RELATÓRIO | TECNOLOGIAS EMERGENTES

Maio 2023

CNCS Centro Nacional de Cibersegurança PORTUGAL
Observatório de Cibersegurança
PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU

Ficha Técnica

Título
Tecnologias Emergentes

Autoria
Rui Luis Aguiar (editor), Mário Antunes, João Paulo Barraca,
Paulo Bartolomeu, Daniel Corujo, Vitor Cunha, Rafael Direito,
Diogo Gomes, Leonardo da Cruz Marcuzzo, Ricardo Martins,
Paulo Mateus, Armando Nolasco Pinto e Nuno Silva
Instituto de Telecomunicações

Coordenação e Revisão
Rui Luis Aguiar e CNCS

Edição
Maio 2023

Conceção gráfica e design da capa
Meio Kilo Unip. Lda.

Paginação
Meio Kilo Unip. Lda.

RELATÓRIO | TECNOLOGIAS EMERGENTES

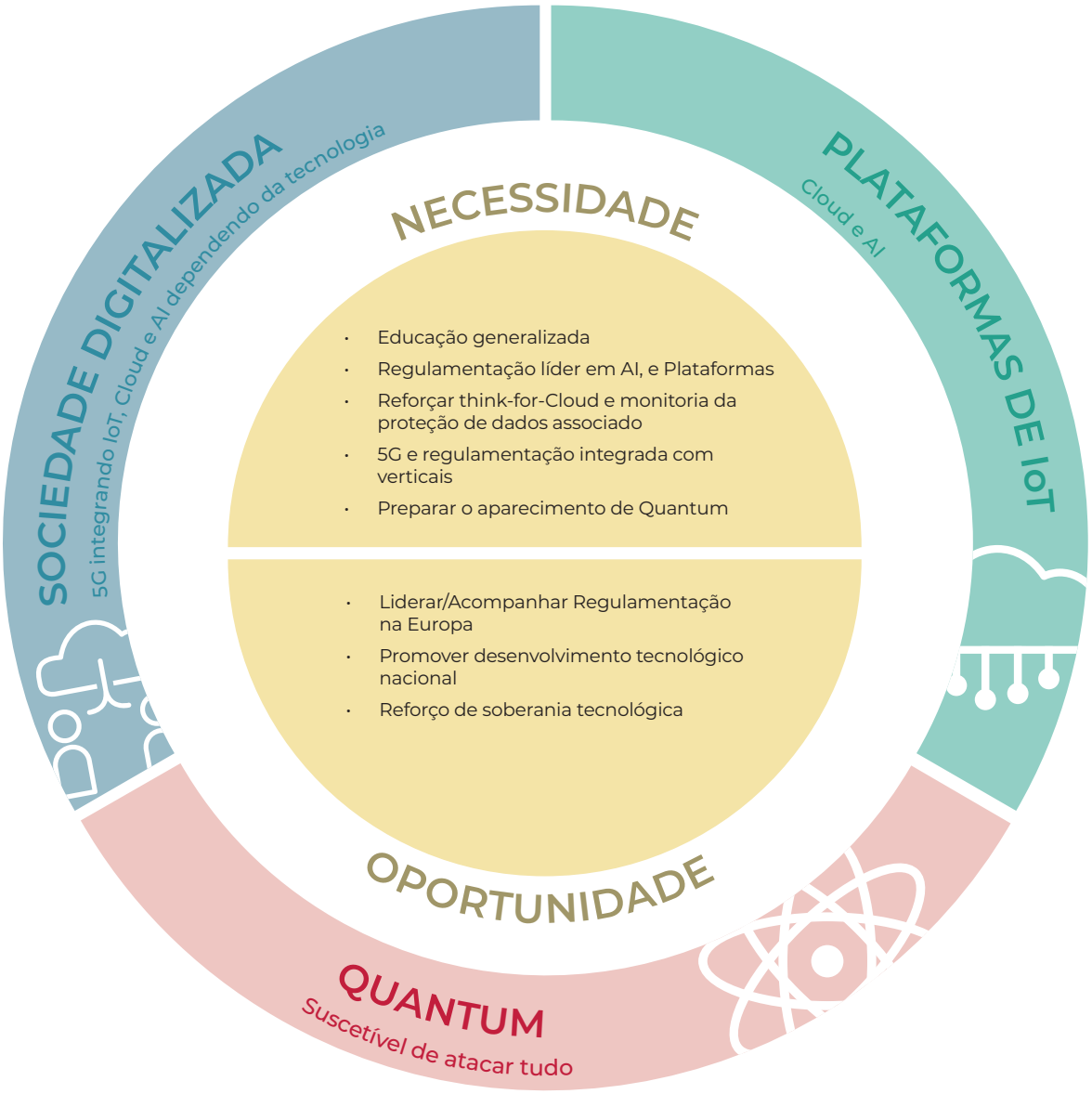
Sumário Executivo

Os problemas da cibersegurança apresentam uma crescente relevância na nossa sociedade. A transição digital em que nos encontramos, com todos os setores a modificarem os seus produtos, processos e serviços para explorarem as virtualidades das tecnologias da informação e comunicação (TIC), aumentou tanto os potenciais perigos de interferência por mecanismos eletrónicos, como o impacto dos mesmos nas diferentes atividades, sectores económicos e interações societais.

Esta realidade, sendo reconhecida, é, no entanto, tratada de uma forma quase pontual: as diferentes instituições, empresas e pessoas maioritariamente reagem a incidentes e preocupações nas circunstâncias em que são criadas, em detrimento de uma abordagem sistémica e estruturada promotora de uma mitigação de base preventiva, baseada num entendimento holístico da intensidade da evolução e obsolescência tecnológica, das relações e impactos inter-tecnologias, e acompanhando as boas práticas e referenciais nacionais e internacionais. As TIC são caracterizadas por elevada intensidade tecnológica, com ritmos de evolução muito elevados. As tecnologias que usamos hoje são substancialmente distintas das que eram usadas cinco anos atrás, e a alteração dos comportamentos e do panorama de risco associados suscita desafios de cibersegurança que são frequentemente associados a especificidades técnicas das tecnologias. Este enquadramento torna necessário uma mudança na abordagem que todas as entidades apresentam, a começar por uma maior resposta *a priori* aos problemas de índole tecnológica que aparecem, em detrimento de uma tradicional abordagem reativa centrada nas circunstâncias presentes.

Este documento apresenta uma visão de cinco tecnologias formadoras do nosso presente e futuro tecnológico, nomeadamente a computação na nuvem (*cloud computing*), a Internet das Coisas (*Internet of Things* ou simplesmente *IoT*), a Inteligência Artificial (AI), a tecnologia móvel 5G, e as tecnologias quânticas. Estas tecnologias serão descritas numa perspetiva histórica, apresentando-se o seu expectável impacto futuro, e salientando-se potenciais aspetos de cibersegurança a serem considerados – designadamente os desafios e as oportunidades.

O documento torna evidente a existência de vários aspetos de cibersegurança em diferentes áreas tecnológicas, evidenciando potenciais impactos futuros e perspetivando abordagens que podem ser consideradas na promoção da resiliência dos sistemas, das entidades e da sociedade.


SOCIEDADE DIGITALIZADA
5G integrando IoT, Cloud e AI dependendo da tecnologia
PLATAFORMAS DE IoT
Cloud e AI
QUANTUM
Suscetível de atacar tudo
NECESSIDADE
Educação generalizada
Regulamentação líder em AI, e Plataformas
Reforçar think-for-Cloud e monitoria da proteção de dados associado
5G e regulamentação integrada com verticais
Preparar o aparecimento de Quantum
OPORTUNIDADE
Liderar/Acompanhar Regulamentação na Europa
Promover desenvolvimento tecnológico nacional
Reforço de soberania tecnológica

ÍNDICE

Lista de figuras

Lista de tabelas

Termos e Abreviaturas

5G	Fifth Generation (mobile/cellular networks)
AI	Artificial Intelligence
AIaaS	Artificial Intelligence as a Service
AIS	Artificial Immune System
ARPANET	Advanced Research Projects Agency Network
DaaS	Desktop as a Service
DARPA	Defense Advanced Research Projects Agency
DB	Database as a Service
DL	Deep Learning
DLT	Distributed Ledger Technologies
DRaaS	Disaster Recovery-as-a-Service
DSA	Digital Signature Algorithm
eMBB	Enhanced Mobile BroadBand
EU	European Union
GPRS	General Packet Radio Service
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IoT	Internet of Things
IIoT	Industrial Internet of Things
KVI	Key Value Indicators
LEO	Low Earth Orbit
ML	Machine Learning
mMTC	Massive Machine Type Communications
NB-IoT	Narrow Band - IoT
OS	Operating System
PaaS	Platform as a Service
PMEs	Pequenas e Médias Empresas
RSA	Rivest Shamir Adleman
SaaS	Software as a Service
SCADA	Supervisory Control And Data Acquisition
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SD-WAN	Software-Defined Wide-Area Networks
SDN	Software Defined Network
TCO	Total Cost Ownership
TLS	Transport Layer Security
TI	Tecnologias de Informação
URLLC	Ultra Reliable Low Latency Communications
VPN	Virtual Private Network
XAI	Explainable AI

É recomendado o acesso ao Glossário da CNCS para mais esclarecimentos sobre terminologia[1].

1 https://www.cncs.gov.pt/pt/glossario/

Introdução

1

A segurança é um tema cada vez mais debatido na nossa sociedade: à medida que esta foi passando por um processo de digitalização crescente (incentivado por um claro aumento da eficiência económica e da qualidade de vida das sociedades que melhor exploram esta digitalização), as vulnerabilidades inerentes a um aumento da interligação entre pessoas e objetos começam a tornar-se cada vez mais relevantes. No contexto atual da nossa sociedade, o aumento da superfície de risco associada a esta maior conectividade tem sido potenciado por novos problemas socioeconómicos (ativistas ideológicos, grupos organizados de crime, aumento do trabalho remoto) e geoestratégicos (competição agressiva entre grandes grupos económicos e entre Estados). As discussões atuais decorrentes das novas realidades impostas pela pandemia (p.ex., sobre mecanismos de trabalho flexíveis) revelam que a digitalização da sociedade é uma realidade inevitável e irreversível, sendo expectável a ocorrência de uma multiplicidade de situações de segurança associadas a essa mesma digitalização.

Diferentes estudos quantificam de forma diferente diferentes parâmetros associados a este problema de segurança. No entanto, diversos relatórios indiciam que o crime cibernético terá tido aumentos de 25%-40% em cada um dos anos de 2020 e 2021[2], revelando uma duplicação de problemas em apenas três anos, precisamente os anos em que a pandemia da COVID19 generalizou o trabalho remoto. Uma análise mais fina a este aumento revela não só uma maior quantidade, mas um conjunto de novos ataques, explorando os desenvolvimentos tecnológicos em diferentes níveis, mostrando a sofisticação e expertise de muitos destes atacantes[3].

Independentemente de todas as boas práticas em termos de sistemas e aplicações, o desenvolvimento tecnológico coloca sempre a sociedade numa posição defensiva, dada a tipicamente lenta adaptação da sociedade: novas tecnologias aumentam a superfície de risco, muitas vezes de modos que só são percetíveis após a prossecução de ataques que exploram esses novos riscos, i.e., a dimensão real do risco só se vai tornando conhecida à medida que as ramificações dessa tecnologia se vão conhecendo. A expressão *fechar a porta de entrada* é atualmente suficientemente conhecida para a população em geral ter este conceito já bem estabelecido, e representa adequadamente a situação da cibersegurança atual: é uma postura defensiva que ajuda a mitigar o risco, mesmo que este ainda esteja por quantificar ou não seja completamente compreendido. Com a velocidade de desenvolvimento de novos ataques, começa a ser importante a comunidade preparar-se para as tecnologias emergentes, que serão particularmente importantes daqui a três ou quatro anos, pois estas colocarão novos problemas quer por aspetos inerentes à tecnologia em si, quer por questões de novos métodos de utilização das mesmas.

2 Global Cybersecurity Outlook 2022, Insight Report, Jan 2022; World Economic Forum
Internet Crime Report 2021, Federal Bureau of Investigation, US.
Relatório Cibersegurança em Portugal, Riscos e Conflitos, Observatório de Cibersegurança, Junho de 2020.

3 Hawdon, J., Parti, K. & Dearden, T.E. Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. Am J Crim Just 45, 546–562 (2020). https://doi.org/10.1007/s12103-020-09534-4
Catching the virus cybercrime, disinformation and the COVID-19 pandemic, Apr 2020, Europol

Este documento ambiciona salientar os impactos que algumas tecnologias emergentes poderão ter na área da cibersegurança, contribuindo para uma maior sensibilização dos potenciais problemas associados e para o desenvolvimento proativo de respostas que possam minimizar os riscos associados. As tecnologias selecionadas para esta análise preliminar são tecnologias consensualmente tidas como potencialmente transformadoras da nossa sociedade, mas que são frequentemente mal compreendidas: as comunicações móveis 5G; a computação na nuvem (*cloud computing*); a inteligência artificial; a Internet-das-Coisas (*Internet of Things* ou *IoT*); e as tecnologias quânticas, todas tecnologias que se perspetivam como elementos constitutivos da nossa sociedade a curto prazo. A utilização destas tecnologias agora e no futuro próximo pode ser sumariada na tabela seguinte.

Tabela 1 - Impactos Futuros

	Presente (2022)	Futuro (2025)
Computação na nuvem	Utilização vasta em diferentes domínios	Sistema de computação de referência para o fornecimento de serviços públicos e privados, essencial para modelo de subscrição de serviços
Internet-das-Coisas	Utilização especializada em diferentes domínios, de forma desestruturada	Ambiente de referência estruturado em múltiplos domínios aplicacionais, incluindo ambientes privados residenciais
Inteligência Artificial	Utilização especializada, e descontrolada, em diferentes domínios	Convergência para metodologias consistentes para utilização global em todos os domínios da sociedade
Comunicações 5G	Implementação gradual de melhorias em redes móveis celulares	Sistema de referência para todas as redes de comunicações durante esta década
Tecnologias quânticas	Utilização especializada em domínios bem identificados	Expansão do alcance dos domínios de uso, para tecnologias alicerce da infraestrutura digital

Estas tecnologias são elementos essenciais para a transição digital que a nossa sociedade está a vivenciar e, como a tabela indica, são já elementos infraestruturais atualmente muito usados, ou em franca expansão. Não é ainda utilizada uma abordagem completamente estruturada aos problemas de cibersegurança que a utilização destas tecnologias de forma isolada ou, e cada vez mais, de forma cumulativa, traz à nossa sociedade. Torna-se, assim, urgente melhorar a nossa compreensão sobre as mesmas, e sobre os riscos que enfrentamos, de forma a podermos encontrar as melhores soluções sociais, legais e técnicas para minorar estes riscos. Uma adequada abordagem nacional a estes problemas permitirá à nossa sociedade reforçar a sua autonomia estratégica e competitividade.

Os capítulos seguintes farão uma pequena retrospetiva sobre cada uma destas tecnologias, irão identificar alguns dos impactos que aquelas terão em termos de segurança, identificando problemas e oportunidades, e, finalmente, apresentarão algumas recomendações para potenciais ações preemptivas associadas a tais tecnologias. De uma forma geral, a discussão será centrada na utilização civil das tecnologias, não detalhando potenciais utilizações em contexto militar ou de infraestruturas críticas. No entanto, há circunstâncias em que, dado o potencial dessas tecnologias, tais dimensões serão brevemente afloradas.

2

Cloud e o Contínuo Computacional

A tecnologia *cloud*, também apelidada de *cloud computing*, tem como base a crescente conectividade entre servidores e computadores de diferentes domínios da internet. Com base nesta conectividade, é possível disponibilizar de forma facilitada, um vasto conjunto de serviços e recursos a diferentes utilizadores, que, para acederem aos mesmos, tipicamente apenas necessitam de um dispositivo com acesso à internet.

A tecnologia *cloud* acaba por permitir, entre outros, a migração de um paradigma de '*on-site computing*' para um paradigma de '*remote computing*', onde os recursos computacionais, muitas vezes virtualizados, são partilhados entre diversos serviços. Isto acaba por resultar em múltiplas vantagens, tradicionalmente identificadas como: (i) redução de custos de infraestrutura, (ii) centralização da informação, (iii) gestão simplificada e centralizada de serviços, (iv) elevada disponibilidade de serviços e recursos, entre outras [1].

Atualmente, é possível distinguir 3 diferentes tipos de *clouds*: (i) *cloud* pública, (ii) *cloud* privada e (iii) *cloud* híbrida. Estas apresentam entre elas grandes variações de custos, disponibilidade, desempenho e facilidade de gestão, pelo que a escolha da sua adoção deve ser suportada por uma análise a priori, dos objetivos que se pretende atingir.

