/technology/how-saudi-womans-iphone-revealed-hacking-around-world-2022-02-17/>

- 491) Exclusive: Senior EU officials were targeted with Israeli spyware – Reuters, <https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11>
- 492) No 10 suspected of being target of NSO spyware attack, Boris Johnson ‘told’ – The Guardian, <https://www.theguardian.com/politics/2022/apr/18/no-10-suspected-of-being-target-of-nso-spyware-attack-boris-johnson>
- 493) Pegasus Project – The Guardian, <https://www.theguardian.com/news/series/pegasus-project>
- 494) French minister’s phone shows traces linked to NSO spyware – The Guardian, <https://www.theguardian.com/world/2021/jul/20/french-ministers-phone-shows-traces-linked-to-nso-spyware>
- 495) Pegasus spyware targets top Catalan politicians and activists – Politico, <https://www.politico.eu/article/pegasus-spyware-targets-top-catalan-politicians-and-activists/>
- 496) Spanish prime minister’s phone ‘targeted with Pegasus spyware’ – The Guardian, <https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware>
- 497) Mexico: reporters and activists hacked with NSO spyware despite assurances – The Guardian, <https://www.theguardian.com/world/2022/oct/04/mexico-nso-spyware-journalists-human-rights-hacked-pegasus>
- 498) Hooking Candiru – The Citizen Lab, <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/>
- 499) Spyware Vendors Target Android With Zero-Day Exploits – Wired, <https://www.wired.com/story/android-spyware-cytrox-predator-google-tag/>
- 500) Inteligência Artificial pode "virar-se contra nós", alerta Margrethe Vestager - Observador, <https://observador.pt/2021/09/28/inteligencia-artificial-pode-virar-se-contra-nos-alerta-margrethe-vestager/>
1. É fake que IA "saiu do controle" no Japão; entenda – Época Negócios, <https://epocanegocios.globo.com/inteligencia-artificial/noticia/2024/09/e-fake-que-ia-saiu-do-controle-no-japao-entenda-gd2024.ghtml>

501) Dutch scandal serves as a warning for Europe over risks of using algorithms - Politico, <https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/>

502) Fisco vai usar Inteligência Artificial para controlar contribuintes. Sindicato fala em "anedota" que "vai demorar anos" a ser implementada – CNN Portugal, <https://cnnportugal.iol.pt/autoridade-tributaria/inteligencia-artificial/fisco-vai-usar-inteligencia-artificial-para-controlar-contribuintes-sindicato-fala-em-anedota-que-vai-demorar-anos-a-ser-implementada/20240912/66e2cb8bd34ea1acf26e3d27>

503) Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI - European Council Council of the European Union, <https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/>

504) An AI Algorithm is Raising Rents on Hundreds of Thousands of People Across the Country – Surviving Tomorrow, <https://www.surviving-tomorrow.com/p/an-ai-algorithm-is-raising-rents>

505) Robot Landlords Are Buying Up Houses – Vice, <https://www.vice.com/en/article/dy7eaw/robot-landlords-are-buying-up-houses>

506) He Used AI to Publish a Children’s Book in a Weekend. Artists Are Not Happy About It – Time, <https://time.com/6240569/ai-childrens-book-alice-and-sparkle-artists-unhappy/>

507) The College Essay Is Dead – The Atlantic, <https://www.theatlantic.com/technology/archive/2022/12/chatgpt-ai-writing-college-student-essays/672371/>

508) OpenAI upgrades GPT-3, stunning with rhyming poetry and lyrics – Ars Technica, <https://arstechnica.com/information-technology/2022/11/openai-conquers-rhyming-poetry-with-new-gpt-3-update/>

509) AI-Created Comic Could Be Deemed Ineligible for Copyright Protection – CBR, <https://www.cbr.com/ai-comic-deemed-ineligible-copyright-protection/>

510) Federal Court Rules Work Generated by Artificial Intelligence Alone Is Not Eligible for Copyright Protection – K & L Gates Hub, <https://www.klgates.com/Federal-Court-Rules-Work-Generated-by-Artificial-Intelligence-Alone-Is-Not-Eligible-for-Copyright-Protection-8-30-2023>

511) What do the latest US and China rulings on AI authorship mean for luxury? - Jing Daily, <https://jingdaily.com/us-china-rulings-ai-authorship-luxury/>

512) Gere texto, imagens, códigos e muito mais com a IA do Google Cloud – Google, <https://cloud.google.com/use-cases/generative-ai?hl=pt-br>

513) AI unmaskes anonymous chess players, posing privacy risks – Science, <https://www.science.org/content/article/ai-unmaskes-anonymous-chess-players-posing-privacy-risks>

514) Study: Deep neural networks don't see the world the way we do – Massachusetts Institute of Technology, <https://news.mit.edu/2023/study-deep-neural-networks-perception-1016>

515) ChatGPT. O prodígio da Inteligência Artificial é "empolgante", mas é preciso ter cuidado com "efeitos secundários" – Diário de Notícias, <https://www.dn.pt/ciencia/chatgpt-o-prodigio-da-inteligencia-artificial-e-empolgante-mas-e-preciso-ter-cuidado-com-efeitos-secundarios-15534842.html>

516) Bard is going to destroy online search – Insider, <https://www.businessinsider.com/ai-chatbots-chatgpt-google-bard-microsoft-bing-break-internet-search-2023-2>

517) Noam Chomsky on ChatGPT: It's "Basically High-Tech Plagiarism" and "a Way of Avoiding Learning" – Open Culture, <https://www.openculture.com/2023/02/noam-chomsky-on-chatgpt.html>

518) IA invade publicações científicas e, para pesquisador, situação deve piorar – Folha de São Paulo, <https://www1.folha.uol.com.br/ciencia/2024/08/ia-invade-publicacoes-cientificas-e-para-pesquisador-situacao-deve-piorar.shtml>

519) AI systems could be on the verge of collapsing into nonsense, scientists warn – Independent, <https://www.independent.co.uk/tech/ai-artificial-intelligence-chatgpt-nonsense-b2585244.html>

520) ChaosGPT And Why We Need AI Regulation – Medium, <https://medium.com/predict/chaosgpt-and-why-we-need-ai-regulation-b6155b293aac>

521) Chaos Gpt - ChaosGpt, <https://chaos-eth.org/>

522) ChaosGPT: Empowering GPT with Internet and Memory to Destroy Humanity – Youtube, <https://www.youtube.com/watch?v=g7YJIpkk7KM>

523) Replacing Humans with AI is Going Horribly Wrong – vídeo do canal ColdFusion, disponível em <https://www.youtube.com/watch?v=QX1Xwzm9yHY>

- 524) MIT report: 95% of generative AI pilots at companies are failing – Fortune, <https://fortune.com/2025/08/18/mit-report-95-percent-generative-ai-pilots-at-companies-failing-cfo/>
- 525) Scarlett Johansson acusa OpenAI de imitar a sua voz. “Sky” retirada do ChatGPT – Público, <https://www.publico.pt/2024/05/21/tecnologia/noticia/scarlett-johansson-acusa-openai-imitar-voz-sky-retirada-chatgpt-2091198>
- 526) What the AI Actor Tilly Norwood Means for the Future of Film – AI Magazine, <https://aimagazine.com/news/what-the-ai-actor-tilly-norwood-means-for-the-future-of-film;>
- 527) AI: Decoded: The tech policy fight of the decade begins — AI bias — Improving Twitter’s algorithm – Politico, <https://www.politico.eu/newsletter/ai-decoded/the-tech-policy-fight-of-the-decade-begins-ai-bias-improving-twitters-algorithm-2/>
- 528) Benefits and Risks of AI: All You Need to Know - hackernoon, <https://hackernoon.com/benefits-and-risks-of-ai-all-you-need-to-know-qga63wtp>
- 529) Perito português em inteligência artificial alerta para riscos da nova tecnologia – RTP, https://www.rtp.pt/noticias/pais/perito-portugues-em-inteligencia-artificial-alerta-para-riscos-da-nova-tecnologia_n1574324
- 530) White House Releases Blueprint for Artificial Intelligence Bill of Rights – PetaPixel, <https://petapixel.com/2022/10/04/white-house-releases-blueprint-for-artificial-intelligence-bill-of-rights/>
- 531) Elements of AI - Elements of AI, <https://www.elementsofai.com/>
- 532) Researchers warn that the Fronton botnet was used by Russia-linked threat actors for coordinated disinformation campaigns. - Security Affairs, <https://securityaffairs.co/wordpress/131574/cyber-warfare-2/fronton-botnet-disinformation.html>
- 533) Bulgaria to set up unit to monitor disinformation in media, social networks – Sofia Globe, <https://sofiaglobe.com/2022/05/20/bulgaria-to-set-up-unit-to-monitor-disinformation-in-media-social-networks/>
- 534) US Military Annoyed When Facebook and Twitter Removed Its PSYOP Bots – The Byte, <https://futurism.com/the-byte/us-military-social-psyop-bots>
- 535) Facebook takes down Russian network impersonating European news outlets – NPR, <https://www.npr.org/2022/09/27/1125217316/facebook-takes-down-russian-network-impersonating-european-news-outlets>

536) Experts: Russia finding new ways to spread propaganda vídeos – Associated Press, <https://apnews.com/article/russia-ukraine-technology-misinformation-0da59f7a72705c5f3fdb59af1fc7af0>

537) China uses AI to generate propaganda on YouTube, report finds – Radio Free Asia, <https://www.rfa.org/english/news/china/china-ai-propaganda-12212023142908.html>

538) The New Normal: The Coming Tsunami of Fakery – Grandy, <https://grandy.substack.com/p/the-new-normal-the-coming-tsunami>

539) To Fight Misinformation, We Need to Teach That Science Is Dynamic – Scientific American, <https://www.scientificamerican.com/article/to-fight-misinformation-we-need-to-teach-that-science-is-dynamic/>

540) Numerous orgs hacked after installing weaponized open source apps – Ars Technica, <https://arstechnica.com/information-technology/2022/09/north-korean-threat-actors-are-weaponizing-all-kinds-of-open-source-apps/>

541) Listen to an AI voice actor try and flirt with you – The Verge, <https://www.theverge.com/2022/2/17/22936978/ai-voice-speech-synthesis-audio-deepfake-sonantic-flirtation>

542) Companies are using AI to monitor your mood during sales calls. Zoom might be next. - Protocol, <https://www.protocol.com/enterprise/emotion-ai-sales-virtual-zoom>

543) Intel calls its AI that detects student emotions a teaching tool. Others call it 'morally reprehensible.' - Protocol, <https://www.protocol.com/enterprise/emotion-ai-school-intel-edutech>

544) We built a 'brain' from tiny silver wires. It learns in real time, more efficiently than computer-based AI – The Conversation, <https://theconversation.com/we-built-a-brain-from-tiny-silver-wires-it-learns-in-real-time-more-efficiently-than-computer-based-ai-216730>

545) AI image generation tech can now create life-wrecking deepfakes with ease – Ars Technica, <https://arstechnica.com/information-technology/2022/12/thanks-to-ai-its-probably-time-to-take-your-photos-off-the-internet/>

546) Deepfakes are now trying to change the course of war – CNN, <https://edition.cnn.com/2022/03/25/tech/deepfakes-disinformation-war/index.html>

547) Deepfake video of Volodymyr Zelensky surrendering surfaces on social media – The Telegraph (Youtube), <https://youtu.be/X17yrEV5sl4>

548) "As fotos vão para a tua família." Chantagem e manipulação de imagens por Inteligência Artificial – Observador, <https://observador.pt/especiais/as-fotos-vaio-para-a-tua-familia-chantagem-e-manipulacao-de-imagens-por-inteligencia-artificial/>

549) Paolla Oliveira faz denúncia após ser vítima de montagem com inteligência artificial – Notícias da TV, <https://noticiasdatv.uol.com.br/noticia/celebridades/paolla-oliveira-faz-denuncia-apos-ser-vitima-de-montagem-com-inteligencia-artificial-122776>

550) Bollywood stars fight for personality rights amid deepfake surge – BBC, <https://www.bbc.com/news/articles/cz08y4ppvr5o;>

551) A “Laudate Deum” e a Inteligência Artificial – 7 Margens, <https://setemargens.com/a-laudate-deum-e-a-inteligencia-artificial/>

552) The growing energy footprint of artificial intelligence – Joule, [https://www.cell.com/joule/fulltext/S2542-4351\(23\)00365-3?returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2542435123003653%3Fshowall%3Dtrue](https://www.cell.com/joule/fulltext/S2542-4351(23)00365-3?returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2542435123003653%3Fshowall%3Dtrue)

553) Guterres defende acesso dos países em desenvolvimento à Inteligência Artificial – RTP Notícias, https://www.rtp.pt/noticias/mundo/guterres-defende-acesso-dos-paises-em-desenvolvimento-a-inteligencia-artificial_n1526532

554) They're Making Technology Worse - (On Purpose) – Upper Echelon (Youtube), <https://www.youtube.com/watch?v=mbmLJViWwIc;>

555) How to Be Free in an Unfree World - Academy of Ideas, <https://academyofideas.com/2020/04/how-to-be-free-in-an-unfree-world/>

556) Document 32014L0053 - EUR-Lex, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1542030329526&uri=CELEX:32014L0053>

557) The Cell Phone Radiation Scandal: Top Brands are Lying About Safety - The Truth About Cancer, <https://thetruthaboutcancer.com/cell-phone-radiation-scandal/>

558) The Latest Outcome for the Apple iPhone Radiation Class Action Lawsuit – HTC America, <https://hctamerica.com/radio-frequency-testing/iphone-radiation-class-action-lawsuit/>

559) Apple Dodges iPhone Radiation Class Action Suit – Courthouse News Service, <https://www.courthousenews.com/apple-dodges-iphone-radiation-class-action-suit/>

560) Microwave Emissions From Cell Phones Exceed Safety Limits in Europe and the US When Touching the Body - IEEE, <https://ieeexplore.ieee.org/document/8688629>

561) Fight Over Berkeley Cellphone Warnings Returns to Court - Courthouse News Service, <https://www.courthousenews.com/fight-over-berkeley-cellphone-warning-mandate-returns-to-federal-court/>

562) Validation of Potential Effects on Human Health of in Vivo Experimental Models Studied in Rats Exposed to Sub-Thermal Radiofrequency. Possible Health Risks Due to the Interaction of Electromagnetic Pollution and Environmental Particles – IEEE Xplore, <https://ieeexplore.ieee.org/document/8737903>

563) Matosinhos com 5G da NOS e da Huawei - it channel, <https://www.itchannel.pt/news/redes-and-telecom/matosinhos-com-5g-da-nos-e-huawei>

564) Operadoras de telecomunicações chinesas lançam serviços 5G esta sexta-feira - Jornal de Notícias, <https://www.jn.pt/mundo/operadoras-de-telecomunicacoes-chinas-lancam-servicos-5g-esta-sexta-feira-11466452.html>

565) 5G: Altice pede dissolução da administração da Anacom - it news, <https://www.itchannel.pt/news/redes-and-telecom/5g-altice-pede-dissolucao-da-administracao-da-anacom>