Uma *cloud* pública assenta em recursos oferecidos para utilização pública por um fornecedor externo a um qualquer cliente que os deseje contratar. A gestão dos recursos computacionais nos quais assenta a *cloud* é responsabilidade do fornecedor da mesma, pelo que retira a necessidade de gestão computacional (disponibilidade, escalabilidade, segurança, entre outros) do lado do cliente. Desta forma, a adoção deste tipo de *cloud* permite a um cliente/empresa não só uma potencial poupança, como também uma elevada disponibilidade dos serviços que nela serão alojados. Algumas empresas de relevo mundial como a AWS, a Oracle, a Microsoft e a Google destacam-se como fornecedores de *clouds* públicas. Nas *clouds* públicas a informação é depositada numa infraestrutura remota, supostamente replicada entre vários servidores. **Esses servidores podem encontrar-se em diferentes países, e mesmo em diferentes continentes, e a confidencialidade interna da informação** (i.e. quanto da informação/meta-informação é acessível pelos próprios serviços de *cloud*) **é muito variável com o serviço de cloud a utilizar, estando sujeita às legislações nacionais das geografias desses servidores.**

Por sua vez, uma *cloud* privada é aquela cuja infraestrutura é totalmente disponibilizada a uma organização de uma forma interna. Desta forma, o acesso à mesma fica restrito aos funcionários, parceiros e clientes desta mesma organização, que tiverem autorizações de acesso, não sendo necessário partilhar quaisquer serviços e informações com entidades externas à organização pois todo o sistema é totalmente internalizado. Para além disto, as *clouds* privadas oferecem uma elevada capacidade de personalização para o objetivo pretendido por uma organização, conseguindo suprir as suas necessidades de forma eficaz e célere. É de esperar que **nas *cloud* privadas o local onde a informação é salvaguardada seja perfeitamente identificado (e dentro das instalações da empresa), embora serviços de backup associados possam violar esta expectativa.** Não obstante estarem posicionadas em ambientes

privados, as *clouds* privadas devem obedecer a regulamentos e leis gerais, sobretudo relacionados com o Regulamento Geral sobre a Proteção de Dados (adiante RGPD, ver secção sobre Legislação Adicional), o que gera alguns desafios na gestão das mesmas. No contexto europeu, este tipo de *cloud* tem também maiores custos do que uma *cloud* pública, uma vez que as organizações necessitam de adquirir uma vasta coleção de hardware, onde será disponibilizada a *cloud*, e vários recursos humanos para fazer a gestão deste dito hardware (ou a subscrição de serviços profissionais para estas tarefas).

Por fim, as *cloud* híbridas acabam por fazer a ponte entre os dois tipos de *cloud* que foram descritos anteriormente. Neste paradigma, uma organização, consoante a necessidade e estratégia definida, pode optar por posicionar recursos numa *cloud* pública, ou na sua *cloud* privada. Desta forma, é possível endereçar as diferentes necessidades de uma organização de uma forma flexível e recorrendo às vantagens de cada uma das soluções, incluindo aspetos de segurança de dados. O recente conceito de *multicloud* estende o conceito de *cloud* híbrida, agregando várias *clouds* (públicas ou privadas) para fornecerem um mesmo serviço de forma transparente.

A diferença de gestão de aspetos de informação e computação permite aos clientes escolherem relações distintas com diferentes serviços de computação-na-nuvem, com acesso a diferentes aspetos de gestão da infraestrutura. Esta elevada versatilidade da *cloud* possibilita o aparecimento de diferentes modelos de serviço, como (i) oferta de infra-estrutura (*IaaS – Infrastructure as a Service*); (ii) oferta de uma plataforma de execução de serviços (PaaS – *Platform as a Service*); e (iii) o fornecimento direto de um serviço de *software* (SaaS - *Software as a Service*) - embora haja muitos outros modelos mais especializados, tal como *DaaS* (*Desktop as a Service*), *CaaS* (*Container as a Service*) ou *DBaaS* (*Database as a Service*). A adoção de modelos de *cloud* pública, privada ou híbrida, e do tipo de serviços a usar, deverão sempre ter em conta o cálculo de *TCO* (*Total Cost Ownership*) das soluções externalizadas e dos custos de instalação, operação e manutenção de infraestruturas internas.

A figura 1 apresenta de forma gráfica as diferenças de gestão dos modelos principais de *cloud computing*, salientando as necessidades cada vez menores de recursos internos e sendo estas grande motivação para a adoção crescente destas soluções por grandes empresas e instituições públicas. A disponibilização de serviços nas redes internas das empresas sempre acarretou custos elevados com equipamento, energia e manutenção. Tais fatores contribuíram para que muitas pequenas e médias empresas se inibissem de avançar para a sua digitalização. No entanto, a evolução destas tecnologias de computação associadas à Internet acabou por criar ferramentas de trabalho económicas, já indispensáveis na vida das empresas e na vida dos indivíduos. Atualmente as tecnologias utilizadas permitem disponibilizar garantias de qualidade de serviço o que possibilita fornecer serviços que antes apenas podiam ser disponibilizados e acedidos a partir da rede Interna da empresa a custos bastante mais elevados.

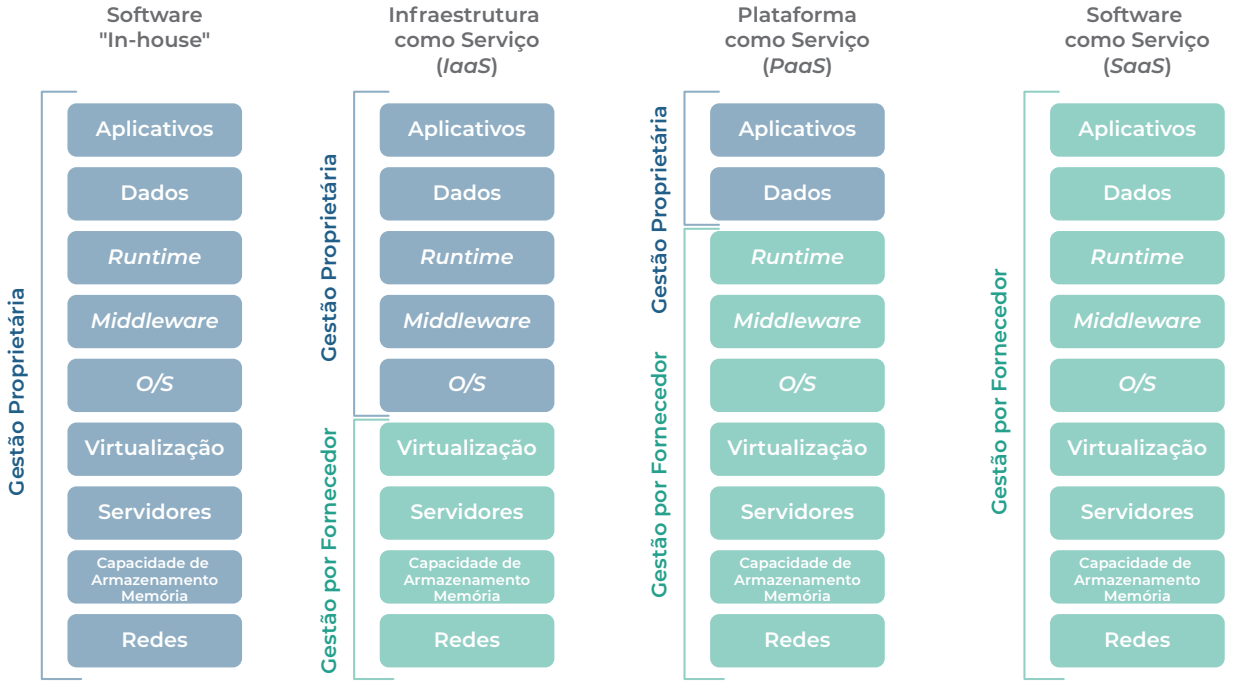


Figura 1 - Modelos de serviço principais de *Cloud computing*

BREVE RESENHA HISTÓRICA

A história da *cloud* começa a desenhar-se em 1963, quando a DARPA (Defense Advanced Research Projects Agency) financiou o projeto MAC (Mathematics and Computation) do MIT (Massachussets Institute of Technology) [2], cujo objetivo era permitir que um sistema computacional fosse usado simultaneamente por múltiplos utilizadores e a partir de localizações diferentes — uma abordagem ao conceito de *time-sharing*. Em 1969 deu-se início à antecessora da Internet, a ARPANET (Advanced Research Projects Agency Network), desenvolvida na ARPA com a liderança de JCR Licklider, que tinha como visão para o futuro a *Intergalactic Computer Network*, segundo a qual qualquer pessoa do planeta se poderia interligar e aceder a informação a partir de qualquer ponto [3]. Com o passar dos anos, estes modelos iniciais de utilização partilhada de recursos, e que recorriam ao conceito de *time-sharing* com acessos remotos, evoluíram para conceitos de partilha mais avançados, como a "virtualização ao nível dos sistemas", depois "ao nível da rede" e a exploração das diferentes tecnologias numa perspetiva de negócio que veio a resultar nos diferentes modelos de *cloud* existentes atualmente.

Genericamente, o conceito de "computação *cloud*" consiste na oferta de recursos a diversos clientes através de uma infraestrutura partilhada e disponibilizada através da Internet. Através de técnicas de virtualização, os recursos são apresentados de forma escalável, redundante e dinâmica em diferentes formatos, tal como mencionados acima, e referenciados como XaaS (*X-as-a-Service*, em que o X é o tipo de oferta fornecida na *cloud*), sendo o sucesso desta estratégia indissociável da facilidade de acesso remoto a estas infraestruturas.

É importante ainda referir que as características que moldaram o sucesso da Internet e dos sistemas interconectados, em particular a acessibilidade, a inovação livre, o acesso global e a adoção voluntária de normas, são também riscos adicionais de segurança, independentes dos riscos associados aos sistemas de *cloud*.

Os principais precursores de serviços *cloud* foram a *Salesforce* que, em 1999, passou a oferecer serviços de gestão de clientes através de um modelo SaaS (ver na Figura 1, em que as letras correspondem aos diferentes modelos de serviço esquematizados na figura) e a Amazon que iniciou a sua oferta *IaaS* (EC2, S3) em 2002 [4]. Hoje em dia todos os principais atores do mercado TI oferecem soluções *cloud* como é o caso da Google (com ofertas *PaaS* como o Google App Engine, ou *SaaS* como o Google Applications, uma suite de documentação e comunicação eletrónica), ou ainda o caso da Microsoft com o Windows Azure (*PaaS*), o Windows Live e Office 365 (*SaaS*), para além de um variado conjunto de ofertas de outros operadores de cobertura global (múltipla informação pode ser encontrada online, tal como em [5]).

Vivemos assim uma verdadeira revolução na adoção e uso de serviços *cloud*, com inúmeras vantagens para os modelos de negócio e de prestação de serviços das empresas e das instituições públicas. As características de escalabilidade, redundância, alta disponibilidade, elasticidade e reutilização inerentes aos modelos *cloud* permitem que as organizações se foquem no seu negócio, podendo deixar de gerir uma componente de TIC que, dependendo da escala, pode ter custos incomportáveis. Demonstrador do crescente interesse estratégico desta área e da sua crescente implementação, foi o aparecimento da "*European Cloud Initiative*" [6], que tem por objetivo promover o acesso seguro, sustentado e interoperável a infraestruturas e serviços *cloud* por parte de todos os operadores, com o objetivo de reforçar o mercado único digital na Europa [7], uma vez que este é um mercado dominado por empresas fora da Europa. Na Europa a adoção de *cloud* tem-se feito a ritmos diferentes e Portugal ocupa o 18º lugar na adoção de serviços *cloud* por parte das empresas [8].

FUTURO A 5 E 10 ANOS

Ao longo de toda a sua evolução, a segurança das infraestruturas, dos serviços e da informação tem sido sempre um fator de preocupação. Atualmente, o crescimento exponencial dos serviços em nuvem e sua adoção para o modelo de transformação digital em curso transformou este problema da segurança e resiliência num aspeto crítico para o funcionamento das organizações e da sociedade. **É assim importante não cair no erro de ofuscar a segurança com a funcionalidade, negligenciando o papel determinante que aquela tem na garantia do funcionamento íntegro de todo o ecossistema**, preferindo-se abordagens menos seguras em função de aspetos conjunturais associados a custos.

O recente cenário pandémico veio acentuar as vantagens da utilização da *cloud* e a necessidade de confiabilidade na mesma. Com a generalização do trabalho remoto, muitas organizações enfrentaram inúmeros problemas na disponibilização dos seus serviços internos para os trabalhadores acederem de "fora da rede da organização". Muitas organizações viram-se subitamente forçadas a exporem as suas redes e serviços internos, o que levou a adotarem o paradigma *cloud*, uma tendência que provavelmente não se reverterá. Contudo, esta mudança drástica na forma de acesso e consumo de serviços, **não foi devidamente acompanhada em muitas empresas pela necessária análise e revisão dos modelos de segurança relevantes neste novo contexto,** havendo recentemente esforços na Europa para corrigir esta situação[4]. Para além da tecnologia, também as componentes que implicam a governação da segurança nas organizações e a interação dos utilizadores precisam de ser revistas.

Segundo a Gartner, é expectável que o mercado de serviços *cloud* aumentem em 21.7%, com um mercado total de 482 mil milhões de USD até ao final de 2022. A Allied Market Research prevê que o mercado global de *cloud* seja de 1.6 trilliões USD em 2030 [9]. Para além disto, é também importante referir que é expectável que, em 2026, 45% das despesas das organizações de TI sejam relacionadas com serviços e infraestrutura *cloud* [10], algo que comprova o forte crescimento deste paradigma. Desta forma, é impreterível analisar quais as tendências futuras para o paradigma *cloud*, e qual será o seu impacto na sociedade à escala mundial, e na segurança da informação em particular. As áreas principais que se preveem ter impactos consideráveis (comparando com a utilização atual) prendem-se com a *IoT*, a AI, e, como veremos abaixo, os desenvolvimentos nos conceitos de *fog* ou *edge* e de armazenamento, que trarão desenvolvimentos no campo da governação. De uma forma mais extensa podemos apontar para:

- Um cenário que será fortemente alavancado pelos avanços tecnológicos da *cloud* é o de *IoT* (*Internet of Things*). O paradigma de *cloud* oferece uma plataforma de alta performance para armazenar e processar dados recolhidos pelos mais diversos sensores, o que simplifica bastante a gestão e processamento de toda esta informação, e permite resolver os grandes desafios de escalabilidade apresentados pela *IoT*. Com a simbiose entre *cloud* e *IoT* estima-se um enorme crescimento deste último paradigma, do qual veremos exemplos no próximo capítulo.

4 https://www.enisa.europa.eu/news/enisa-news/after-cloud-cybersecurity-certification-launching-the-enisa-ad-hoc-working-group-on-cloud-services

- Para além disso, a oferta de serviços diversificados de inteligência artificial, via *cloud*, é também um fator importante para a ampla adoção deste paradigma. Atualmente, a criação e utilização de ferramentas de inteligência artificial envolve elevados investimentos em poder de computação e em recursos humanos com elevadas capacidades técnicas, como veremos adiante. Contudo, a oferta de *Artificial Intelligence* as a Service (A*IaaS*), via *cloud*, terá um forte impacto no desenvolvimento destas ferramentas, sendo que o valor estimado para 2025 deste mercado é de 89 mil milhões de USD [11].

- Avanços na expansão das capacidades de armazenamento vão ter, também, um forte impacto no paradigma *cloud*. Atualmente, existe uma grande procura de armazenamento na *cloud*, que seja facilmente acessível por vários utilizadores e clientes de uma organização, incluindo aspetos de redundância geográfica, pelo que a adoção da *cloud* será significativamente acelerada com a inovação de mecanismos de armazenamento mais rápidos, mais fiáveis e, sobretudo, mais baratos.

De uma forma mais abrangente, é expectável que o paradigma de "*Fog Computing*" ganhe cada vez mais relevo no setor de TI. Este termo foi introduzido pela Cisco, que o descreve como a oferta de um modelo de *cloud-computing* que é disponibilizado na fronteira da rede, permitindo que os recursos estejam mais próximos dos utilizadores finais [13], e em última instância recorrendo a recursos dos utilizadores. Um exemplo típico será o fornecimento de serviços associados ao tráfego numa estrada, em que os utilizadores poderão aceder a serviços localizados de informação, potenciando novas experiências de utilização. Este modelo de *cloud* será capaz de fornecer uma melhor qualidade de serviço, com latências reduzidas e menor consumo energético. Para além disto, a utilização de um paradigma de *Fog/Edge Computing* será também responsável por uma redução do tráfego na Internet, uma vez que os utilizadores conseguem realizar todas as funções que pretendem através da computação na fronteira das redes, não sendo necessário recorrer a *datacenters* centrais para realizar tais funções [14].

Estas previsões de evoluções na *cloud* implicarão a adoção de modelos de governação nas organizações que assentem, essencialmente, numa estratégia de gestão de risco, que garanta que a adoção da tecnologia é eficaz e o receio da sua utilização não se sobrepõe à utilidade. **Estas mudanças terão um impacto profundo em aspetos de localização de informação (e cumprimentos de regras de privacidade), de confiabilidade na provisão de serviços, e de enquadramento regulatório das próprias entidades envolvidas nestes processos, para além de incrementar de forma significativa a superfície de exposição dos utilizadores a novos e potenciais perigos.**

A proposta legislativa Digital Services Act [16] da Comissão Europeia e a estratégia European Data Strategy [17] apresentam direções para o incentivo da adoção progressiva da *cloud* como meio de desenvolvimento económico da UE e fornecem um enquadramento para todas as organizações (fornecedores de serviço, consumidores de serviço e reguladores) desenvolverem as suas estratégias. Em Portugal, e no que respeita à Administração Pública (AP),

a Estratégia para a Transformação Digital da Administração Pública 2021-2026 [27] prevê um eixo dedicado especificamente à promoção da *cloud* como estratégia de desenvolvimento das TIC no setor[5]. No entanto, é de notar que estas iniciativas regulatórias correm sempre o risco de serem ultrapassadas pela rapidez das dinâmicas inerentes aos ecossistemas digitais.

PERIGOS EM CIBERSEGURANÇA

Nas vertentes atuais mais tradicionais, já hoje falhas na segurança dos sistemas e serviços *cloud* podem levar as organizações a exporem os seus dados, com potenciais consequências catastróficas, quer legais, quer de negócio. A centralização de serviços num ambiente de *cloud* faz com que o comprometimento da gestão dessa *cloud* coloque sérios riscos à disponibilidade desses serviços e continuidade do negócio. Similarmente, o comprometimento da gestão da *cloud* poderá levar a riscos substanciais de integridade dos serviços prestados, como *defacing* (e.g., *hacktivistas*), destruição de dados, ou fraudes (e.g., modificação de preços). Segundo a Gartner [10], em 2025, 90% das empresas que não controlem o seu ambiente de *cloud*, verão os seus dados expostos. Assim, esperam-se fortes avanços tecnológicos nos aspetos de segurança da *cloud*, tanto que a Gartner estima que, em 2026, 99% das falhas de segurança da *cloud* tenham como origem os próprios utilizadores da *cloud*, e não a infraestrutura onde assenta a mesma [11].

A implementação de soluções baseadas na *cloud* carece de uma revisão dos modelos de riscos, adaptando-os ao paradigma das arquiteturas *cloud*. Em particular, a perceção sobre a segurança na *cloud* é distorcida por uma deficiente identificação das responsabilidades dos operadores das infraestruturas *cloud* e das responsabilidades dos clientes que fazem a implementação dos serviços, especialmente dados os diferentes modelos de implementação de *cloud* que existem.

A Checkpoint no seu *Cloud Security Report* de 2022 [22] reforça o facto de a *cloud* representar uma oportunidade ímpar para o desenvolvimento económico e social da sociedade, mas também apresentar um conjunto significativo de riscos:

- A *Cloud* apresenta uma maior superfície de ataque para potenciais atacantes.
- Falta de visibilidade da infra-estrutura inerente, já que os *cloud* providers abstraem as plataformas inerentes escondendo os seus problemas (e potenciais implicações de segurança e regulatórias).
- As cargas de processamento na *cloud* são dinâmicas fruto da natureza elástica deste tipo de serviços controlados programaticamente, algo que os utilizadores frequentemente não compreendem e que pode ter consequências no desempenho dos serviços.
- A automação crescente destas plataformas introduz novos riscos ao nível da instalação dos serviços, uma vez que os programas que instalam serviços e aplicações para a *cloud* podem estar eles próprios comprometidos.

5 https://portugaldigital.gov.pt/promover-servicos-publicos-mais-digitais/mobilizar-e-transformar-a-administracao-publica/estrategia-cloud-para-a-administracao-publica

- A definição de papéis para os utilizadores *cloud* nas empresas é em grande medida muito liberal sendo frequente a atribuição de permissões a utilizadores que não necessitam de grandes privilégios, mas que por questões de falta de cultura em cibersegurança lhes são atribuídos como medida facilitadora.

- A complexidade dos ambientes *cloud*, hoje em dia compostos por milhares de serviços de pequenas dimensões (arquiteturas baseadas em micro-serviços), obriga a esforços extra pelas equipas de segurança que necessitam conhecer e monitorar portfólios muito alargados de serviços.

- Embora os prestadores de serviços *cloud* cumpram com as principais normas no que diz respeito à segurança e privacidade de dados (e.g. ISO 27001, NIST SP 800-53 [18], PCI-DSS 3.2 [19], HIPAA [20] e RGPD [21]) nem sempre os utilizadores destes serviços asseguram a sua eficaz aplicação.

A tendência crescente para a adoção de ambientes *multicloud* (e a sua potencial evolução para ambientes fog) introduz novas dimensões aos riscos de segurança já enumerados, tornando essenciais as soluções de automação e orquestração que permitam assegurar uma política consistente ao longo de toda a superfície exposta – mas que por sua vez introduzem outros riscos de segurança.

As empresas prestadoras de serviços, em particular na área do desenvolvimento aplicacional, tendem a recorrer de forma crescente aos ambientes *cloud* para disponibilizar serviços em modelos (por vezes mistos) de PaaS, CaaS ou SaaS. No entanto, a escassez de recursos humanos capacitados para o desenho de soluções e desenvolvimento em ambientes *cloud* vem colocar desafios adicionais de segurança aos sistemas.

Como desafio à utilização crescente da *cloud* está ainda a regulação, em especial no que respeita às condições para o tratamento de dados estabelecidas pelo RGPD, assim como, acima de tudo, a soberania dos dados e as consequências/restrições à implementação de arquiteturas globais. **A opacidade das implementações físicas de cloud, e a sua implementação redundante (por vezes entre continentes), são problemas para qualquer regulamentação associada a esta tecnologia.**

OPORTUNIDADES

Com base nas características apresentadas anteriormente, facilmente podem ser listadas algumas das oportunidades que advêm da adoção de tecnologias *cloud* por parte das empresas. De referir e reforçar que a adoção da *cloud* deve fazer parte da Arquitetura Empresarial (EA), como parte integrante da estratégia de desenvolvimento de negócio da Organização. A *cloud* representa uma oportunidade para a transformação organizacional, através da oferta de um vasto conjunto de serviços que permitirão automatizar serviços, reduzir o tempo de desenvolvimento e reduzir o *time-to-market* das soluções. A transformação digital, a inteligência artificial, a flexibilidade exigida pelos negócios trará grande oportunidade de desenvolvimento aos serviços de *cloud* nos seus diversos formatos.

Uma das oportunidades mais relevantes é o dinamismo que este paradigma permite, sobretudo no espectro das PMEs. Uma PME ou uma start-up, adotando um paradigma *cloud*, pode facilmente desenvolver toda a sua infraestrutura sem investimentos elevados, utilizando serviços como *IaaS* ou PaaS. Desta forma, estas organizações podem adquirir infraestrutura de alta performance e altamente resiliente num curto espaço de tempo [23]. Paralelamente, delegar a gestão da infraestrutura em parceiros externos extremamente experientes na gestão de infraestruturas *cloud* (AWS, Google, Microsoft, entre outros) reduz bastante a complexidade que implica ser a própria empresa a assegurar por si a segurança dos seus sistemas. Mecanismos de DRaaS (*Disaster Recovery-as-a-Service*) disponibilizados por estes parceiros externos permitem uma rápida recuperação de falhas e de dados, o que, na atualidade, se revela um aspeto fulcral [7].

Através de mecanismos SD-WAN (*Software-Defined Wide-Area Networks*), providenciados por operadores que ofereçam serviços *cloud*, os funcionários e clientes de uma organização podem ter acesso a todas as aplicações disponibilizadas pela mesma, sem necessitar de usar redes seguras privadas (VPNs) para se conectarem à rede da organização. Este modelo, apesar de ainda muitas vezes ignorado, providencia uma conectividade mais simples e eficiente, facilitando também a configuração e gestão das redes de uma organização. Estima-se que, em 2024, 60% das empresas implementem mecanismos de SD-WAN, sendo que, em 2020, apenas 30% das organizações recorriam a estas soluções [24].

Por fim, há que mencionar a possibilidade de criação de ambientes de desenvolvimento e testes contínuos, o que pode acelerar bastante o processo de desenvolvimento de novos serviços e sistemas. O paradigma de *Continuous Integration*, suportado pelas tecnologias *cloud*, permitirá, desta forma, um *time-to-market* mais reduzido, oferecendo claras vantagens competitivas para as organizações que o adotarem.

Ao nível do emprego, deve ser destacada a necessidade de novas competências e de novos postos de trabalho qualificados, que vão desde a gestão operacional, até à gestão de negócio, passando pela arquitetura, pela gestão de risco e, em particular, pela segurança [26]. É também um fator relevante a criação de postos de trabalho de alto valor e de competências mais vastas e transversais.

POTENCIAIS INDICADORES DA ÁREA

Identificam-se um conjunto de indicadores que podem permitir um quadro situacional da adoção da *cloud* em Portugal e do nível de segurança associado aos serviços prestados.

Tabela 2 – Métricas potenciais para avaliação societal de segurança no uso de computação na nuvem

Métrica	Significado	Mecanismo de obtenção
Número de empresas que declaram ter os seus serviços na cloud	Identificação do nível de adoção de serviços cloud por parte das empresas portuguesas	Inquérito alargado às empresas e consulta a bases de dados adequadas*
Número de empresas que declaram ter uma estratégia para a cloud definida	Identificação da percentagem de empresas com estratégia de TI que envolve a utilização de cloud	
Número de empresas que declaram ter uma estratégia de segurança definida	Identificação da percentagem de empresas que já definiram uma estratégia interna de cibersegurança ou de segurança da informação	
Percentagem de infraestrutura alojada dentro do território nacional	Quantificação da percentagem de infraestrutura de TI das empresas alojada na jurisdição do ciberespaço nacional e grau de dependência da organização de legislações ou jurisdições desfavoráveis ao cumprimento de determinados parâmetros de segurança e privacidade dos dados	
Percentagem de infraestrutura própria dentro de um operador de cloud nacional	Identificação da dimensão relativa da infraestrutura em regime de housing	
Número de CVE's associados a cloud providers (AWS, Cloud Engine, Azure, Digital Ocean)	Identificação do nível de exposição e ameaça dos serviços de cloud pública.	Consulta ao www.cve.org
Proporção de serviços/processos dependentes de serviços cloud	Identificação do grau de dependência da cloud para a atividade e operação das empresas	Inquérito alargado às empresas
Proporção de RH TI com competências cloud do total de recursos TI	Identificação da adequação das competências internas relativamente ao grau de dependência da cloud	
Proporção de Entidades que dispõem de serviço de resposta a incidentes	Identificação da capacidade de resposta das empresas a incidentes de segurança	
Número médio de ameaças de cibersegurança por organização	Identificação do número médio de ameaças anuais por organização	
Proporção de adoção de cloud por setor de atividade definido na NIS	Identificação do grau de adoção da cloud para as entidades abrangidas pela NIS	Inquérito alargado às empresas com atividade abrangida pela NIS
Proporção de TI assente dependente da cloud por setor de atividade definido na NIS	Identificação do grau de dependência da cloud para as entidades abrangidas pela NIS	
Número médio de ameaças de cibersegurança por setor de atividade definido na NIS	Identificação do número médio de ameaças anuais por organização do âmbito da NIS	Inquérito alargado às empresas e informação CERT
Número de operadores de serviços de cloud proprietários em território nacional (IaaS, PaaS, SaaS, CaaS)	Quantificação dos operadores de serviços de cloud proprietária em Portugal, permitindo a identificação da tipologia de serviços prestados.	Inquérito aos operadores de serviços de cloud
Volume de negócios da cloud por tipo de fornecedor	Identificação do volume de negócios por tipo de fornecedor (infraestrutura própria ou revenda)	
Número de operadores nacionais que revendem serviços cloud	Quantificação dos operadores que revendem serviços de cloud em Portugal.	

* Entre as bases de dados a considerar, estarão os dados do Instituto Nacional de Estatística, da Direção-Geral de Estatísticas da Educação e Ciência, e da Associação Portuguesa para a Promoção da Segurança da Informação. É recomendável que estas métricas venham a ser coligidas adequadamente num documento, tal como, p.ex., o Relatório Anual de Cibersegurança de Portugal.

REALIDADE NACIONAL E RECOMENDAÇÕES

Segundo a IDC, [28] os principais fornecedores de serviços *cloud* no mercado português são a Microsoft, a AWS, a Salesforce e a GCS, representando o setor um valor total 300 M€ em 2020. Ainda de acordo com o Eurostat, em 2021, 35% das empresas portuguesas usam algum serviço *Cloud* [29], abaixo da média europeia. Em termos de serviços destaca-se a utilização do email (89%), do armazenamento de ficheiros (71%), das aplicações de segurança (66%) e das aplicações de produtividade/office (61%). Os números fornecidos pela IDC [30] são algo diferentes, identificando 2/3 das organizações portuguesas como já utilizadoras de serviços de *cloud* pública ou privada, com 1/3 dessas já numa fase de maturidade Gerida ou Otimizada (i.e. a tecnologia está em utilização disseminada na empresa). Independentemente dos números, todos os relatórios coincidem na tendência de crescimento da *cloud* e da sua importância para as organizações. A oferta no mercado português é, em termos de serviços de *cloud*, baseada nos atores internacionais e em alguns dos operadores de telecomunicações que estão a passar a disponibilizar também no seu portfólio de serviços, em particular, *IaaS*, BaaS (Backup as a Service) e CaaS (*Container as a Service*).

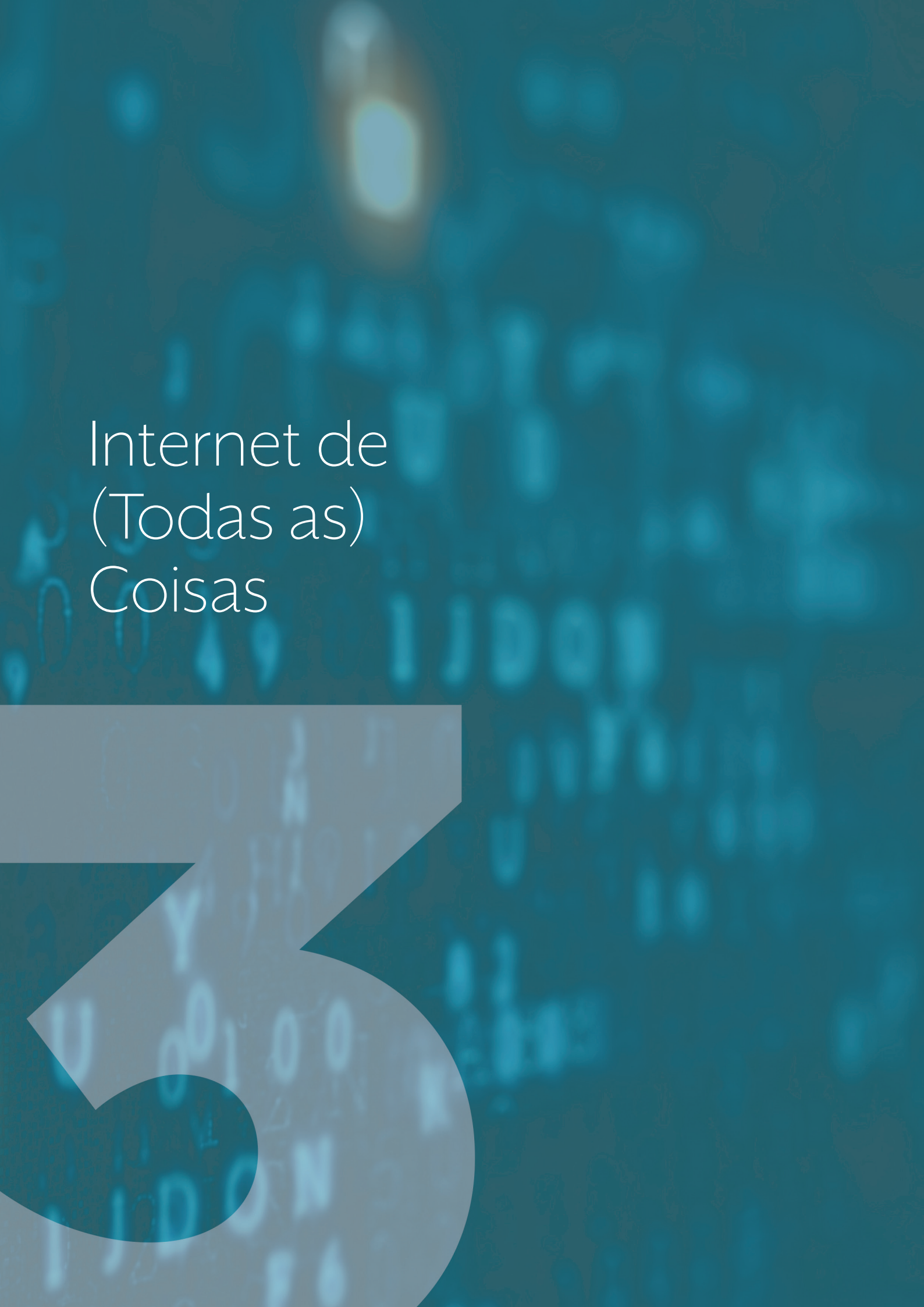
É de salientar ainda a crescente oferta [25] de "serviços de *cloud*" por muitas empresas nacionais da área de desenvolvimento de soluções, quer através da reutilização das *clouds* dos grandes atores internacionais, quer, em particular, através da disponibilização de serviços próprios nos seus *Datacenters*. A maioria desta oferta é realizada através de pequenos operadores, que desempenham o papel de revendedores, geralmente sem capacidade técnica de intervenção nas infraestruturas e com muita dependência das empresas internacionais.