566) Health Concerns May Slow Rollout of Super-Fast 5G Mobile Networks, Analyst Warns - Fortune, <https://fortune.com/2019/05/22/health-concerns-5g-cellphones-cancer/>

567) Trump Urgently Pushes for 5G! Elon musk Issues WARNINGS!!! - WeAreChange, <https://www.youtube.com/watch?v=rmbW7ktlV5I>

568) Swisscom launches 5G network in 102 locations in Switzerland - The Local ch, <https://www.thelocal.ch/20190417/swisscom-launches-5g-network-in-102-locations-in-switzerland>

569) Court deals blow to FCC's bid to speed 5G rollout - CNN, <https://edition.cnn.com/2019/08/09/tech/5g-fcc-regulations-ruling/index.html>

570) Aliens! 5G Stopped In Cali? Trump Takes On World At G20 PLUS A LOT MORE - WeAreChange, <https://www.youtube.com/watch?v=qho0UXhrUz4&t=28s>

571) Mobile industry 'shouldn't wait' for 5G to roll out small cells - TechRadar, <https://www.techradar.com/news/mobile-industry-shouldnt-wait-for-5g-to-roll-out-small-cells>

572) 5G Is The Future And That Is Frightening! - WeAreChange,
<https://www.youtube.com/watch?v=3AFTxADq4GI>

573) 5G can be tonic for smartphone saturation - TechRadar,
<https://www.techradar.com/news/5g-can-be-tonic-for-smartphone-saturation>

574) GSMA: Operators need prime spectrum to fulfill 5G potential - TechRadar,
<https://www.techradar.com/news/gsma-operators-need-prime-spectrum-to-fulfill-5g-potential>

575) European mobile giants urge pro-5G investment policies - TechRadar,
<https://www.techradar.com/news/european-mobile-giants-urge-pro-5g-investment-policies>

576) Barriers to 5G could stop UK being a global leader - TechRadar,
<https://www.techradar.com/news/barriers-to-5g-could-stop-uk-being-a-global-leader>

577) Expensive spectrum puts European 5G at risk - TechRadar,
<https://www.techradar.com/news/expensive-spectrum-puts-european-5g-at-risk>

578) 5G will help smartphone sales recover in late 2019 - TechRadar,
<https://www.techradar.com/news/5g-will-help-smartphone-sales-recover-in-late-2019>

579) Ericsson: Consumers will pay more for 5G and there are use cases - TechRadar,
<https://www.techradar.com/news/ericsson-consumers-will-pay-more-for-5g-and-there-are-use-cases>

580) 5G set to deliver £15.bn in business revenue by 2025 - TechRadar,
<https://www.techradar.com/news/5g-set-to-deliver-pound157bn-in-business-revenue-by-2025>

581) FC Barcelona's Nou Camp will be 'first' 5G stadium - TechRadar,
<https://www.techradar.com/news/fc-barcelonas-nou-camp-will-be-first-5g-stadium>

582) 5G will account for a quarter of UK mobile data traffic by 2022 - TechRadar,
<https://www.techradar.com/news/5g-will-account-for-a-fifth-of-uk-mobile-data-traffic-by-2022>

583) UK switches on first 5G factory trials- TechRadar,
<https://www.techradar.com/news/uk-switches-on-first-5g-factory-trials>

584) Nokia says it is the one-stop shop for 5G network gear - TechRadar,
<https://www.techradar.com/news/nokia-says-it-is-the-one-stop-shop-for-5g-network-gear>

- 585) Intel wants to be your one-stop shop for 5G -TechRadar,
<https://www.techradar.com/news/intel-wants-to-be-your-one-stop-shop-for-5g>
- 586) Huawei will do 'anything' to be trusted 5G partner - TechRadar,
<https://www.techradar.com/news/huawei-will-do-anything-to-be-trusted-5g-partner>
- 587) 5G could add billions to world GDP - TechRadar,
<https://www.techradar.com/news/5g-could-add-billions-to-world-gdp>
- 588) Landmark Study on Impact of 5G Mobile Technology Released - Qualcomm,
<https://www.qualcomm.com/news/releases/2017/01/17/landmark-study-impact-5g-mobile-technology-released>
- 589) Security and cost worries could harm 5G - TechRadar,
<https://www.techradar.com/news/security-and-cost-worries-could-harm-5g>
- 590) 5G Swiss Telcos Ignore Official Laws and Launch 5G; Rule Of Law Under Attack - Take Back Your Power, <https://takebackyourpower.net/5g-swiss-telcos-ignore-laws-and-launch-5g-rule-of-law-under-attack/>
- 591) Japanese government will hack citizens' IoT devices - TechRadar,
<https://www.techradar.com/news/japanese-government-will-hack-citizens-iot-devices>
<https://www.techradar.com/news/japanese-government-will-hack-citizens-iot-devices>
- 592) Trump lays out US 5G strategy - TechRadar, <https://www.techradar.com/news/trump-signs-order-laying-out-us-5g-strategy>
- 593) US set to lose out to China in 5G race - TechRadar,
<https://www.techradar.com/news/us-set-to-lose-out-to-china-in-5g-race>
- 594) Five Eyes "needs major 5G vendor" - TechRadar,
<https://www.techradar.com/news/five-eyes-needs-major-5g-vendor>
- 595) Secure 5G networks: Commission endorses EU toolbox and sets out next steps – European Commission, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123
- 596) Secure 5G networks: Questions and Answers on the EU toolbox – European Commission, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127
- 597) Huawei & ZTE banned from Australia 5G networks - TechRadar,
<https://www.techradar.com/news/huawei-and-zte-banned-from-australia-5g-networks>

598) Trump vows not to nationalise 5G as FCC makes funding and spectrum available - TechRadar, <https://www.techradar.com/news/trump-vows-not-to-nationalise-5g-as-fcc-makes-funding-and-spectrum-available>

599) US urges EU to reconsider role of Huawei in 5G - TechRadar, <https://www.techradar.com/news/us-urges-eu-to-reconsider-role-of-huawei-in-5g>

600) Huawei faces US probe as Germany considers 5G options - TechRadar, <https://www.techradar.com/news/huawei-faces-us-probe-as-germany-considers-5g-options>

601) European Huawei and ZTE 5G ban would cost operators 55 billion euros <https://www.techradar.com/news/european-huawei-and-zte-5g-ban-would-cost-operators-euro55bn>

602) Huawei 5G ban could cost UK economy £6.8bn - TechRadar, <https://www.techradar.com/news/huawei-5g-ban-could-cost-uk-economy-pound68bn>

603) UK 'doesn't need to ban' Huawei 5G kit - TechRadar, <https://www.techradar.com/news/uk-doesnt-need-to-ban-huawei-5g-kit>

604) UK government won't rush 5G security report despite growing operator unrest - TechRadar, <https://www.techradar.com/news/uk-government-wont-rush-5g-security-report-despite-growing-operator-unrest>

605) China urges UK to act independently over Huawei and 5G - TechRadar, <https://www.techradar.com/news/china-urges-uk-to-act-independently-over-huawei-and-5g>

606) MPs: No technical reason to ban Huawei from UK 5G - TechRadar, <https://www.techradar.com/news/mps-no-technical-reason-to-ban-huawei-from-uk-5g>

607) The UK will let Huawei build selected parts of its 5G infrastructure - TechRadar, <https://www.techradar.com/news/the-uk-will-let-huawei-build-selected-parts-of-its-5g-infrastructure>

608) Huawei works on 5G with Russian operator MTS - TechRadar, <https://www.techradar.com/news/huawei-works-on-5g-with-russian-operator-mts>