Analisando o setor público, Portugal tem também, desde novembro 2020, uma Estratégia *Cloud* para a Administração Pública, que assenta nos princípios da segurança e soberania da informação e dos dados, da adoção de uma *framework* comum de serviços, na integração *multicloud*, na monitorização do consumo e da qualidade e na independência de fornecedor (*no lockin*) [31], i.e. garantir que os serviços da AP não ficarão dependentes de um único fornecedor de serviços. Paralelamente, a legislação presente no Decreto Lei 65/2021 [217] obriga fornecedores destes serviços e administração pública a identificar serviços críticos, possuir processos específicos para a gestão de risco, procedimentos de segurança e inventário, o que irá aumentar a visibilidade sobre estas infraestruturas e da sua exposição.

Portugal está assim bem integrado nas tendências internacionais, com um conjunto de pequenos operadores secundários, que fornecem apoio técnico mais localizado, mas frequentemente sem o conhecimento detalhado dos grandes fornecedores mundiais de serviços *cloud*.

As recomendações principais do ponto de vista nacional poderão assim sumariar-se como a **implementação eficaz e atempada das recomendações e regulamentações internacionais** (ver secção de Legislação Adicional), **com as adaptações necessárias para este ecossistema**, bem como a monitorização do cumprimento destas recomendações. Dado o carácter internacional de muitos dos modelos de utilização de *cloud*, e dada a abrangência das recomendações internacionais em termos de cibersegurança, não se antevê necessidade de grandes modificações em termos de especificidades para recomendações nacionais.

Internet de (Todas as) Coisas



A Internet das Coisas (*Internet of Things* ou *IoT*) surge como uma evolução da Internet e um novo paradigma tecnológico, social, cultural e digital. Vem revolucionar a forma como a sociedade interage com o ambiente, e ao mesmo tempo levar a uma alteração substancial dos modelos de negócios. A ENISA - Agência da União Europeia para a Cibersegurança define a *IoT* como um "ecossistema ciber-físico de sensores e atuadores em rede que habilitam a tomada de decisão de forma inteligente". A *IoT* pode também ser definida como uma "rede global e infraestrutura de serviços de conectividade e densidade variáveis com capacidade de autoconfiguração e baseada em normas e protocolos interoperáveis que integram dispositivos heterogéneos caracterizados por identidades, atributos físicos e virtuais integrados de forma transparente e segura na Internet" [32].

Em termos muito simples, é uma rede em que tudo se pode conectar à Internet, como por exemplo lâmpadas, sensores de temperatura, ou qualquer dispositivo *IoT* em geral, dispositivos de computação que se conectam a uma rede sem fios e que são capazes de transmitir dados. Desta forma, os dispositivos *IoT* não se limitam a uma conectividade com a Internet baseada em dispositivos comuns como *Smartphones* ou Desktops [33]. O conceito de *IoT* é amplo, essencialmente proporcionando aos objetos do dia-a-dia uma capacidade computacional e de comunicação, podendo desta forma haver dados transmitidos e processados remotamente. Assim, os objetos poderão ser considerados dispositivos inteligentes e podem ser monitorizados ou controlados à distância.

A massificação da tecnologia *IoT* traduz-se num valor de mercado cada vez maior. De acordo com o Statista [34], o número de dispositivos *IoT* a nível global deverá quase triplicar de 8.78 mil milhões em 2020 para 25.4 mil milhões em 2030. A mesma fonte projeta que 60% de todos os dispositivos *IoT* conectados serão encontrados no segmento do mercado de consumo, primariamente em *smartphones* para Internet de consumo e multimédia. A McKinsey & Company [35] estima que em 2030 o valor global capturado pela Internet das Coisas atinja um valor entre 5.5 e 12.6 biliões de euros. Este potencial de valor será concentrado em cenários específicos, nomeadamente de fabricação, controlo e gestão que acumularão 26% de todas as receitas em 2030. Neste âmbito, a tecnologia *IoT* é usada para otimizar operações e potenciar a gestão do dia-a-dia de ativos e de pessoas de forma eficiente. Atualmente, os principais verticais na indústria distribuem-se por aplicações em eletricidade, gás, A/C, abastecimento de água e gestão de resíduos, retalho e logística. Um outro cenário de aplicação é a saúde que representará entre 10% a 14% do valor económico da Internet das Coisas em 2030, representando tecnologias implantadas (p.ex, monitores conectados de glucose) ou que afetam o corpo humano (p.ex., desfibrilhadores conectados). Para 2030 o Statista projeta vários casos de uso com mais de 1000 milhões de dispositivos *IoT* nas áreas da mobilidade inteligente e conectada, infraestruturas de tecnologias de informação, rastreabilidade e monitorização de objetos de valor, e redes inteligentes de distribuição de energia. O cenário onde a maior fatia do valor será criada é em aplicações *Business-to-Business* (B2B), projetadas a acumular até 2030 entre 62% a 65% de todo o valor potencial gerado pela Internet das Coisas.

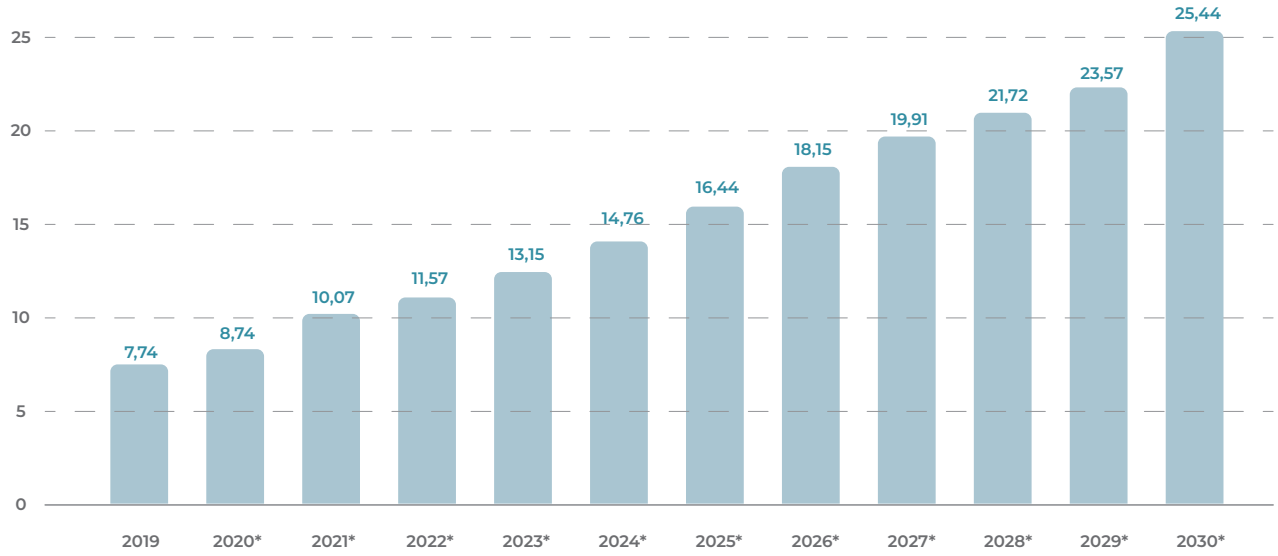


Figura 2 - Número de dispositivos conectados globalmente de 2019 a 2030 [34]

A adoção massiva de dispositivos *IoT*, combinada com uma elevada diversidade de características e heterogeneidade de requisitos, considerando a enorme variabilidade de contextos de utilização, desafia os paradigmas de computação tradicional [36]. Em função do caso de uso e do contrato de nível de serviço (*Service Level Agreement* - SLA), os dispositivos podem precisar de processamento e armazenamento de dados localmente, na *cloud*, ou em algum elemento intermédio. A heterogeneidade das "Coisas" em termos dos requisitos computacionais (processamento, memória, armazenamento), de conectividade (protocolos de comunicação e standards) e desenvolvimento de *software* (natureza distribuída, requisitos de paralelização e de dinâmica) habilita a implementação de aplicações e casos de uso até recentemente difíceis de atingir. Contudo, o aumento de complexidade tem impacto no cumprimento dos requisitos dos contratos de nível de serviço. Por exemplo, a mobilidade de utilizadores e dispositivos, confiabilidade, disponibilidade e escalabilidade tornam-se difíceis de garantir [37], embora a adoção de protocolos normalizados e de interfaces abertas potencie uma maior escalabilidade às soluções *IoT*, simultaneamente facilitando o desenvolvimento de produtos e serviços de modo mais expedito e com melhor escalabilidade. No entanto, a grande heterogeneidade tecnológica impõe limitações de eficácia na sua integração, tal como ocorre noutras abordagens verticais onde existe uma oferta diversificada de sistemas operativos, *middleware* e de soluções empresariais [38].

BREVE RESENHA HISTÓRICA

Os dispositivos de *IoT* podem simplificar o dia-a-dia dos cidadãos, pois apresentam interfaces de programação e configuração muito apelativas e de fácil utilização. Isto permite ao cidadão comum (e a empresas não especializadas) instalar e explorar benefícios, frequentemente com custos muito reduzidos, que estes dispositivos oferecem, sem ser necessário treino técnico específico.

Contudo, o conceito da *IoT* tem uma longa história: surgiu ainda no início dos anos 80 na Universidade de Carnegie Melon, quando um grupo de estudantes criou uma forma de fazer com que a máquina de venda de Coca-Cola reportasse o seu stock através de uma rede de comunicações. A ideia surgiu da necessidade de evitar o inconveniente aos estudantes de fazer o caminho até à máquina apenas para a encontrar sem Coca-Colas frescas. Para isso, os alunos instalaram uma placa eletrónica na máquina de venda que detetava a existência de latas para consumo e os eventos de reabastecimento, reportando esta informação através da rede ARPANET- a precursora da Internet dos dias de hoje e que na altura servia menos de 300 computadores a nível global. Com esta informação os estudantes conseguiam saber o número exato de Coca-Colas frescas disponíveis sem ter de se deslocar à máquina. Posteriormente, em 1990, John Romkey ligou o primeiro dispositivo *IoT* à Internet que hoje conhecemos. Este dispositivo era uma torradeira que poderia ser ligada e desligada remotamente. Na conferência onde apresentou o seu projeto, John Romkey conectou a torradeira a um computador com rede TCP / IP, o que para a época foi um evento revolucionário. Embora neste teste o pão tenha sido introduzido manualmente na torradeira, em pouco tempo esse requisito foi corrigido passando a ter um robot controlado pela Internet, que colocava o pão na torradeira de forma automatizada.

A investigação nesta área continuou, e em 1991, Weiser escreveu um artigo onde abordava o futuro da *IoT* afirmando que os dispositivos iriam estar conectados em todos os lugares de forma tão transparente para o ser humano ao ponto que se iriam tornar imperceptíveis possibilitando, de forma natural, a realização das atividades, sem haver preocupação em instalar, configurar e manter os recursos computacionais. Em 1996, Venkatesh mencionou também o aparecimento de casas especializadas que iriam permitir a automatização de tarefas domésticas. Essas casas são agora denominadas por casas inteligentes (*Smart Homes*).

Em 1999, surge pela primeira vez o nome *Internet of Things* (*IoT*). Kevin Ashton, numa palestra para a Procter & Gamble, considerou que uma forma de chamar a atenção dos executivos seria intitular a sua apresentação como *Internet of Things*, o conceito que iria conectar os objetos do mundo físico com a Internet. Desde então, a investigação nesta área ganhou uma nova dimensão e a partir de 2005 a discussão sobre *IoT* generalizou-se e começaram a surgir os primeiros problemas com a utilização deste tipo de dispositivos na sociedade, essencialmente com aspetos de segurança e privacidade. Ainda em 2005, foi lançado o primeiro objeto comercializado em larga escala, o Nabaztag, que podia ser programado para receber previsão do tempo e ler e-mails, entre outros.

Os anos de 2008/2009 são considerados o período de nascimento de *IoT* por neles se ter passado a haver mais objetos — entre *smartphones* e *tablets* — conectados do que população mundial. Também neste período começaram a surgir plataformas *IoT* com o objetivo de facilitar a comunicação entre dispositivos heterogéneos, gerir o fluxo de dados e de dispositivos, salvaguardar informação e suportar novas funcionalidades para aplicações *IoT*. Foi a partir de 2011 que se discutiu a criação de padrões internacionais para a criação de objetos [39][40], tendo o pico de novas plataformas *IoT* ocorrido em 2013 com o surgimento de 52 *startups*. Nessa altura, paralelamente aos esforços de padronização internacional, começam a criar-se padrões *de facto* (i.e., soluções que pela sua popularidade se tornam referência; p.ex., o universo Eclipse *IoT* para auto-hospedagem e criação de serviços *IoT* em escala, Home Assistant para auto-hospedagem e uso individual de serviços a escala residencial, e AWS *IoT*, Azure *IoT*, Google *Cloud IoT* para serviços de subscrição do tipo PaaS). Estas plataformas de *IoT* são uma solução de software, quer na *cloud*, quer *on-premises* (i.e. dentro das instalações privadas da empresa), que monitoriza e/ou controla diferentes tipos de dispositivos (sensores/atuadores), permitindo a sua integração com processos empresariais. Algumas das plataformas são de uso geral, enquanto outras são especializadas em áreas de negócio bem definidas (e.g. [41][42]), oferecendo ferramentas altamente especializadas para determinados modelos de negócio. Estas plataformas oferecem um número crescente de mecanismos de análise de negócio (muitas vezes baseados em Inteligência Artificial), cada vez mais integrados com o ambiente ciberfísico associado a esse modelo de negócio. A Figura 3 apresenta o modelo de operação típico associado a estas plataformas, que permitem até uma implementação funcional fisicamente distribuída, permitindo a diferentes modelos de negócio as melhores escolhas em termos de implementação. De notar a prevalência de armazenamento e processamento de muita informação, o que traz problemas específicos de segurança e privacidade de informação, similares aos problemas dos serviços de *cloud*.

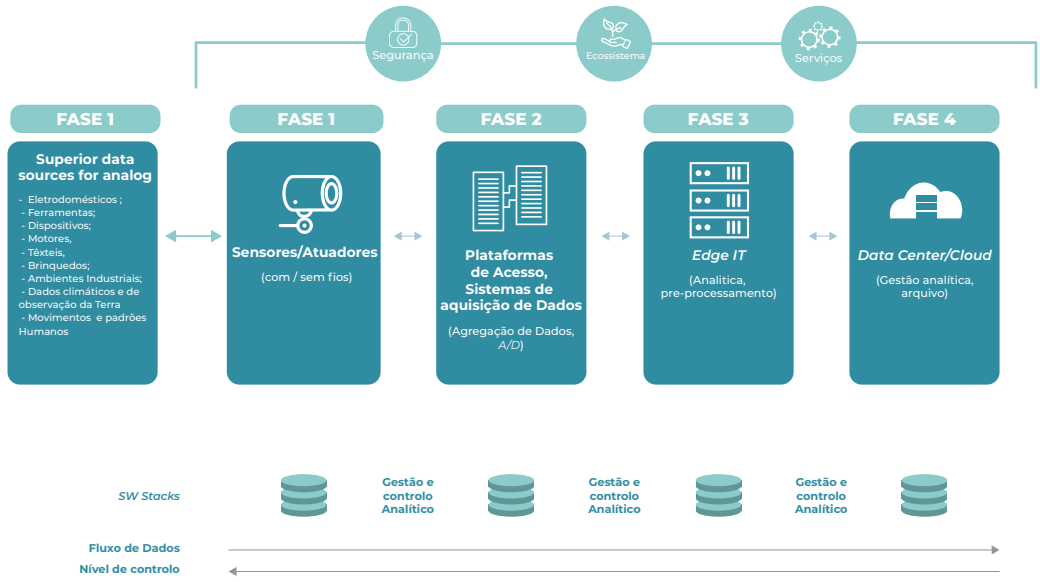


Figura 3 – Modelo de operação para sistemas *IoT*

Atualmente, e **graças a estas plataformas** [43], a *IoT* é um conceito generalizado que faz parte do dia-a-dia de muitos cidadãos e que está presente nas suas casas, veículos, serviços públicos e em muitos outros serviços comerciais. É cada vez mais uma área de forte interesse de desenvolvimento técnico, sendo objeto de estudo em domínios tão distintos como a eletrónica, telecomunicações, sistemas operativos, segurança, direitos e ética, entre outros.