609) Huawei looks to capitalise on 5G demand with new Brazil factory - TechRadar, <https://www.techradar.com/news/huawei-looks-to-capitalise-on-5g-demand-with-new-brazil-factory>

610) UK 'needs to create Huawei 5G competitor' - TechRadar, <https://www.techradar.com/news/uk-needs-to-create-huawei-5g-competitor>

- 611) UK's Huawei decision ends uncertainty for 5G operators - TechRadar, <https://www.techradar.com/news/uks-huawei-decision-ends-uncertainty-for-5g-operators>
- 612) The unsung heroes of 5G: which companies are pushing the tech forward? - TechRadar, <https://www.techradar.com/news/the-unsung-heroes-of-5g>
- 613) Huawei controversies timeline - Computerworld, <https://www.computerworld.com/article/3427998/huawei-controversies-timeline.html>
- 614) Huawei ban: Full timeline as Trump's tech chief slams countries working with Chinese company - CNET, <https://www.cnet.com/news/huawei-ban-full-timeline-fcc-carriers-china-trump-ban-security-threat-mate-x/>
- 615) U.S.'s Pompeo: Nations should rethink use of China's Huawei amid coronavirus - Reuters, <https://www.reuters.com/article/us-huawei-tech-usa-pompeo/u-s-s-pompeo-nations-should-rethink-use-of-chinas-huawei-amid-coronavirus-idUSKBN21Z21J>
- 616) Europe Is Taking a Harder Look at China After Virus Suspicions - Bloomberg, <https://www.bloomberg.com/news/articles/2020-04-17/europe-is-taking-a-harder-look-at-china-after-virus-suspicions>
- 617) Exclusive: U.S. drafts rule to allow Huawei and U.S. firms to work together on 5G standards - sources - Reuters, <https://www.reuters.com/article/us-usa-china-huawei-tech-exclusive/exclusive-u-s-drafts-rule-to-allow-huawei-and-u-s-firms-to-work-together-on-5g-standards-sources-idUSKBN22I1ZY>
- 618) Trump could withdraw US spy planes and agents from the UK if Boris Johnson pushes ahead with Huawei 5G deal - Business Insider, <https://www.businessinsider.com/us-could-withdraw-spy-planes-agents-uk-huawei-5g-deal-2020-5>
- 619) Shunned by U.S., Huawei Winning China's \$170 Billion 5G Race - Bloomberg Quint, <https://www.bloombergquint.com/business/shunned-by-u-s-huawei-winning-in-china-s-170-billion-5g-race>
- 620) Acordo entre Reino Unido e Huawei para redes 5G é uma "decisão firme" e não deverá ser repensada - Sapo Tek, <https://tek.sapo.pt/noticias/telecomunicacoes/artigos/acordo-entre-reino-unido-e-huawei-para-redes-5g-e-uma-decisao-firme-e-nao-devera-ser-repensada>
- 621) The EU rewrote a report detailing China's coronavirus 'disinformation' campaign following pressure from Beijing - Business Insider, <https://www.businessinsider.com/coronavirus-eu-rewrote-coronavirus-disinformation-report-china-pressure-covid-2020-4>

- 622) Virus crisis will open doors to Huawei 5G in Europe - Asian Times,
<https://asiatimes.com/2020/04/virus-crisis-will-open-doors-to-huawei-5g-in-europe/>
- 623) Washington's Anti-Huawei Tactics Need a Reboot In Europe - Foreign Policy,
<https://foreignpolicy.com/2020/04/30/huawei-5g-europe-united-states-china/>
- 624) US targets Huawei with tighter chip export rules; China could retaliate - Business Standard,
https://www.business-standard.com/article/international/us-targets-huawei-with-tighter-chip-export-rules-china-eyes-retaliation-120051600116_1.html
- 625) U.S. extends temporary general license for Huawei - Reuters,
<https://www.reuters.com/article/us-usa-china-huaweitech/u-s-extends-temporary-general-license-for-huawei-idUSKBN22R1NT>
- 626) Huawei consegue certificação no 5G mas vê Trump tirar chips (e Google) - Dinheiro Vivo,
<https://www.dinheirovivo.pt/buzz/huawei-consegue-certificacao-no-5g-mas-ve-trump-tirar-google-e-acesso-a-chips/>
- 627) China asks US to stop 'unreasonable suppression' of Huawei - Reuters,
<https://www.reuters.com/article/us-usa-huawei-tech/china-asks-united-states-to-stop-unreasonable-suppression-of-huawei-idUSKBN22S0DE>
- 628) Canada to ban Huawei and ZTE from its 5G networks – MSN,
<https://www.msn.com/en-us/news/technology/canada-to-ban-huawei-and-zte-from-its-5g-networks/ar-AAXuYi1>
- 629) Huawei teardown shows US ban made company turn to Chinese parts - Nikkei,
<https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-teardown-shows-US-ban-made-company-turn-to-Chinese-parts>
- 630) Huawei Loses Millions Of Users As Serious New Threat From China Gets Real - Forbes,
<https://www.forbes.com/sites/zakdoffman/2020/05/16/huawei-loses-millions-of-users-as-serious-new-threat-from-china-gets-real/#35a8d49e4891>
- 631) Governo português não vai impedir Huawei ou qualquer outra marca de fornecer tecnologias 5G - Exame Informática,
<https://visao.sapo.pt/exameinformatica/noticias-ei/mercados/2020-06-05-governo-portugues-nao-vai-impedir-huawei-ou-qualquer-outra-marca-de-fornecer-tecnologias-5g/>
- 632) Eric Schmidt, ex-CEO da Google, diz que a Huawei encaminhou dados para Pequim-Pplware,
<https://pplware.sapo.pt/informacao/eric-schmidt-ex-ceo-da-google-diz-que-a-huawei-encaminhou-dados-para-pequim/>

- 633) Trump administration claims Huawei 'backed by Chinese military' – BBC, News, <https://www.bbc.com/news/business-53172057>
- 634) Trump wants to help Cisco buy Nokia or Ericsson to ruin Huawei's 5G plans – Input, <https://www.inputmag.com/culture/trump-wants-to-help-cisco-buy-nokia-or-ericsson-to-rival-huawei-at-5g>
- 635) Ericsson CEO Signals U.S. Ownership Would Not Be Appropriate – Bloomberg, <https://www.bloomberg.com/news/articles/2020-06-17/ericsson-ceo-signals-u-s-ownership-would-not-be-appropriate-kbjq95p>
- 636) Deutsche Telekom intensifica parceria com Huawei para o 5G – O Jornal Económico, <https://jornaleconomico.sapo.pt/noticias/deutsche-telekom-intensifica-parceria-com-huawei-para-o-5g-610284>
- 637) França não proibirá a Huawei, mas incentivará as empresas de comunicações 5G a evitá-la – Pplware, <https://pplware.sapo.pt/informacao/franca-nao-proibira-huawei-incentivara-empresas-comunicacoes-5g-evita-la>
- 638) Huawei's window of opportunity closes: how geopolitics triumphed over technology – The Conversation, <https://theconversation.com/huaweis-window-of-opportunity-closes-how-geopolitics-triumphed-over-technology-142158>
- 639) Huawei will not be prevented from investing in France: Le Maire – Reuters, <https://www.reuters.com/article/us-france-huawei-idUSKCN24M0S6>
- 640) UK to ban Huawei from 5G network – Reuters, <https://www.reuters.com/article/us-britain-huawei-ban-idUSKCN24F1CX>
- 641) UK officials reportedly told Huawei its 5G ban could be revisited if Trump loses the 2020 election – Business Insider, <https://www.businessinsider.com/uk-reportedly-tells-huawei-5g-ban-could-be-revisited-2020-7>
- 642) U.K. to Support Nokia and Ericsson in Huawei Phase-Out Plan – Bloomberg, <https://www.bloomberg.com/news/articles/2020-07-22/u-k-to-support-nokia-and-ericsson-in-huawei-phase-out-plan>
- 643) China May Retaliate Against Nokia and Ericsson If EU Countries Move to Ban Huawei – Wall Street Journal, <https://www.wsj.com/articles/china-may-retaliate-against-nokia-and-ericsson-if-eu-countries-move-to-ban-huawei-11595250557>