O futuro da tecnologia *IoT* promete um forte crescimento do número de dispositivos ligados tendo como catalisador a adoção maciça da tecnologia 5G. É expectável um aumento significativo de volume de negócios em produtos e serviços daí resultante, progressivamente contribuindo para transformar a tecnologia *IoT* num dos principais motores da economia global.

FUTURO A 5 E 10 ANOS

A constante integração de dispositivos *IoT* nas tarefas diárias dos utilizadores tem vindo a crescer nos últimos tempos e prevê-se que este crescimento se acentue. A *IoT* tem uma visão multidisciplinar para beneficiar vários domínios, como o ambiental, industrial, público/privado, saúde, transportes, entre outros. Vários têm sido os projetos de investigação e industriais focados em potenciar o crescimento desta tecnologia de forma a tirar proveito da mesma. Dentro destas áreas, podemos mencionar, a título de exemplo:

- **Cidades inteligentes** – A pressão populacional e a diversidade de requisitos a atender impõem uma grande exigência aos serviços oferecidos nas cidades inteligentes, amplificando a necessidade de fornecer soluções inteligentes em várias áreas, incluindo a mobilidade (estacionamento, tráfego, transportes públicos), iluminação, saúde, qualidade do ar, segurança pública e gestão de resíduos, entre outras. Neste contexto, tem havido uma integração crescente de sensores *IoT* que permitem a monitorização remota de parâmetros usados posteriormente para o suporte à decisão, e de atuadores com funcionalidades de controlo, capazes de comandar à distância diversos tipos de equipamento.

- **Casas inteligentes** – Uma casa inteligente consiste numa habitação com eletrodomésticos, sistemas de ar condicionado/aquecimento, televisão, dispositivos de transmissão de áudio/vídeo e sistemas de segurança, que comunicam (usando tecnologias *IoT*) de forma a proporcionar um melhor conforto, aumentando a qualidade de vida. Os dispositivos *IoT* ajudam na poupança energética e numa melhor gestão de recursos, contribuindo para uma diminuição de custos de uma forma geral.

- **Veículos/Mobilidade inteligente** - Atualmente a esmagadora maioria dos veículos está equipada com dispositivos e sensores inteligentes que controlam a maioria dos componentes, desde a suspensão do carro até ao motor [43]. Os veículos mais recentes com capacidade de condução semi-autónoma (e futuramente potencialmente autónoma) incorporam mecanismos de comunicação e controlo complexos, permitindo a partilha de informação sensorial que pode ser usada para articular manobras cooperativas tais como condução em pelotão, *lane merging* (junção de faixas na autoestrada, como p.ex. a entrada na autoestrada), entre outras.

- **eHealth** - Em termos de saúde, a *IoT* tem sido a base para revolucionar os serviços convencionais de saúde, por exemplo, estendendo o alcance da telemedicina aos instrumentos de cirurgia. Existe um compromisso das organizações nacionais de saúde para aumentar o suporte para cuidados personalizados e integrados de forma a prevenir e gerir doenças mais graves, como doenças crónicas, existindo um número cada vez maior de aplicações relacionadas com a saúde. A título de exemplo, a monitorização médica foi introduzida nas últimas décadas graças aos avanços nos dispositivos móveis e *IoT* [66].

Num futuro próximo, é expectável que a *IoT* continue a fazer parte do dia-a-dia dos cidadãos e que cresça no sentido de abranger quase todas as áreas de aplicação. A progressiva redução de custos que se espera no 5G irá promover uma maior integração desta tecnologia em dispositivos embutidos, algo que terá um impacto decisivo na sua uniformização como tecnologia de conectividade de facto em contexto *IoT*. No entanto, a tecnologia *IoT* apresenta ainda muitos desafios que precisam de ser tidos em conta para apoiar a sua expansão e ampla aceitação. As cidades inteligentes serão cada vez mais comuns, os prestadores de cuidados de saúde serão cada vez mais automatizados com base em dispositivos *IoT*, os veículos autónomos tornar-se-ão frequentes: de uma forma geral, a *IoT* irá abranger todas as áreas de aplicação. Abordaremos algumas destas áreas numa seção posterior, salientando consequências dos perigos destas técnicas na sociedade atual.

Mas, para além dos avanços na *IoT* que hoje conhecemos e exploramos, é plausível que os ecossistemas *IoT* evoluam de modo a ter um impacto ainda mais profundo na qualidade de vida humana. Existem três grandes áreas de aplicação emergentes que se perspetivam para o futuro: no espaço (*Internet of Space Things*), no oceano (*Internet of Underwater Things*), e à escala nano/micro (*Internet of Nano Things*) [67]. As tecnologias empregues nestas aplicações possuem requisitos técnicos e operacionais muito distintos da *IoT* convencional, e terão impactos muito distintos em termos de segurança, que irão precisar de análises diferenciadas no futuro.

Internet of Space Things (IoST)

A IoST aborda o estabelecimento de uma cobertura global de Internet de alta velocidade e reduzida latência através de redes de satélites na baixa órbita terrestre (*Low Earth Orbit* - LEO) [68]. Motivada pelo aumento maciço de dispositivos *IoT* e pela falta de elevadas taxas de transmissão e de largura de banda em muitas zonas do globo, a IoST potenciará a redução de congestionamento das redes existentes estabelecendo redes alternativas de *backhaul* capazes de assegurar cobertura contínua com elevada qualidade de serviço tanto em áreas de elevada densidade populacional como em áreas remotas onde os custos de infraestrutura são proibitivos.

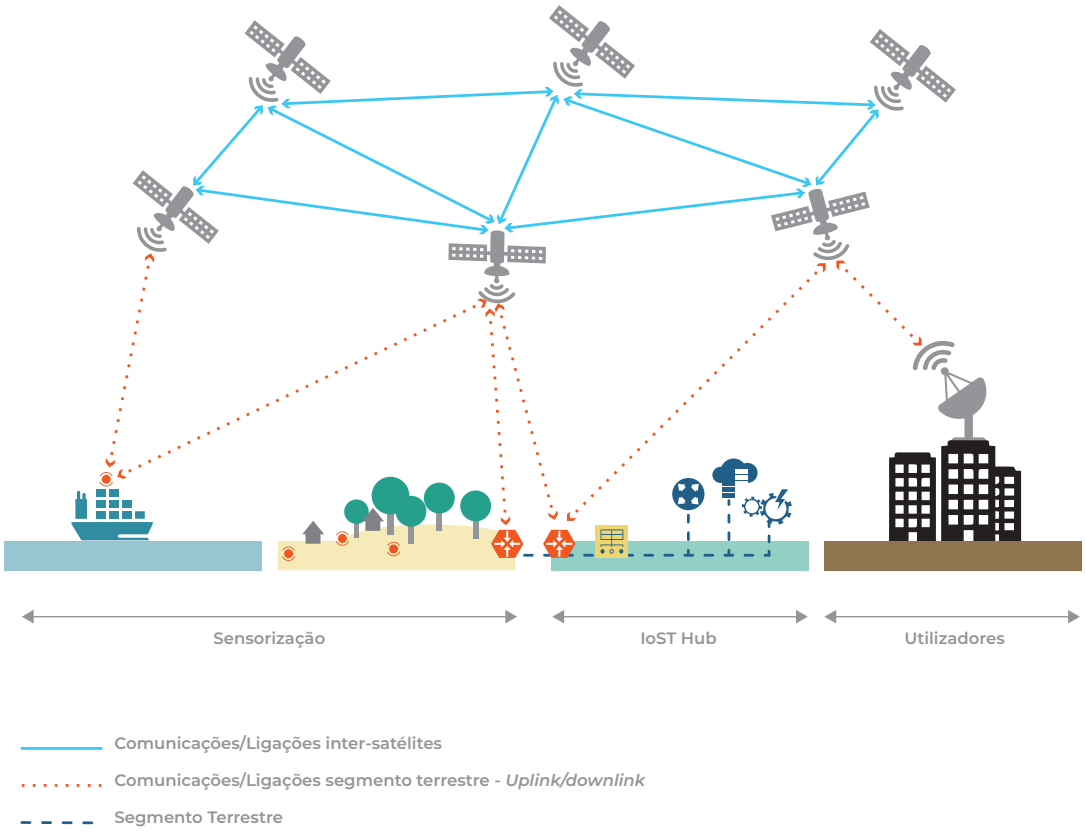


Figura 4 - *Internet of Space Things* [67]

Embora empresas como a Google, Facebook, SpaceX e OneWeb tenham já realizado investimentos significativos para disponibilizar acesso à Internet em zonas remotas, a expectativa é que na próxima década ocorra um alargamento da IoST através de satélites de reduzida escala de serviço em LEOs para suportar tráfego *IoT* a nível global. Por exemplo, o projeto Starlink prevê lançar mais de 30 mil satélites TinTin que formarão constelações utilizando feixes laser para comunicar entre si de modo a disponibilizar cobertura de Internet de alta-velocidade nos locais mais remotos do planeta.

O futuro das redes IoST poderá contemplar também órbitas distintas para suportar diferentes classes de tráfego (*IoT* ou genérico) e/ou de cobertura geográfica, potenciando níveis de serviço e aplicações com elevada heterogeneidade [69]. Atendendo à dimensão da sua área marítima nacional, **a IoST deverá ser uma tecnologia estratégica para Portuga**l. A monitorização de grandes áreas

geográficas usando meios convencionais é globalmente onerosa, apresentando uma complexidade elevada tanto na coordenação de meios técnicos como de meios humanos. A IoST oferece uma alternativa de monitorização com custos moderados de implantação e exploração e com um nível de automatização muito elevado.

Internet of Underwater Things (IoUT)

A IoUT preconiza o estabelecimento de uma rede de comunicações subaquática que contribua para melhorar a qualidade dos oceanos, acelerar operações de busca e salvamento, e que habilite sistemas fiáveis de gestão de desastres para salvar vidas humanas. O principal objetivo é a criação de um sistema interconectado de dispositivos, sensores, e veículos autónomos subaquáticos que disponibilize e reencaminhe informação através da Internet. Esta rede visa a identificação e resposta a desastres naturais (derrames de petróleo, tsunamis e naufrágios), a monitorização da qualidade do leito oceânico (estudo da barreira de coral), e o estudo da saúde das espécies que habitam o oceano profundo. A existência de redes de comunicação subaquática poderá ainda ser potenciada para aplicações de patrulhamento geográfico (geofencing), facilitando a monitorização e governo de águas internacionais. Pelas mesmas razões expressas no caso anterior, **a IoUT deverá vir a ser uma tecnologia estratégica para Portugal**.

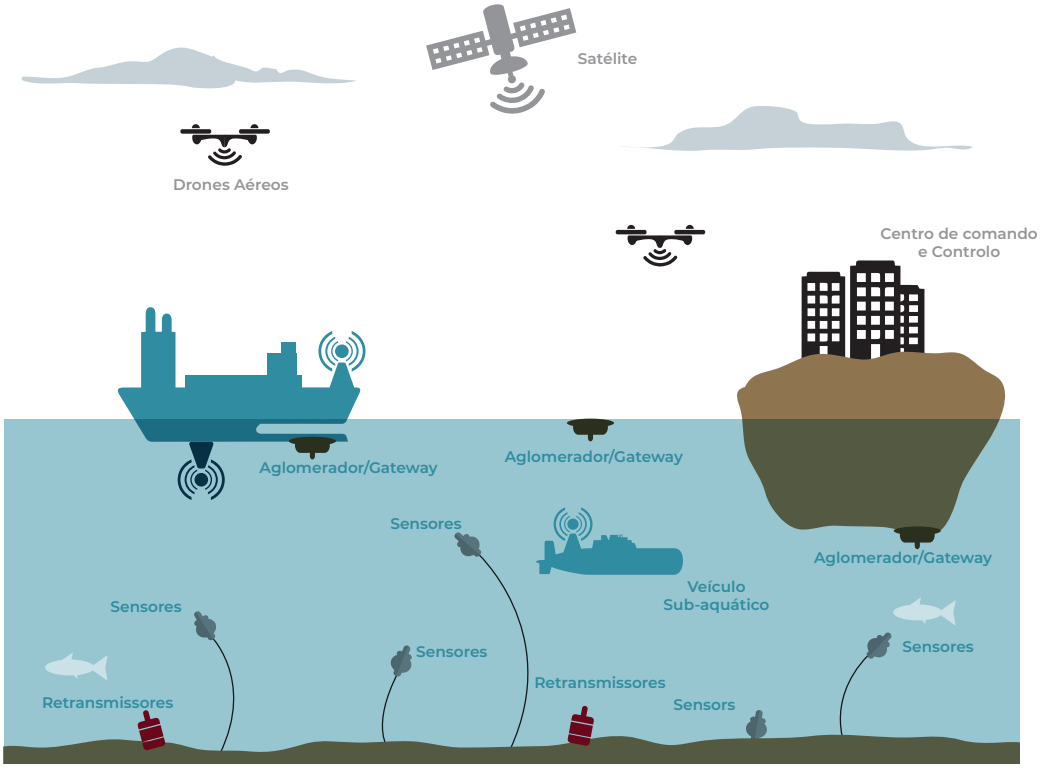


Figura 5 - *Internet of Underwater Things*

As tecnologias a adotar no meio subaquático são muito distintas das que se utilizam para a *IoT* convencional ou mesmo para a IoST. Apesar de ser possível usar comunicações rádio neste meio, tal apenas é possível para distâncias, frequências e larguras de banda significativamente reduzidas face à atenuação e atraso de propagação neste meio. A alternativa mais promissora reside no uso de comunicações óticas, mas os custos de instalação, complexidade e consumo de potência são grandes entraves à sua adoção [70].

Internet of Nano Things (*IoNT*)

A IoNT corresponde à introdução de nanotecnologia no conceito de *IoT*, caracterizando-se na sua forma mais simples como uma rede *IoT* a uma escala mais reduzida onde nanosensores e dispositivos de dimensão ultra reduzida assumem funções de sensorização e/ou atuação em aplicações conectadas de monitorização ambiental e médica, entre outras. Neste contexto, a conectividade é assegurada por comunicações moleculares (baseadas em fluxo ou em difusão) ou não-moleculares (eletromagnéticas ou óticas) [71], algo que diferencia substancialmente as aplicações da IoNT relativamente à *IoT* tradicional.

De modo a assegurar uma autonomia compatível com a sua dimensão física, os sensores da IoNT caracterizam-se por consumos energéticos extremamente reduzidos e comunicações de muito curta distância (Wireless Body Area Networks - WBANs) usando Gateways como "ponte" para o mundo exterior.

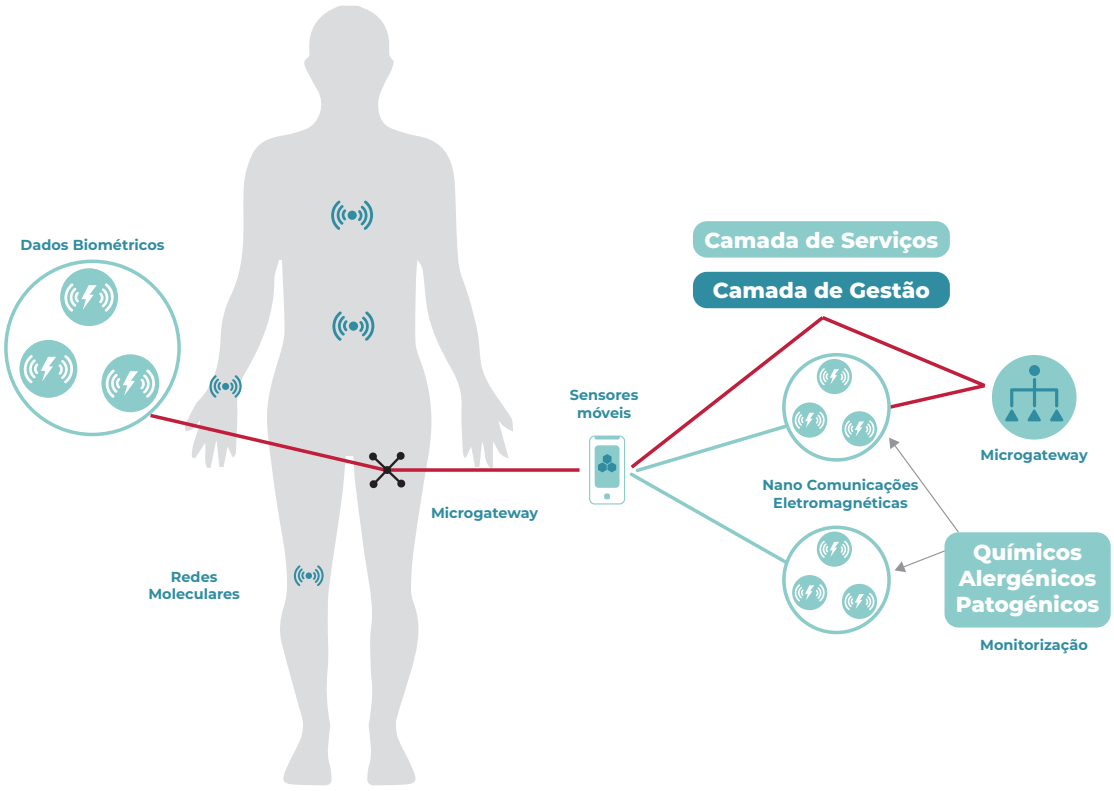


Figura 6 - *Internet of Nano Things* [37]

Apesar da abundância de soluções técnicas e avanços tecnológicos, estes ecossistemas *IoT* carecem de uma reformulação tecnológica desde a base face às condições operacionais muito distintas que exigem novas soluções para a pilha tecnológica da *IoT*, com especial atenção aos aspetos de segurança, privacidade e políticas de governança que exigem não só avanços tecnológicos, mas, sobretudo, uma arquitetura unificada e escalável que possa endereçar os requisitos de aplicações tão heterogéneas. A sua utilização massificada ainda demorará alguns anos, mas essencialmente consistirá num extremar dos casos de uso de aplicações de eHealth que já existem.

DESAFIOS DE CIBERSEGURANÇA

Vários têm sido os ataques de cibersegurança reportados na *IoT*. Essencialmente, a *IoT* está interligada aos desenvolvimentos de comunicações móveis (de que o 5G é o último exemplo), da tecnologia de *cloud computing*, onde são hospedadas muitas das plataformas de *IoT*, e de novos mecanismos de processamento de informação (de que a Inteligência Artificial é um dos exemplos recentes mais populares). **Nesse sentido, a IoT é particularmente sensível aos perigos de cibersegurança associados a cada uma destas áreas.**

O uso de plataformas de *IoT* apresenta um conjunto de perigos específicos em termos de cibersegurança. Em primeiro lugar, encontrando-se estas plataformas ligadas aos processos de negócio das empresas, os **problemas de cibersegurança têm um mapeamento direto na operação e sustentabilidade das empresas**. Em segundo lugar, estas plataformas são frequentemente hospedadas fora das empresas, e coligem dados de diferentes ambientes de negócio, criando pontos de vazamento de informação que são frequentemente invisíveis para os utilizadores das plataformas. Finalmente, estas plataformas, mesmo quando localizadas *on-premises*, apresentam diferentes falhas de segurança (especialmente quando são desenvolvidas *in-house* recorrendo a soluções abertas), que podem ser facilmente exploradas por atacantes.

No entanto, é tradicional discutir-se os perigos de segurança da *IoT* mais centrados no impacto das diferentes áreas de aplicação, e não tanto nas tecnologias associadas. Esta seção irá assim abordar os perigos de cibersegurança em quatro áreas críticas com impacto direto no quotidiano dos utilizadores e no funcionamento da economia nacional: energia, indústria, transportes/mobilidade e eletrónica de consumo. As principais motivações para a seleção destas áreas são:

- O sector da distribuição de energia é instrumental para o desenvolvimento do país e representa o maior risco para o funcionamento global da economia face ao impacto que ataques de segurança causam na sua dependência.
- A indústria cria valor económico e postos de trabalho representando também um sector crítico.
- A mobilidade é fundamental para o desenvolvimento económico e social do país, potenciando novas formas de criação de valor, aumentos de eficiência e impacto no bem-estar dos cidadãos sendo, por isso, um sector estratégico.
- Por fim, a heterogeneidade de dispositivos de eletrónica de consumo origina uma panóplia de aplicações e serviços que captam valor para os seus utilizadores e facilitam as suas tarefas do dia-a-dia, proporcionando maior conforto e sensação de bem-estar.

Adicionalmente, alguns sectores tal como a saúde, estão expostos a um risco particularmente elevado e , em que algumas vulnerabilidades da IoT podem ter consequências fatais. Um outro tipo de criticallidade, mas que também afeta o cidadão, prende-se com ataques a funções empresariais criticas, e à exfiltração de dados confidenciais dos clientes (e empresas). O relatório de ameaças de *IoT* pela Unit 42 em 2020 [45] indicava que 98% do tráfego de dispositivos *IoT* não é transmitido de forma segura, possivelmente expondo dados pessoais e confidenciais na rede. O mesmo relatório conclui que 51% das ameaças no domínio da saúde envolvem dispositivos de imagem com impacto na qualidade dos cuidados de saúde, permitindo a exfiltração dos dados dos doentes. Uma das vulnerabilidades na origem destes ataques em cuidados de saúde é a existência de VLANs que integram simultaneamente tanto os dispositivos da *IoT* como os de TI, habilitando a propagação de *malware* na rede dos computadores dos utilizadores para dispositivos vulneráveis.

Energia

Os operadores de rede elétrica têm vindo a integrar a tecnologia *IoT* como forma de mitigar a volatilidade de consumo na transmissão e distribuição de potência. Contudo, a crescente penetração da tecnologia de comunicação na rede elétrica aumenta a base de ataque para atores maliciosos, criando oportunidade para ataques com consequências potencialmente devastadoras [72]. A rede de controlo de processos ("*Process Control Network*" - PCN) liga o centro de controlo das empresas de distribuição diretamente aos dispositivos de campo, tipicamente através dos protocolos DNP3 (utilizado nos EUA e parte da Ásia) ou IEC 60870-5-104 (resto do mundo). Os comandos do centro de controlo são diretamente recebidos por controladores lógicos programáveis que atuam sobre os comutadores das subestações. A interligação de dados entre a rede local do operador e a PCN deve ocorrer sempre através de um servidor dedicado que opere como intermediário de segurança, assegurando a autorização das ações pedidas pelo centro de comando e a inexistência de *malware* nos ficheiros enviados. Contudo, devido à existência de outros mecanismos de comunicação direta com a PCN como, por exemplo, VPNs ou linhas dedicadas de manutenção remota (para diagnóstico e *update* de *firmware*), estas ficam diretamente expostas a ciberataques tal como o que ocorreu na rede de distribuição Ucraniana [73]. Em 2015, três empresas de distribuição de energia na Ucrânia foram alvo de um ciberataque que afetou 225.000 utilizadores, causando disrupção do serviço de fornecimento por um período superior a 3 horas. O ataque foi perpetrado sobre uma rede local e posteriormente estendido à rede de controlo de processo operada por várias empresas de distribuição, comprometendo o funcionamento dos sistemas de Supervisory Control And Data Acquisition (SCADA) através do acesso remoto a comutadores em várias subestações de média tensão.

A dificuldade de realizar alterações físicas a redes de controlo de processo no sector da distribuição de energia, cujo planeamento de longevidade é medido em décadas (e não em anos), constitui um sério impedimento à rápida atualização de mecanismos e protocolos de segurança, colocando um forte entrave ao acompanhamento da evolução da técnica na área da segurança industrial. Adicionalmente, face a terem sido desenvolvidos há mais de 20 anos,

os protocolos DNP3 e IEC 60870-5-104 não suportam os mecanismos básicos de autenticação e proteção de integridade, sendo vulneráveis contra vários tipos de ataques ("man-in-the-middle" - interceção de dados por uma entidade intermédia, negação de serviço, "replay" - repetição/reprodução de dados, e "spoofing" - imitação de identidade) [72]. Quando as PCNs não estão suficientemente isoladas das redes genéricas ligadas à Internet, atacantes podem mover-se entre as duas (uma técnica conhecida como *pivoting*), permitindo o uso de ferramentas (simples!) para comunicar, usando os protocolos DNP3 e IEC 60870-5-104 para controlar remotamente dispositivos e comprometer o funcionamento da rede de distribuição, tal como ocorreu na Ucrânia [73].

Além disso, estruturalmente, há novos cenários de energia que aumentam os riscos de segurança da rede elétrica. O interesse público em fontes de energia renovável tem vindo a aumentar devido à diminuição do custo de investimento, pressão para redução das emissões de CO_2 e de custos energéticos. O aumento de recursos distribuídos de energia (*Distributed Energy Resources - DERs*), necessariamente interligados pela *IoT* a uma grelha elétrica global, representa uma ameaça aos sistemas tradicionais de distribuição de energia nos quais os operadores da rede procuram manter um fornecimento de potência ininterrupto. Apesar dos mecanismos de ajuste à natureza intermitente da produção de energia baseadas em fontes renováveis, a inexistência de mecanismos para prever e dimensionar reservas que possam dar resposta a disrupções artificiais pode colocar em causa o funcionamento da rede em situações de alta penetração de *DERs*, problemas que podem ser artificialmente replicados por problemas de integridade da *IoT*. A natureza distribuída das *DERs* e a elevada heterogeneidade sobre quem as controla (propriedade) aumenta os perigos de cibersegurança, de forma que não ocorria nos sistemas tradicionais SCADA, a segurança alcançava-se sobretudo pelo isolamento físico das redes, abrindo caminho a ataques coordenados com elevado potencial de disrupção do fornecimento de eletricidade [75]. Em contrapartida, nos tradicionais sistemas SCADA, à medida que os DER se tornarem mais prevalentes e interconectados com dispositivos de consumo, vendedores, agregadores e tecnologias *smart grid*, aumentará a exposição a vetores de ataque deste tipo.

Indústria

A utilização de *IoT* em aplicações industriais tem vindo a ser descrito como o novo paradigma da Indústria 4.0, integrando um leque diverso de tecnologias disruptivas com potencial para alterar profundamente a forma como os sistemas cooperaram, aumentando o leque de possíveis aplicações. Com a Internet Industrial das Coisas (*Industrial Internet of Things - IIoT*) a ganhar tração no terreno, as comunicações autónomas entre múltiplos dispositivos industriais distribuídos por uma fábrica e ligados à Internet são cada vez mais uma realidade. A ligação de ativos industriais (por exemplo, máquinas e sistemas de controlo) com sistemas de informação e processos empresariais potencia a análise de dados conducente a operações industriais ótimas [76].

Um dos aspetos essenciais promovidos pelo paradigma da Indústria 4.0 é a mudança de sistemas de comunicação centrados em serviços de nuvem/Internet para arquiteturas em que os processos industriais trocam informações

diretamente de uma forma ponto-a-ponto, promovendo assim a descentralização de aplicações e a distribuição da carga computacional pelas entidades participantes [77]. Contudo, dado que a I*IoT* integra tecnologias operacionais (Operational Technologies - OTs) caracterizadas por longos ciclos de vida e elevado potencial de obsolescência, está mais exposta a riscos de cibersegurança que outros cenários *IoT* comuns onde predominam dispositivos de consumo, tipicamente com menor tempo de vida (por exemplo, em aplicações de retalho e qualidade de vida).

A segurança e a privacidade são determinantes em aplicações I*IoT* e Indústria 4.0 [78]. O estabelecimento de confiança entre "parceiros, prestadores de serviços, fabricantes, fornecedores, e governos" é um requisito central para permitir transações de confiança [77]. No entanto, tal confiança só pode ser alcançada se as tecnologias utilizadas incluírem mecanismos de apoio à transparência e responsabilidade, preservando ao mesmo tempo a privacidade (que tem de ser reinterpretada em função do caso de uso concreto de I*IoT*).

A necessidade de I*IoT* suportar um número maciço de dispositivos *IoT* heterogéneos (estáticos e móveis) coloca um desafio às tradicionais soluções de segurança centralizadas, especialmente quando estas tecnologias devem ser implantadas em ambientes inconfiáveis ou precisam de interagir com dispositivos *IoT* configurados em tais ambientes. Nestes cenários, para além de operações regulares como manutenção e substituição, os dispositivos I*IoT* também podem ser obrigados a estabelecer interações pouco frequentes e oportunistas uns com os outros. Além de constituírem um ponto único de falha, confiar numa autoridade central para autenticar e autorizar estas operações acrescenta despesas de comunicação e aumenta as hipóteses de ataques maliciosos. Em particular, com dispositivos com idades diferentes, com grandes dificuldades de atualização de *firmware*, quaisquer processos de autenticação podem revelar-se poucos seguros com o passar dos anos.

Transportes/Mobilidade

A crescente heterogeneidade de veículos autónomos conjugada com a integração entre fornecedores de serviço que empregam tecnologias automatizadas acarretam elevados desafios de segurança e confiança de modo a permitir a interoperabilidade e a partilha de dados em cenários de aplicação de múltiplos fornecedores/operadores. De acordo com o relatório da McKinsey de 2020 [79], o risco de hackers interferirem com a direção ou travagem "fomentará o medo de carros autónomos e porá toda a tecnologia em risco". De facto, com uma superfície de ataque cada vez maior, o risco enfrentado pelas tecnologias de condução autónoma aumenta, tornando a procura de soluções um esforço holístico envolvendo múltiplas "partes ao longo da cadeia de valor, para todo o ciclo de vida digital dos veículos modernos". De notar que estas tecnologias encontram-se já num estado embrionário nas viaturas atuais, com diagnósticos remotos e sistemas controlados por computador. Lidar com um ecossistema de transportes tão diversificado representa um desafio de segurança significativo para todas as partes interessadas.

Um estudo recente [80] concluiu que "a fraqueza do fator humano" é um elemento-chave que conduz ao ciberterrorismo, sugerindo assim a necessidade de uma maior automatização. No entanto, tal opção acarreta uma exposição adicional e a necessidade de mecanismos de cibersegurança mais ágeis e mais fortes. Dado que vários ataques passados resultaram da exploração de comunicações veiculares, a evolução para a integração e interface com veículos autónomos que operam em áreas geográficas críticas deve adotar tecnologias que protejam plenamente as suas comunicações. Em geral, para permitir a autenticação segura de veículos, é adotada alguma forma de infraestrutura de Chave Pública de Veículos (centralizada) (VPKI - *Vehicle Public Key Infrastructure*). No entanto, em cenários de aplicações heterogéneas que abrangem diferentes tipos de veículos possivelmente pertencentes a múltiplos operadores, o número de Autoridades de Confiança (AA) e as interações necessárias para completar um processo de autenticação pode facilmente tornar-se um problema. Além disso, se uma dessas AA for comprometida, todo o ecossistema pode ser impedido de funcionar corretamente devido à natureza centralizada do sistema.

Nos últimos anos surgiram várias soluções descentralizadas de autenticação e autorização, por exemplo, baseadas em tecnologias de registo distribuído (*Distributed Ledger Technologies* - DLTs). Em geral, estas soluções visam "garantir a segurança das comunicações veiculares através do intercâmbio de dados criptográficos" [81]. No entanto, dado que neste caso a fonte de confiança é o *ledger* (registo remoto), a segurança proporcionada pelas DLTs implica vários compromissos, nomeadamente o aumento da latência, custos gerais de comunicação, e redução da eficiência energética.

A situação em desenvolvimento nas aplicações *IoT* aplicadas a sistemas veiculares vai requerer um acompanhamento cuidado das diferentes componentes de cibersegurança que se irão desenvolver nos próximos anos.

Electrónica de Consumo

A crescente penetração da eletrónica de consumo conectada à Internet tem sido potenciada por um vasto conjunto de casos de uso no mercado de consumo, por exemplo, localização de bens; rastreamento de pessoas vulneráveis; *wearables* (anéis, pulseiras, relógios inteligentes); medição e monitorização (energia, água, jardim), alarmes e segurança e casas digitais (automatização da temperatura, iluminação, rega). Este crescimento deve-se não só ao aumento de aplicações na área da eletrónica de consumo, mas sobretudo à disponibilidade crescente de tecnologias de ligação que potenciam a emergência destas aplicações. Em 2020, a Ericsson previu a existência de 1,5 mil milhões de dispositivos *IoT* com ligações celulares até 2022, contra cerca de 400 milhões de *IoT* no final de 2016 [46]. No mesmo estudo, a Ericsson prevê que até 2026 se atinja cerca de 6000 milhões de dispositivos *IoT* ligados à Internet. O crescimento mais rápido do que o esperado está a ser impulsionado pela utilização da conectividade celular convencional em vez de NB-*IoT* e LTE-M. No mercado de consumo, as redes celulares convencionais estão a ser utilizadas para ligar dispositivos *IoT* de consumo, tais como veículos, artigos de uso pessoal, localizadores de bens e câmaras de segurança, entre muitos outros.

A massificação de dispositivos heterogéneos ligados à Internet usando diferentes tecnologias implica um reforço da segurança dos componentes da *IoT*, dado que quando o produto é implantado comercialmente torna-se difícil operar atualizações, especialmente ao nível do hardware. Por isso, é imperativo que os mecanismos de segurança sejam implementados na fase de conceção, onde os custos associados são reduzidos comparativamente com cenários onde os dispositivos são comprometidos em funcionamento, com limitações de serviço para os seus utilizadores. No entanto, muitos dispositivos *IoT* continuam a ser fabricados sem componentes de segurança essenciais tais como a incorporação de uma forma segura de gerar chaves no dispositivo ou um mecanismo que assegure a exclusividade dos identificadores usados. Num cenário onde algumas organizações nem sequer são capazes de identificar todos os seus dispositivos *IoT*, manter um registo de configurações e atualizações de todos os dispositivos é uma tarefa árdua mas absolutamente essencial para assegurar a segurança dos dispositivos ao longo do seu ciclo de vida, uma vez que a rede é apenas tão segura quanto o seu elo mais fraco.