- 644) China Sends Huawei Soaring To Dizzy New Heights – Forbes,
<https://www.forbes.com/sites/zakdoffman/2020/07/28/china-huawei-soaring-trump-blacklist-5g-iphone-xiaomi-update/>
- 645) Ericsson: 5G Winner By No Contest – Seeking Alpha,
<https://seekingalpha.com/article/4361829-ericsson-5g-winner-no-contest>
- 646) Qualcomm forecasts sales above estimates, settles dispute with Huawei – Yahoo! Finance, <https://finance.yahoo.com/news/qualcomm-forecasts-current-quarter-revenue-200510342.html>
- 647) Huawei Supplier Hires Ex-U.S. Official as China Tensions Grow- Yahoo! Finance, <https://finance.yahoo.com/news/huawei-supplier-hires-ex-u-052719534.html>
- 648) Embaixador alerta possível debandada de empresas se Brasil aceitar 5G da Huawei – Gazeta Brasil, <https://gazetabrasil.com.br/mundo/embaixador-alerta-possivel-debandada-de-empresas-se-brasil-aceitar-5g-da-huawei/>
- 649) Huawei: Banned and Permitted in Which Countries? List and FAQ - Channele2e, <https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/>
- 650) Europe telecoms lobby group 'denounces' bans on Chinese vendors – Reuters, <https://www.reuters.com/article/us-huawei-europe/europe-telecoms-lobby-group-denounces-bans-on-chinese-vendors-idUSKBN2711I7>
- 651) Poland spy arrest: China telecoms firm Huawei sacks employee – BCC, <https://www.bbc.com/news/world-europe-46851777>
- 652) Which countries have banned Huawei products – Statista, <https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products/>
- 653) Spotlight: Who leads Brazil's Cloud Market? - Bnamericas, <https://www.bnamericas.com/en/features/spotlight-who-leads-brazils-cloud-market-and-in-which-verticals>
- 654) China going local in Latin America, harvesting data – Bnamericas, <https://www.bnamericas.com/en/interviews/china-going-local-in-latin-america-harvesting-data>
- 655) Huawei Launches 5G in Bangladesh in Collaboration with Teletalk – Huawei, <https://www.huawei.com/en/news/2021/12/bangladesh-5g-launch>

656) Top 3 reasons why Huawei remains first in the Chinese 5G smartphone market – Gizchina, <https://www.gizchina.com/2021/12/20/top-3-reasons-why-huawei-remains-first-in-the-chinese-5g-smartphone-market/>

657) NATO's New Focus Reflects China's Rise – VOA, <https://www.voanews.com/a/nato-s-new-focus-reflects-china-s-rise-/6282496.html>

658) Speech by NATO Secretary General Jens Stoltenberg at the event: NATO's outlook towards 2030 and beyond – OTAN, https://www.nato.int/cps/en/natohq/opinions_189089.htm

659) China: A nemesis that NATO wouldn't want – The Pioneer, <https://www.dailypioneer.com/2021/columnists/china--a-nemesis-that-nato-wouldn---t-want.html>

660) NATO – Wikipedia, <https://en.wikipedia.org/wiki/NATO>

661) Organização do Tratado do Atlântico Norte - Wikipedia, https://pt.wikipedia.org/wiki/Organiza%C3%A7%C3%A3o_do_Tratado_do_Atl%C3%A2ntico_Norte

662) Belt and Road Initiative – Wikipedia, https://en.wikipedia.org/wiki/Belt_and_Road_Initiative

663) China investe pesado na nova rota da seda – Com Ciência, <https://www.comciencia.br/a-nova-rota-da-seda-na-pandemia/>

664) China's 2022 Government Work Report Looks Inward to Economic Stabilizers - The Diplomat, <https://thediplomat.com/2022/03/chinas-2022-government-work-report-looks-inward-to-economic-stabilizers/>

665) The Backlash to Huawei's Global 5G Expansion – Carnegie Endowment for International Peace, <https://carnegieendowment.org/publications/interactive/huawei-timeline#>

666) Criticism of Huawei - Wikipedia, https://en.wikipedia.org/wiki/Criticism_of_Huawei

667) Xiaomi acusada de estar a recolher demasiados dados dos seus utilizadores - pplware, <https://pplware.sapo.pt/smartphones-tablets/android/xiaomi-acusada-de-estar-a-recolher-demasiados-dados-dos-seus-utilizadores/>

668) Xiaomi domina lista de celulares que emitem mais radiação; veja o ranking - Olhar Digital, <https://olhardigital.com.br/noticia/xiaomi-domina-lista-de-celulares-que-emitem-mais-radiacao-veja-o-ranking/89649>

669) The Phones Emitting the Most Radiation – Statista, <https://www.statista.com/chart/12797/the-phones-emitting-the-most-radiation/>

670) SAR Suche - Bundesamt für Strahlenschutz, http://www.bfs.de/SiteGlobals/Forms/Suche/BfS/DE/SARsuche_Formular.html?gts=6048912_list%253DSAREar_double%252Bdesc&csstring_SARAdditional=aktuell

671) The race to 5G explained - Youtube, <https://www.youtube.com/watch?v=ou27oYe5a6g>

672) 5G – Wikipedia, <https://en.wikipedia.org/wiki/5G>

673) ITU towards “IMT for 2020 and beyond” – ITU, <https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx>

674) 5G Timescales & Timeline - Electronic Notes, <https://www.electronics-notes.com/articles/history/cellphone-history/5g-history-timeline-dates.php>

675) Who invented 5G? - Qualcomm, <https://www.qualcomm.com/5g/what-is-5g>

676) From 1G to 5G: A Brief History of the Evolution of Mobile Standards – Brain Bridge, <https://www.brainbridge.be/en/blog/1g-5g-brief-history-evolution-mobile-standards>

677) IMT 2020 – Wikipedia, <https://en.wikipedia.org/wiki/IMT-2020>

678) What Is IMT-2020? - SDx Central, <https://www.sdxcentral.com/5g/definitions/what-is-5g/5g-standards/imt-2020/>

679) 5G Action plan – European Commission, <https://digital-strategy.ec.europa.eu/en/policies/5g-action-plan>

680) Europe’s 5G Action Plan – European Commission, <https://digital-strategy.ec.europa.eu/en/library/europes-5g-action-plan>

681) Legislative Train Schedule – European Parliament, <https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-5g-action-plan>

682) What is the European 5G Observatory? - European 5G Observatory,
<https://5gobservatory.eu/about/what-is-the-european-5g-observatory/>

683) THE 5G Action Plan - European 5G Observatory,
<https://5gobservatory.eu/category/5g-action-plan/>

684) Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho de 11 de Dezembro de 2018 que Estabelece o Código Europeu das Comunicações Eletrónicas - EUR-Lex.europa.eu, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018L1972&from=fr>

685) Plano Estratégico do Espetro – ANACOM,
https://www.anacom.pt/streaming/decisaofinalplanoespectro10082016.pdf?contentId=1392818&field=ATTACHED_FILE

686) História – ANACOM, <https://www.anacom.pt/render.jsp?categoryId=83290>

687) NOS integra a primeira zona livre tecnológica em Portugal – NOS,
https://www.nos.pt/institucional/PT/media/Documents/2019%2004%2002_%20NOS%20e%20CEiiA%20na%20primeira%20ZTL-PR%205G.pdf

688) NOS demonstra 5G aplicado à vigilância das praias em Matosinhos – NOS,
<https://news.cision.com/pt/nos/r/nos-demonstra-5g-aplicado-a-vigilancia-das-praias-em-matosinhos,c636958644070000000>

689) NOS torna Matosinhos na primeira cidade 5G em Portugal – NOS,
<https://www.nos.pt/institucional/PT/media/Documents/NOS%20torna%20Matosinhos%20na%20primeira%20cidade%205G%20em%20Portugal.pdf>

690) Aprovado | PAN Matosinhos pede urgência na realização de campanha de informação sobre o 5G – PAN, <https://pan.com.pt/aprovado-pan-matosinhos-pede-urgencia-na-realizacao-de-campanha-de-informacao-sobre-o-5g/>

691) Aveiro Tech City Lança Novos Desafios – Câmara Municipal de Aveiro,
<https://www.cm-aveiro.pt/inovacao/aveiro-steam-city/noticia/aveiro-tech-city-lanca-novos-desafios>

692) Aveiro 5G Challenges – Câmara de Aveiro,
<https://www.aveirotechcity.pt/pt/atividades/aveiro-5g-challenges>

693) Anacom anuncia leilão do 5G para abril de 2020 - Observador,
<https://observador.pt/2019/10/23/anacom-anuncia-leilao-do-5g-para-abril-de-2020/>

694) CDS-PP vai propor à Assembleia da República que organize conferência sobre o 5G - Observador, <https://observador.pt/2020/03/08/cds-pp-vai-propor-a-assembleia-da-republica-que-organize-conferencia-sobre-o-5g/>

695) Anacom pode obrigar operadoras à partilha de rede no leilão do 5G - ECO, <https://eco.sapo.pt/2020/01/09/anacom-pode-obrigar-operadoras-a-partilha-de-rede-no-leilao-do-5g/>

696) Anacom vai aumentar número de lotes do leilão para o 5G - Jornal de Negócios, <https://www.jornaldenegocios.pt/empresas/telecomunicacoes/detalhe/anacom-vai-aumentar-numero-de-lotes-do-leilao-para-o-5g>

697) Grupo Nowo/Oni disponível para ir ao leilão do 5G - O Jornal Económico, <https://jornaleconomico.sapo.pt/noticias/grupo-nowo-oni-disponivel-para-ir-ao-leilao-do-5g-596620>

698) ANACOM divulga condições do leilão do 5G e de outras faixas relevantes – ANACOM, <https://anacom.pt/render.jsp?contentId=1567662>

699) 5G: Portugal vai ter "um recorde" de quantidade de espectro no leilão - Notícias Ao Minuto <https://www.noticiasao minuto.com/economia/1390835/5g-portugal-vai-ter-um-recorde-de-quantidade-de-espectro-no-leilao>

700) Operadoras limitam valor do leilão do 5G a cem milhões - Eco, <https://eco.sapo.pt/2020/01/24/operadoras-limitam-valor-do-leilao-do-5g-a-cem-milhoes-cada/>

701) Anacom deverá fazer novo leilão para 5G “ultrarrápido” em 2023 - Eco, <https://eco.sapo.pt/2020/03/11/anacom-devera-fazer-novo-leilao-para-5g-ultrarrapido-em-2023/>

702) Governo quer uma cidade do interior com 5G até Dezembro - Público, <https://www.publico.pt/2020/02/07/economia/noticia/governo-quer-cidade-interior-5g-ate-dezembro-1903241>

703) Centros de saúde, universidades e PME podem pedir cobertura específica de 5G - Público, <https://www.publico.pt/2020/02/11/economia/noticia/centros-saude-universidades-pme-podem-pedir-cobertura-especifica-5g-1903621/amp>

704) Aprovação do início do procedimento regulamentar do leilão para a atribuição de direitos de utilização de frequências nas faixas dos 700 MHz e outras faixas – ANACOM, <https://www.anacom.pt/render.jsp?contentId=1492822>

- 705) Consulta sobre o projeto de Regulamento do Leilão para a atribuição de DUF nas faixas dos 700 MHz, 900 MHz, 1800 MHz, 2,1 GHz, 2,6 GHz e 3,6 GHz - Anacom, <https://www.anacom.pt/render.jsp?contentId=1502250>
- 706) Consulta pública sobre leilão para o 5G adiada até 1 de abril - Dinheiro Vivo, <https://www.dinheirovivo.pt/telecomunicacoes/consulta-publica-sobre-leilao-para-o-5g-adiada-ate-1-de-abril/>
- 707) Anacom suspende processo de consulta pública para leilão de 5G - Dinheiro Vivo, <https://www.dinheirovivo.pt/telecomunicacoes/anacom-suspende-processo-de-consulta-publica-para-leilao-de-5g/>
- 708) Resolução do Conselho de Ministros n.º 30/2020 - Diário da República Eletrónico, <https://dre.pt/web/guest/home/-/dre/132133788/details/maximized>
- 709) 5G e TDT: voltou a “haver condições” para retomar os trabalhos mas é preciso “prudência” - Sapo Tek, <https://tek.sapo.pt/noticias/telecomunicacoes/artigos/5g-e-tdt-voltou-a-haver-condicoes-para-retomar-os-trabalhos-mas-e-preciso-prudencia>
- 710) 5G. Governo já sinalizou à Altice necessidade de novo plano para migração da TDT - Dinheiro Vivo, <https://www.dinheirovivo.pt/empresas/5g-governo-ja-sinalizou-a-altice-necessidade-de-novo-plano-para-migracao-da-tdt/>
- 711) 5G está suspenso, mas PAN quer esclarecimentos do Governo sobre desenvolvimento da nova rede - Jornal Económico, <https://jornaleconomico.sapo.pt/noticias/pan-pede-esclarecimentos-ao-governo-sobre-implementacao-da-rede-5g-575552>
- 712) Pela segunda vez em dois meses, o PAN questiona o Governo sobre o impacto do 5G no ambiente e na saúde - Jornal Económico, <https://jornaleconomico.sapo.pt/noticias/pela-segunda-vez-em-dois-meses-o-pan-questiona-o-governo-sobre-o-impacto-do-5g-no-ambiente-e-na-saude-594309>
- 713) Anacom retoma processo para atribuição do 5G em Portugal - Sol, <https://sol.sapo.pt/artigo/698611/anacom-retoma-processo-para-atribuicao-do-5g-em-portugal>
- 714) 5G: Anacom retoma dossier e defende obrigações de cobertura da população - Público, <https://www.publico.pt/2020/06/01/economia/noticia/5g-anacom-retoma-dossie-defende-obrigacoes-cobertura-populacao-1918966>
- 715) Sob pressão do setor, Anacom explica 5G no Parlamento - O Jornal Económico, <https://jornaleconomico.sapo.pt/noticias/sob-pressao-do-setor-anacom-explica-no-5g-no-parlamento-597508>