A conceção de produtos *IoT* é frequentemente baseada numa combinação de código fonte *open-source* e proprietário, empregando um processo de desenvolvimento que permite integrar o código e construir aplicações funcionais. O World Wide Web Consortium (W3C) relata que 91% dos programadores de *IoT* utilizam *software* de código aberto, open hardware ou dados abertos em pelo menos uma parte do desenvolvimento [47]. Face à elevada probabilidade de existirem vulnerabilidades em repositórios de código fonte aberto, é necessário adotar mecanismos eficazes de rastrear falhas e atualizar em tempo útil e de modo remoto os dispositivos *IoT* que incorporem peças de *software* aberto que possuam vulnerabilidades. De acordo com o relatório OSSRA da Synopsis [48], 64% das bases de código *IoT* aberto possuem vulnerabilidades, algo que pode comprometer severamente o seu funcionamento. O aumento do trabalho remoto veio também revelar fragilidades na segurança da *IoT*, particularmente em dispositivos de consumo instalados em casa. Um dispositivo de consumo que um funcionário liga ao seu *router* ou *smartphone* aumenta a potencial superfície de ataque à sua empresa. Isso ocorre porque frequentemente estes dispositivos (p. ex., lâmpadas inteligentes) são menos seguros que equipamentos industriais ou mesmo computadores convencionais, *smartphones*, etc., devido a constrangimentos de custo num mercado extremamente competitivo. Por exemplo, a COMCAST identifica [49] que a partir do momento em que as empresas optaram por manter os seus funcionários em casa no início da pandemia do SARS-CoV-2 deu-se um aumento de 12% no número de ciberataques a dispositivos *IoT* domésticos, tentando tirar partido de uma maior atividade online de casas conectadas.

A *IoT* é maioritariamente protegida utilizando soluções baseadas em arquiteturas centralizadas, cliente-servidor, frequentemente assentes em plataformas *cloud* que facilitam o desenvolvimento de soluções recorrendo a diferentes serviços de computação na nuvem. Além da gestão de dispositivos e do armazenamento de dados em massa, as plataformas *IoT* tipicamente disponibilizam serviços de análise e partilha de informação que habilitam a implantação de soluções *IoT* em larga-escala com tempos de colocação no mercado reduzidos. Contudo, o caráter centralizado destas soluções aumenta não só o risco de ameaças mas, sobretudo, o impacto de potenciais ataques face ao elevado

volume de informação que pode ser exposto, resultando em perda de dados, violação da sua integridade e/ou acesso não autorizado. Na perspetiva *IoT* tal é crítico, visto que os clientes estão inteiramente dependentes dos fornecedores de serviço para garantir que os seus dados estão seguros. Em maio de 2022, uma equipa de investigadores da Mandiant[50] descreveu a forma como através de metadados é possível obter as credenciais de aplicações AWS vulneráveis e aceder aos seus dados.

OPORTUNIDADES

A crescente penetração da *IoT* em múltiplos domínios da economia acarreta riscos de segurança que devem ser geridos preventivamente, procurando identificar antecipadamente ameaças e responder a ataques de forma pronta e eficaz. Num cenário de adoção massificada de dispositivos *IoT* com o potencial de transformar radicalmente negócios e mercados, é importante considerar as oportunidades de melhorar a segurança dos ecossistemas apostando numa evolução dos métodos e processos de desenvolvimento e em tecnologias emergentes que reforcem a segurança dos produtos e serviços oferecidos na *IoT*.

Métodos e Processos

A recente recomendação para rotulagem de produtos de consumo *IoT* ao nível da cibersegurança [51] lançada pelo NIST representa uma oportunidade para estabelecer um ecossistema de entidades acreditadas para conferir rótulos de segurança a produtos *IoT* e estabelecer metodologias de teste que avaliem o seu cumprimento. A recomendação tem como principais objetivos:

- Tornar as disposições de cibersegurança transparentes para consumidores, habilitando-os a diferenciar de forma simples dispositivos com segurança deficiente e sem conhecimentos prévios de cibersegurança;
- Ajudar os fabricantes a diferenciar-se no mercado, promovendo um incentivo para que produzam dispositivos mais seguros;
- Estimular o crescimento da economia, o trabalho com parceiros internacionais para reconhecimento mútuo, e reduzir a duplicação de procedimentos de teste, melhorando o acesso ao mercado.

A rotulagem permitirá aos consumidores evitar produtos *IoT* com baixo nível de segurança e empresas incapazes de demonstrar a sua conformidade. Contudo, há um caminho de sensibilização a percorrer que só será bem-sucedido se for construído sobre um ecossistema de entidades acreditadas e de processos de rotulagem globalmente reconhecidos. O custo do processo e o acesso próximo a entidades e que confiram o rótulo serão também fatores decisivos no sucesso desta iniciativa.

A adoção de práticas de referência no desenvolvimento de produtos de hardware e *software* na *IoT* é outra oportunidade que potenciará o surgimento de dispositivos mais seguros e de serviços em que os utilizadores podem confiar. A Agência da União Europeia para a Cibersegurança (ENISA) tem vindo a publicar várias recomendações que promovem a aplicação de um conjunto mínimo de requisitos

de cibersegurança em diversas áreas *IoT*. Em termos de infraestruturas críticas de informação, a ENISA publicou um grupo de recomendações base [52] visando instalações, redes, serviços e equipamento tecnológico cuja destruição ou perturbação poderia ter consequências importantes para a saúde, a segurança e/ou o bem-estar económico dos cidadãos, bem como para o funcionamento eficiente das instituições do Estado e das Administrações Pública. A ENISA publicou também um guia para reforçar a segurança em cadeias de abastecimento [53] tendo como objetivos a análise das diferentes fases do processo e os desafios enfrentados em cada uma, identificando ameaças, medidas de segurança e diretrizes para dar suporte aos diferentes intervenientes de como fortalecer a sua segurança. A ENISA disponibiliza um guia interativo de boas práticas para *IoT* e infraestruturas inteligentes [54] que permite a engenheiros e programadores identificar as ameaças, medidas de segurança e melhores práticas para o desenvolvimento de soluções *IoT* em diferentes áreas, desde os veículos e cidades inteligentes até à Indústria 4.0. As empresas têm por isso a oportunidade de usar esta ferramenta de referência como um elemento central no seu processo de criação de produtos e do seu melhoramento ao longo do ciclo de vida.

Além dos modelos de desenvolvimento focados na garantia de segurança dos serviços e produtos *IoT* é necessário considerar que estes podem ter ciclos de vida longos sem intervenção técnica especializada. Neste sentido, é importante não só criar consciência junto dos proprietários dos dispositivos *IoT* que operam no seu ambiente e que, sistematicamente, partilham informação na Internet mas, sobretudo, adotar mecanismos de identificação e monitorização do seu comportamento, recorrendo, por exemplo, a algoritmos de inteligência artificial para detetar anomalias de funcionamento. Adicionalmente, o acompanhamento e a atualização dos dispositivos face a vulnerabilidades identificadas deve ser acautelada, assegurando mecanismos de atualização seguros e fáceis de realizar, preferencialmente de modo não intrusivo para o seu utilizador.

A criação de programas de imersão em cibersegurança (desenvolvimento, operação, auditorias, por exemplo) para engenheiros e programadores juntamente com a promoção de comunidades profissionais de cibersegurança pode ser também o motor de uma maior consciencialização para o tema entre profissionais, transportando para as empresas e produtos *IoT* as melhores práticas no setor.

Tecnologias

A evolução das tecnologias na área da *IoT* potencia um conjunto alargado de oportunidades de melhorar a segurança de produtos e serviços, tornando-os mais robustos e confiáveis. A elevada disseminação e adoção de tecnologias de rádio definido por *software* (SDN) que tem ocorrido nos últimos anos pode beneficiar largamente soluções de rede com maior capacidade de sobreviver ao "teste do tempo" em redes de controlo de processo, caracterizadas por ciclos de vida muito longos. Esta flexibilidade permitirá uma evolução das redes que acompanhe a evolução dos *standards* de cibersegurança para incorporar mecanismos de segurança melhorados, evitando as soluções que hoje ocorrem com hardware obsoleto (mas ainda em uso) nas áreas da Energia e Indústria.

A identidade digital como parte de um quadro de segurança há muito que é apoiada por sistemas de informação centralizados, frequentemente de

terceiros, que representam um ponto único de falha e que pode prejudicar globalmente infraestruturas, interrompendo o seu funcionamento regular. Além disso, as abordagens centralizadas acarretam preocupações de privacidade com a possibilidade de exposição da identidade digital se a autoridade central for comprometida. O paradigma de *Self-Sovereign Identity* (SSI - identidade soberana) consiste num "sistema de gestão de identidade que permite aos indivíduos possuir e gerir plenamente a sua identidade digital". Neste sentido, a fonte de confiança (identidade) é delegada aos utilizadores e entidades que os possuem, permitindo armazenar em segurança os seus artefactos de identidade em carteiras digitais. Estes artefactos são designados como Identificadores Descentralizados (DIDs) [55] e podem incluir credenciais verificáveis [56] a partir das quais se podem gerar representações verificáveis para demonstrar a prova de atributos diretamente a um requerente sem ter de passar por um intermediário que avalie a sua validade. O paradigma SSI defende a normalização dos dados permitindo a interoperabilidade entre as diferentes intervenções, preservando segurança, controlabilidade e portabilidade, mesmo em circunstâncias em que a interação dos utilizadores ou equipamentos é esporádica. No contexto da *IoT* pode vir a tornar-se uma tecnologia chave para habilitar casos de uso que careçam de autenticação espontânea e segura de dispositivos e/ou utilizadores sem recurso a um sistema de chaves centralizado.

O paradigma SSI é construído com base em tecnologias de registo distribuído que, além de suportar novas abordagens de identidade digital, potencia aplicações heterogéneas, face à sua capacidade de suportar a transferência de valor através de criptoactivos e de assegurar um registo inviolável e público de transações, facilitando a sua verificação externa, algo que promove uma maior transparência e confiança. Neste âmbito as DLTs têm vindo a ser usadas em inúmeras aplicações tais como, por exemplo, *Smart Farming* [57], gestão da cadeia de abastecimento [58] e comunicações industriais [59], estabelecendo mecanismos de confiança entre diferentes atores, algo que constitui uma oportunidade para outras áreas de aplicação no contexto *IoT*.

Face à sua capacidade de suportar pagamentos digitais em moeda criptográfica *feeless* [60] ou *near-feeless* [61], as DLTs potenciam também o estabelecimento de interações monetárias automáticas máquina-máquina recorrendo, por exemplo, a contratos inteligentes (*smart contracts*) que são executados quando um determinado evento *trigger* é verificado, algo que promove uma agilização e uma maior eficiência das interações entre dispositivos *IoT* a um custo relativamente reduzido e que poderá vir a massificar-se num futuro próximo.

O desenvolvimento de ecossistemas de dados em silos que tem ocorrido, particularmente em contexto *IoT*, deverá dar lugar a uma maior colaboração entre domínios através da adoção de padrões emergentes de identidade digital e de partilha de dados que melhor defenda a interoperabilidade e a soberania dos dados disponibilizados. O uso de DLTs, combinado com o novo paradigma SSI, constitui uma oportunidade para criar novos ecossistemas de partilha de informação que sejam mais flexíveis, interoperáveis e que assegurem um elevado nível de rastreabilidade de utilização, algo que poderá vir a ser determinante na valorização da informação gerada na *IoT*.

O crescimento e popularidade das arquiteturas *Chip-to-Cloud* decorre da sua capacidade de habilitarem a criação de redes seguras de dispositivos de baixo

consumo energético que tem conectividade direta com plataformas de nuvem *IoT*. Neste âmbito, os dispositivos *IoT* criam túneis de comunicação segura a partir de um *chip* para um serviço na *cloud*, tornando-o opaco para o resto do sistema operativo, incluindo o processador do sistema e a memória principal. Esta abordagem permite oferecer proteção contra ataques de memória, ataques de canal lateral e erros de lógica empresarial. A tecnologia Chip-to-*Cloud* oferece uma forma de contrabalançar a falta de poder computacional e de medidas de segurança nativas nos dispositivos *IoT*, impossibilitando o roubo/falsificação de identidade e o desvio do acesso à rede empresarial mais ampla.

POTENCIAIS INDICADORES DA ÁREA

O desenvolvimento de soluções de hardware e *software* em contexto da *IoT* tem vindo a crescer em Portugal, estabelecendo um ecossistema empresarial diversificado que envolve *startups*, PMEs e grandes empresas que disponibilizam no mercado produtos, serviços e plataformas competitivas. Para melhor conhecer e acompanhar o panorama nacional da cibersegurança em *IoT* recomenda-se a monitorização das seguintes métricas:

Tabela 3 - Métricas potenciais para avaliação societal de segurança no uso de Internet das Coisas

Métrica	Significado	Mecanismo de obtenção
Número de empresas com produtos próprios de "embedded hardware" com conectividade à Internet	Universo de empresas nacionais com produtos *IoT* de hardware	Inquérito anual dirigido às empresas nacionais com vista à recolha de métricas relacionadas com a tipologia de produtos e serviços desenvolvidos (*IoT* ou não), metodologias empregues no seu desenvolvimento, incorporação de tecnologias e mecanismos de segurança, e diagnóstico de ataques e respetivas consequências para a empresa e seus clientes; enriquecido por dados do Serviço de Estatística da União Europeia – Eurostat*
Número de produtos de "embedded hardware" com suporte para atualização de *firmware* assinado "over-the-air"	Produtos *IoT* de hardware nacionais com capacidade de atualizar o seu *firmware* remotamente e de forma segura	
% de produtos de "embedded hardware" conectado com dependendência de plataformas *IoT* fora do território nacional/UE	Produtos *IoT* de hardware nacionais dependentes de plataformas alojadas em territórios possivelmente hostis	
Número de empresas com serviços e/ou plataformas de conectividade e agregação de dados *IoT*	Universo de empresas nacionais que desenvolvem soluções de conectividade e agregação de dados *IoT*	
Número de empresas com dispositivos/ serviços/plataformas *IoT* com processos de desenvolvimento que contemplem a qualidade de *software* na perspetiva da segurança (secure by design, penetration testing, ...)	Empresas nacionais com processos de desenvolvimento que englobam requisitos de segurança	
Número de empresas com protocolos de resposta a incidentes de segurança com os seus dispositivos/serviços/ plataformas *IoT*	Empresas nacionais com mecanismos de resposta a incidentes de segurança definidos	
Número de produtos/serviços/ plataformas *IoT* alvo de ataques de cibersegurança	Determinação do grau de exposição (i.e., risco) para as empresas nacionais	
"Impacto" de ataques de cibersegurança a dispositivos/ serviços/ plataformas *IoT*	Quantificação do volume e impacto de ataques de cibersegurança realizados sobre soluções *IoT* nacionais	
Uso da *IoT* por sector e dimensão da empresa	Natureza da utilização das tecnologias *IoT* (segurança, logística, produção, etc.) em empresas de pequena, média e grande dimensão	Relatório do uso da Internet das Coisas na União Europeia** ou inquérito direto às empresas

* Exemplos do último ano seriam Eurostat (2022). Use of Internet of Things in enterprises – (https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_Internet_of_Things_in_enterprises) e Eurostat (2022). Smart technologies in EU enterprises: AI and IoT – (https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20220609-1

** "Use of Internet of Things in enterprises", EUROSTAT, Maio 2022

Acompanhando a tendência global, a realidade da *IoT* em Portugal modificou-se significativamente na última década. Motivada por um aumento da literacia tecnológica, tecnologias e ferramentas de desenvolvimento mais acessíveis, programas de estímulo ao empreendedorismo e acesso a financiamento mais facilitado, surgiram inúmeras empresas com produtos e serviços *IoT* capazes de colocar globalmente os seus produtos em vários sectores.