- 716) Os polícias dos mercados – Rádio Renascença, <https://especiais.rr.pt/reportagem-entidades-reguladoras/index.html>
- 717) Leilão do 5G vai realizar-se até ao final do ano, garante a Anacom - Público, <https://www.publico.pt/2020/06/09/economia/noticia/leilao-5g-vai-realizar-se-ate-final-ano-garante-anacom-1920079>
- 718) Portugal: Não haverá 5G em 2020! ANACOM adia leilão das frequências – pplware, <https://pplware.sapo.pt/informacao/portugal-nao-havera-5g-em-2020-anacom-adia-leilao-das-frequencias/>
- 719) Altice regressa ao terreno – Sol, <https://sol.sapo.pt/artigo/702214/altice-regressa-ao-terreno>
- 720) “O mundo mudou” e o 5G “não pode ser a prioridade número um” - Público, <https://www.publico.pt/2020/05/21/economia/noticia/mundo-mudou-5g-nao-prioridade-numero-1917521>
- 721) 5G é “importante”, mas pandemia mostrou que 4G está “à altura dos desafios” - ECO, <https://eco.sapo.pt/2020/05/21/5g-e-importante-mas-pandemia-mostrou-que-4g-esta-a-altura-dos-desafios/>
- 722) Ericsson Portugal pede implementação das redes 5G “o mais rápido possível” - Exame Informática, <https://visao.sapo.pt/exameinformatica/noticias-ei/mercados/2020-05-26-ericsson-portugal-pede-implementacao-das-redes-5g-o-mais-rapido-possivel/>
- 723) Huawei Portugal diz que o 5G será uma “mais valia para a competitividade das empresas” – Jornal Económico, <https://jornaleconomico.sapo.pt/noticias/huawei-portugal-diz-que-o-5g-sera-uma-mais-valia-para-a-competitividade-das-empresas-615846>
- 724) “5G é importante para o país não perder competitividade tecnológica” – Eco, <https://eco.sapo.pt/entrevista/5g-e-importante-para-o-pais-nao-perder-competitividade-tecnologica/>
- 725) Plano de retoma defende aposta no 5G e na fibra ótica para combater desigualdades – Eco, <https://eco.sapo.pt/2020/07/09/plano-de-retoma-defende-aposta-no-5g-e-na-fibra-otica-para-combater-desigualdades/>
- 726) Concorrência: "Setor das telecomunicações tem pouca dinâmica concorrencial". 5G é oportunidade para mudar – O Jornal de Negócios, <https://www.jornaldenegocios.pt/empresas/telecomunicacoes/detalhe/concorrencia-setor-das-telecomunicacoes-tem-pouca-dinamica-concorrencial-5g-e-oportunidade-para-mudar>

727) Governo diz que tecnologia 5G “não está pensada” para cobrir um país inteiro – Eco, <https://eco.sapo.pt/2020/06/23/governo-diz-que-tecnologia-5g-nao-esta-pensada-para-cobrir-um-pais-inteiro/>

728) 5G: Governo acusa Anacom de criar perturbação no mercado e quer uma revisão do regulamento do leilão – SapoTek, <https://tek.sapo.pt/noticias/telecomunicacoes/artigos/5g-governo-acusa-anacom-de-criar-perturbacao-no-mercado-e-quer-uma-revisao-do-regulamento-do-leilao>

729) Governo avisa Anacom: “Espero que cumpra a lei do país” no processo do 5G – Jornal de Negócios, <https://www.jornaldenegocios.pt/empresas/telecomunicacoes/detalhe/governo-avisa-anacom-espero-que-cumpra-a-lei-do-pais-no-processo-do-5g>

730) 5G em Portugal e na Europa (além das questões políticas) – Smart Cities, <https://smart-cities.pt/opiniao-entrevista/5g-pvmeendes-0411/>

731) 5G. Vodafone ameaça com mais um processo, Altice e Nos criticam Anacom – Expresso, <https://expresso.pt/economia/2021-06-01-5G.-Vodafone-ameaca-com-mais-um-processo-Altice-e-Nos-criticam-Anacom-3252761d>

732) António Costa diz que Anacom “inventou o pior modelo de leilão possível” para o 5G - Sapo, <https://eco.sapo.pt/2021/10/20/antonio-costa-diz-que-anacom-inventou-o-pior-modelo-de-leilao-possivel-para-o-5g/>

733) Notícias – ANACOM, <https://www.anacom.pt/render.jsp?categoryId=406877>

734) ANACOM emite DUF à DENSE AIR em resultado do leilão do 5G – ANACOM, <https://www.anacom.pt/render.jsp?contentId=1711179>

735) ANACOM emite DUF e NOS pode iniciar exploração comercial do 5G – ANACOM, <https://www.anacom.pt/render.jsp?contentId=1711165>

736) ANACOM emite DUF e VODAFONE pode iniciar exploração comercial do 5G – ANACOM, <https://www.anacom.pt/render.jsp?contentId=1711277>

737) ANACOM emite DUF à DIXAROBIL em resultado do leilão 5G – ANACOM, <https://www.anacom.pt/render.jsp?contentId=1711414>

738) ANACOM emite DUF e NOWO pode iniciar exploração comercial do 5G – ANACOM, <https://www.anacom.pt/render.jsp?contentId=1711372>

739) ANACOM aprova projeto de decisão sobre a emissão de DUF no leilão do 5G à MEO – ANACOM, <https://www.anacom.pt/render.jsp?contentId=1711783>

740) Anacom lança consulta pública para aferir “interesse” no 5G ultrarrápido - Sapo, <https://eco.sapo.pt/2021/12/13/anacom-lanca-consulta-publica-para-aferir-interesse-no-5g-ultrarrapido/>

741) Este pode finalmente ser o ano do 5G – Sapo, <https://eco.sapo.pt/2022/01/03/este-pode-finalmente-ser-o-ano-do-5g/>

742) Altice Portugal garante cobertura de 5G em todas as capitais de distrito e nas regiões autónomas – Sapo, <https://tek.sapo.pt/noticias/telecomunicacoes/artigos/altice-portugal-garante-cobertura-de-5g-em-todas-as-capitais-de-distrito-e-nas-regioes-autonomas>

743) Ericsson Mobility Report: 5G terá 4,4 mil milhões de clientes em 2027 – APDC, <https://www.apdc.pt/noticias/atualidade-internacional/ericsson-mobility-report-5g-tera-44-mil-milhoes-de-clientes-em-2027>

744) Probabilidade de o país cumprir metas no 5G é "média-alta" apesar do atraso – Dinheiro Vivo, <https://www.dinheirovivo.pt/empresas/telecomunicacoes/probabilidade-do-pais-cumprir-metas-no-5g-e-media-alta-apesar-do-atraso-14523260.html>

745) Proposta de Lei 83/XIV/2 – Assembleia da República, <https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=110660>

746) Proposta de Lei n.º 83/XIV – Assembleia da República, <https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063484d364c793968636d356c6443397a6158526c6379395953565a4d5a5763765247396a6457316c626e527663306c7561574e7059585270646d45765a6a4e6a5a6a63325a6d5574597a677a4e6930305a4449784c546c6d5a54557459544e684d5459304e544269596d466a4c6d527659773d3d&fich=f3cf76fe-c836-4d21-9fe5-a3a16450bbac.doc&Inline=true>

747) Metas do 5G podem estar em causa e operadoras querem mais tempo para cumprir objetivos de cobertura – Sapo, <https://tek.sapo.pt/noticias/telecomunicacoes/artigos/metas-do-5g-podem-estar-em-causa-e-operadoras-querem-mais-tempo-para-cumprir-objetivos-de-cobertura>

748) Operadores pedem mais tempo ao governo para cumprir metas do 5G – Dinheiro Vivo, <https://www.dinheirovivo.pt/empresas/telecomunicacoes/operadores-pedem-mais-tempo-ao-governo-para-cumprir-metas-do-5g-14951973.html>

749) After the virus: A 5G gold rush? - Politico, <https://www.politico.com/news/2020/04/02/coronavirus-5g-network-160296>

- 750) 82 percent of World's E-Waste Not Recycled – Computer Business Review,
<https://www.cbronline.com/news/e-waste-un-report>
- 751) UN reports global e-waste production soared beyond 53 million tonnes in 2019 – ZDNet, <https://www.zdnet.com/article/un-reports-global-e-waste-production-soared-beyond-53-million-tonnes-in-2019/>
- 752) World's E-Waste 'Unsustainable', Says UN Report Citing China, India, and US – Gadget 360°, <https://gadgets.ndtv.com/laptops/news/worlds-e-waste-unsustainable-says-un-report-citing-china-india-and-us-2256324>
- 753) E-waste: Five billion phones to be thrown away in 2022 – BBC,
<https://www.bbc.com/news/science-environment-63245150>
- 754) Why is the EU's right to repair legislation important? - European Parliament,
<https://www.europarl.europa.eu/news/en/headlines/society/20220331STO26410/why-is-the-eu-s-right-to-repair-legislation-important>
- 755) Right to Repair – European Parliament,
[https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698869/EPRS_BRI\(2022\)698869_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698869/EPRS_BRI(2022)698869_EN.pdf)
- 756) European Right To Repair: Poor Repairability Shamed With Rating System – Hackaday, <https://hackaday.com/2020/12/02/european-right-to-repair-poor-repairability-shamed-with-rating-system/>
- 757) Govt plans 'Right to Repair' framework to facilitate self, third party repair of products – The Indian Express, <https://indianexpress.com/article/technology/tech-news-technology/govt-plans-right-to-repair-framework-to-facilitate-self-third-party-repair-of-products-8030785/>
- 758) Why Centre wants to bring in 'Right to repair', and how it will benefit consumers – MSN, <https://www.msn.com/en-in/news/other/why-centre-wants-to-bring-in-e2-80-98right-to-repair-e2-80-99-and-how-it-will-benefit-consumers/ar-AAZzfOI>
- 759) Deal on common charger: reducing hassle for consumers and curbing e-waste - European Parliament,
<https://www.europarl.europa.eu/news/en/press-room/20220603IPR32196/deal-on-common-charger-reducing-hassle-for-consumers-and-curbing-e-wastehttps://www.europarl.europa.eu/news/en/press-room/20220603IPR32196/deal-on-common-charger-reducing-hassle-for-consumers-and-curbing-e-waste>
- 760) EU rules to force USB-C chargers for all phones - BCC,
<https://www.bbc.com/news/technology-58665809>

761) USB-C vai ser obrigatório em todos os smartphones na UE, incluindo iPhones – IGN Portugal, <https://pt.ign.com/iphone-12-2/112948/news/usb-c-vai-ser-obrigatorio-em-todos-os-smartphones-na-ue-incluindo-iphones>

762) Deal on common charger: reducing hassle for consumers and curbing e-waste – The Verge, <https://www.theverge.com/2022/6/7/23156361/european-union-usb-c-wired-charging-iphone-lightning-ewaste>

763) The Brussels Effect: How the European Union Rules the World – Columbia Law School, <https://scholarship.law.columbia.edu/books/232/>

764) Snowden: Tech Workers Are Complicit in How Their Companies Hurt Society – Vice, https://www.vice.com/en_us/article/wxqx8q/snowden-tech-workers-are-complicit-in-how-their-companies-hurt-society

765) Economic inequality has deepened during the pandemic. That doesn't mean it can't be fixed – World Economic Forum, <https://www.weforum.org/agenda/2022/04/economic-inequality-wealth-gap-pandemic/>

766) 5G APPEAL, <http://www.5gappeal.eu/>

767) Over 400 Medical Professionals Sign Letter to the FCC! - 5G Crisis, <https://mailchi.mp/ee004f8b85dc/ready-set-comment-to-the-fcc-5002370>

768) Brighton and Hove City Council join growing list of local authorities banning 5G masts - ITPRO, <https://www.itpro.co.uk/network-internet/34621/brighton-and-hove-city-council-join-growing-list-of-local-authorities-banning>

769) Kaboom! Switzerland Halts 5G Rollout Over Health Concerns - Technocracy News and Trends, <https://www.technocracy.news/switzerland-halts-5g-rollout-over-health-concerns/>

770) Switzerland halts rollout of 5G over health concerns - Financial Times, <https://www.ft.com/content/848c5b44-4d7a-11ea-95a0-43d18ec715f5>

771) Bericht zeigt erstmals: Strahlung von Mobilfunkantennen und Co. liegt unter Grenzwert – Aargauer Zeitung, <https://www.aargauerzeitung.ch/news-service/inland-schweiz/nichtionisierende-strahlung-bericht-zeigt-erstmal-strahlung-von-mobilfunkantennen-und-co-liegt-unter-grenzwert-ld.2304962>

772) Computerworld-Newsticker – Computerworld, <https://www.computerworld.ch/business/unternehmensnachrichten/computerworld-newsticker-2773548.html>

773) Keine neuen 5G-Antennen mehr ohne Bewilligungsverfahren – SRF,
<https://www.srf.ch/news/wirtschaft/neue-mobilfunktechnologie-keine-neuen-5g-antennen-mehr-ohne-bewilligungsverfahren>

774) International Actions To Halt And Delay 5G - Tap News,
<http://tapnewswire.com/2019/05/international-actions-to-halt-and-delay-5g/>

775) BioInitiative 2012, <https://bioinitiative.org/>

776) Princípio da precaução – Wikipedia, https://pt.wikipedia.org/wiki/Princ%C3%ADpio_da_precau%C3%A7%C3%A3o

777) Declaração do Rio de Janeiro - Sci Flo Brasil,
<https://www.scielo.br/j/ea/a/szzGBPjxPqnTsHsnMSxFWPL/?format=pdf&lang=pt>

778) The Precautionary Principle and Enlightened Doomsaying: Rational Choice before the Apocalypse – Arcade, <https://arcade.stanford.edu/occasion/precautionary-principle-and-enlightened-doomsaying-rational-choice-apocalypse>

779) Portugal suspende vacina da AstraZeneca com base no princípio de "precaução em saúde pública" – TVI, <https://tvi.iol.pt/noticias/videos/sociedade/portugal-suspende-vacina-da-astrazeneca-com-base-no-principio-de-precaucao-em-saude-publica/604fc7910cf280db40fd9a6d>

780) Consequencialismo – Wikipedia, <https://pt.wikipedia.org/wiki/Consequencialismo>

781) A baseless paper that linked skin cells, 5G and coronavirus has been retracted - Full Fact, <https://fullfact.org/online/5g-skin-cells-paper/>

782) Report linking 5G to COVID-19 swiftly debunked – Medical Xpress,
<https://medicalxpress.com/news/2020-07-linking-5g-covid-swiftly-debunked.html>

783) What well-being is (and isn't), according to neuroscience | Mary Helen Immordino-Yang – The Well, <https://www.youtube.com/watch?v=jzRrDG9RKfM>

784) Leaked Google research shows company grappling with censorship and free speech – The Verge, <https://www.theverge.com/2018/10/10/17961806/google-leaked-research-good-censor-censorship-freedom-of-speech-research-china>

785) 10 BEST Private Search Engines: Secure Anonymous Search 2022 – Software Testing Help, <https://www.softwaretestinghelp.com/best-private-search-engines/>

786) DuckDuckGo will demote Russian propaganda in search results – Engadget, <https://www.engadget.com/duck-duck-go-reverses-course-will-demote-russian-propaganda-in-search-results-014336389.html>

787) Search Engine Independence – Brave, <https://search.brave.com/help/independence>