O surgimento de empresas capazes de desenvolver e comercializar soluções *IoT* em áreas tão diversas como a robótica, conectividade, segurança, smart cities, mobilidade e energia aumenta a exposição do sector a ameaças e ataques de cibersegurança que podem comprometer setores críticos da economia, tal como as telecomunicações. Além das empresas focadas no desenvolvimento de tecnologias na área *IoT*, há um número crescente de empresas e outras entidades a adotar esta tecnologia em processos de produção e operacionais, ampliando potenciais riscos de ciberataques, dada a facilidade de uso que as tecnologias de *IoT* trouxeram para a área. É, no entanto, importante garantir que **os perigos de cibersegurança associados ao uso de diferentes tipos de plataformas e de soluções IoT são compreendidos pela sociedade em geral.**

O relatório de 2021 da ANACOM sobre adoção da Internet das Coisas nos segmentos residencial e empresarial [62] conclui que "23% das empresas com 10 ou mais pessoas ao serviço utilizaram equipamentos *IoT*" e que a utilização destes equipamentos se encontra concentrada nos sectores da "Eletricidade e Água" (41%), "Alojamento e Restauração" (30%) e "Comércio por grosso e a retalho" (28%). No segmento residencial, o mesmo estudo indica que 19% dos utilizadores de Internet possuem equipamentos domésticos ligado à Internet, destacando-se os "assistentes virtuais na forma de orador inteligente ou de uma aplicação de Internet (9,7% dos utilizadores de Internet), as soluções de segurança, como sistemas de alarme doméstico, detetor de fumos, câmaras de segurança, fechaduras (6,6%), os eletrodomésticos, como aspiradores, frigoríficos, fornos, máquinas de café (5,6%) e os equipamentos que permitem gerir a energia da casa como luzes, tomadas, termostato do sistema de aquecimento, contadores de eletricidade, gás ou água (5,1%)".

O *Capability Maturity Model Integration* (CMMI) [63] é um processo e modelo comportamental que ajuda as empresas a racionalizar a melhoria de processo e a encorajar comportamentos produtivos e eficientes que diminuem os riscos no desenvolvimento de software, produtos e serviços, expressando a sua maturidade em vários níveis. O modelo ITmark é um esquema de certificação que endereça PMEs tecnológicas e que possui objetivos semelhantes ao CMMI, nomeadamente potenciar níveis de eficácia organizacional mais elevados nos "processos de negócio dedicados ao desenvolvimento, manutenção de sistemas, aplicações e produtos de software" [64]. Esta *framework* baseia-se em vários referenciais de certificação, incluindo o CMMI e a ISO 27001, entre outros.

De acordo com o INE [65] existiam em Portugal um total de 1 316 256 empresas em 2020, das quais 21 312 afetas a "Actividades de informação e de comunicação". Contudo, apenas 16 empresas nacionais possuem certificação CMMI válida na área de desenvolvimento (CMMI DEV V1.3 e CMMI DEV) de acordo com a página oficial de *appraisals* CMMI. Relativamente ao IT-Mark,

contabilizam-se em Portugal apenas 17 empresas certificadas, não havendo informação sobre quantas mantêm válido este selo de qualidade. Dado que apenas empresas de desenvolvimento de *software* e de tecnologias de informação e comunicação possuem capacidade técnica para conceber produtos/serviços/plataformas *IoT*, **o reduzido número de certificações na área da qualidade do software poderá indiciar alguma incapacidade** para lidar com os riscos e desafios associados, nomeadamente ao nível da cibersegurança. Neste sentido, **recomenda-se a promoção das melhores práticas de desenvolvimento de software**, estimulando a obtenção de certificações do processo reconhecidas internacionalmente por parte de empresas TIC. Adicionalmente, **deve-se fomentar a adoção de práticas específicas de cibersegurança propugnadas pela ENISA** através de programas de imersão para engenheiros e programadores, estimulando e apoiando à criação de comunidades profissionais de cibersegurança.

Ao nível de tecnologias recentes, e numa perspetiva de evoluções futuras, recomenda-se a exploração de novas abordagens de segurança, particularmente recorrendo a tecnologias emergentes tais como as DLTs e as plataformas *Chip-to-Cloud* como mecanismos para estabelecer comunicações mais seguras entre dispositivos *IoT* e com plataformas de agregação de dados. Neste âmbito, poderão ser exploradas novas avenidas para o estabelecimento de confiança entre entidades do ecossistema *IoT*, por exemplo tendo como base o paradigma emergente de *Self-Sovereign Identity*, em particular nos cenários de mobilidade onde a utilização de soluções clássicas de PKI implicam um elevado custo operacional face à volatilidade das interações *IoT*.

Relativamente a utilizadores finais, **sugere-se a adoção da rotulagem de produtos de consumo IoT ao nível da cibersegurança** como forma de permitir uma identificação mais simples e direta de quais os produtos "seguros" no sector. É fundamental que a rotulagem a adotar seja globalmente reconhecida e promovida junto da população em ações de divulgação alargadas que alcancem o maior número de (potenciais) utilizadores. O surgimento de um padrão global parece ser uma realidade eminente (1º trimestre de 2023), promovida por empresas líderes na oferta de produtos *IoT* tais como a Google, Intel e Samsung e por grandes organizações do sector, destacando-se o American National Standards Institute (ANSI), Consumer Technology Association, CTIA e a Connectivity Standards Alliance, que promove o standard de interoperabilidade *IoT* conhecido por Matter.

Adicionalmente, é importante criar programas de sensibilização para utilizadores finais que estimulem a consciencialização para um número crescente de dispositivos *IoT* presentes no dia-a-dia e para a necessidade de os conhecer e manter atualizados.

Inteligência Artificial e as suas aplicações

4

APRESENTAÇÃO DO CONCEITO

A definição de Inteligência Artificial (também conhecida por *Artificial Intelligence* ou AI) é algo complexa nos dias de hoje, não por falta de rigor na definição formal, mas devido ao contexto atual da utilização extensa do termo na sociedade em geral.

A definição formal de AI é "qualquer forma de inteligência demonstrada por meios artificiais e não naturais" [82]. Atualmente a UE (União Europeia) define como sistema inteligente todo aquele capaz de aprender, modelar ou raciocinar usando para isso meios tecnológicos. Assim, aplicado ao contexto de informática, é qualquer programa ou serviço que tenha a capacidade de tomada de decisão inteligente para atingir o seu objetivo de forma mais eficiente. Usando esta definição, o conhecido motor de busca da Google ou o sistema de recomendação de compras da Amazon são sistemas com capacidade de AI.

A perceção da sociedade sobre o tema é bastante diferente. O termo AI está fortemente conectado a robots, androides, ou outros equipamentos eletrónicos que poderão substituir os humanos em múltiplas tarefas, ou as tarefas de decisão associadas a todos os cenários de *IoT*. Embora todas essas áreas utilizem métodos e algoritmos da área de AI, não são a área em si. O problema desta perceção é que desvia a atenção de AI de outras áreas (menos mediáticas) onde técnicas de AI podem estar a ser implementadas/utilizadas, e ofuscam os problemas intrínsecos à área, confundindo-os com os problemas aplicacionais dessas áreas.

Finalmente é importante fazer a distinção entre Inteligência Artificial, Aprendizagem Máquina (também conhecido por *Machine Learning* ou ML) e Aprendizagem Profunda (também conhecido por *Deep Learning* ou DL). Estes conceitos são muitas vezes usados como sinónimos, quando na verdade representam três áreas com características distintas. Uma forma simples de perceber as relações entre estas três áreas é através do diagrama apresentado na Figura 7. Como se pode ver a área de AI inclui as restantes duas áreas, ou seja, tanto a área de aprendizagem máquina, como a área de aprendizagem profunda, são subáreas de inteligência artificial. E a mesma relação existe com aprendizagem máquina e aprendizagem profunda. Aprendizagem Máquina é definida como algoritmos informáticos que utilizam dados para melhorar o seu funcionamento. A aprendizagem profunda, sendo uma subárea, são também algoritmos que usam dados externos para melhorar o seu funcionamento. A diferença perante a anterior é a utilização de modelos mais complexos (tipicamente usam mais camadas para a operação de aprendizagem, dando origem ao nome).

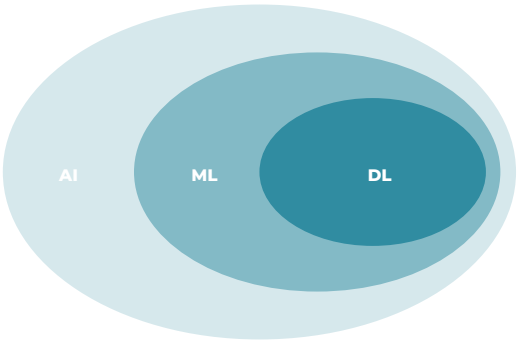


Figura 7 – Diferentes áreas de Inteligência Artificial

Atualmente, os algoritmos de aprendizagem máquina são muito populares em diferentes aplicações, conseguindo ultrapassar a capacidade de deteção de humanos em diversas tarefas (embora muito específicas). No entanto, nenhum destes algoritmos possui um nível de inteligência generalizada similar a um ser humano.

BREVE RESENHA HISTÓRICA

O início da AI está ligado aos filósofos clássicos que tentaram descrever o funcionamento do pensamento humano utilizando a manipulação lógica de símbolos. No entanto, somente em 1946 foi desenvolvido o primeiro computador do mundo (ENIAC - Electronic Numerical Integrator and Computer), criando as condições necessárias para os cientistas discutirem o desenvolvimento de um cérebro eletrónico, capaz de resolver problemas de forma semelhante a um ser humano. A área de AI foi oficialmente fundada durante uma conferência no Dartmouth College no verão de 1956.

Na sua evolução desde os anos 50, a área de AI passou por três períodos de crescimento pontuados por dois períodos de menor interesse (frequentemente chamados de "invernos de AI") como representado na Figura 8. Estes períodos de esmorecimento representam a estagnação de uma determinada técnica dentro da área de AI.

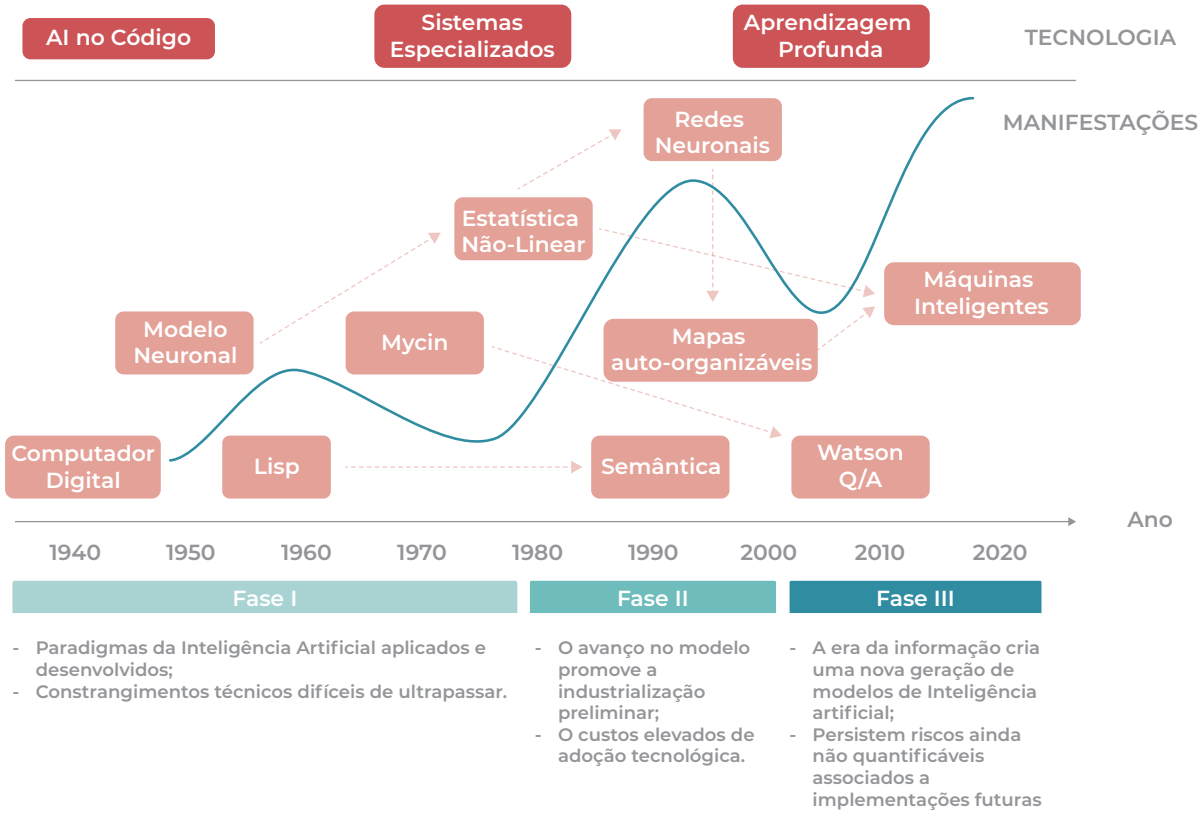


Figura 8 – Fases de evolução da AI.

O primeiro período de crescimento começou por volta da época em que a área começou, em 1950. Durante esse período desenvolveram-se modelos para reconhecimento de fala, agentes para jogar jogos clássicos, robots simples e algoritmos de resolução de problemas. Mas os investigadores não conseguiram concretizar as suas ambições associadas à área, e os seus patrocinadores retiraram fundos em meados da década de 1970. O investimento retornou no início da década de 1980, quando o projeto Japonês de Quinta Geração investiu grandes somas na investigação da AI e em máquinas lógicas de alto desempenho. Este período durou até ao final dos anos 80, quando mais uma vez os resultados obtidos não corresponderam às expectativas. O terceiro período de crescimento começou no início dos anos 90 com o desenvolvimento de tecnologias chamadas *Machine Learning*, que começaram a produzir resultados significativos, úteis, e muitas vezes surpreendentes e que foram acompanhados de grandes doses de propaganda sobre o futuro da AI. A aprendizagem máquina refere-se a programas que desenvolvem a sua função a partir da exposição a muitos exemplos, e não a partir de regras estabelecidas pelos programadores. De notar que **ML depende inerentemente da existência de muitos dados, e da sua adequação para a função que se pretende implementar.** Alguns investigadores de AI fizeram grandes apostas sobre este e outros métodos de alcançar inteligência artificial geral que pode estar fora do alcance das máquinas. Neste momento, estão a ser usadas técnicas de aprendizagem profunda (*Deep Learning*), que são modelos com múltiplas camadas de inferência que permitem a aprendizagem de problemas e padrões mais complexos.

Historicamente existem 7 níveis na hierarquia de AI:

1. **Nível 0 - Automação:** conceção e implementação de autómatos que realizam ou controlam processos (simples) com pouca ou nenhuma intervenção humana.

2. **Nível 1 - Sistemas de Regras:** são programas que resolvem problemas usando para isso inferências baseadas num conjunto de regras lógicas definidas por um perito.

3. **Nível 2 - Aprendizagem supervisionada:** são modelos de ML que conseguem aprender um modelo (simplificação da realidade) dado um conjunto de dados de entrada. Para este nível é necessário que o conjunto de dados contenha os parâmetros de entrada assim como o resultado expectável para cada conjunto de dados de entrada.

4. **Nível 3 - Aprendizagem não supervisionada:** são modelos de ML que aprendem usando um conjunto de dados de entrada, no entanto este conjunto de dados não possui o resultado esperado para cada conjunto de parâmetros de entrada. Neste caso, o modelo tem de procurar padrões nos dados de forma autónoma.

5. **Nível 4 - Interações multiagentes:** a este nível, a inteligência de máquina emerge das interações de milhares ou milhões de agentes, cada um com uma função específica. A capacidade de aprendizagem da máquina surge do coletivo.

6. **Nível 5 - AI Criativa:** este é um nível intermédio entre máquinas que apoiam equipas criativas e máquinas que demonstram inteligência generalizada: modelos capazes de produzir resultados com elevado nível de criatividade (sendo exemplos disso músicas ou pinturas).

7. **Nível 6 - Inteligência generalizada:** É o nível mais elevado de inteligência, similar ou superior ao nível de um ser humano.

É importante referir que os últimos dois níveis, embora estejam a ser considerados pela comunidade académica, não são possíveis de serem implementados com a tecnologia atual. Ainda existem bastantes avanços nos três níveis anteriores até a tecnologia poder ser considerada madura. Existe uma tendência crescente para a simplificação destes processos através de plataformas de AI (tipicamente associadas a plataformas de *IoT*, como mencionado na seção anterior). Estas novas plataformas têm cada vez mais capacidade e funções para recolha de dados e cada vez mais existem plataformas de *IoT* a recolher dados e dotadas de algoritmos de AI para fornecer serviços personalizados e adaptados aos utilizadores. Estes serviços personalizados oferecem mais qualidade de vida aos utilizadores, tornando-os dependentes das comodidades oferecidas. No entanto, o uso dos dados destas plataformas não é transparente e o controlo sobre os dados recolhidos e processados é frequentemente algo relaxado.

FUTURO A 5 E 10 ANOS

O desenvolvimento de um novo tipo de ambiente cibernético irá trazer alguns constrangimentos em termos sociológicos e tecnológicos. O uso de dispositivos inteligentes e a utilização cada vez maior de ambientes inteligentes (explorando ML, e necessitando de grandes volumes de dados) criam um problema diário de proteção de dados com os quais os utilizadores comuns já têm de lidar [81], mas que será um problema cada vez maior à medida que ML for usada em mais aplicações, necessitando de mais dados. A monitorização constante das tarefas diárias dos utilizadores leva ao armazenamento de uma grande quantidade de dados pessoais, pondo em causa a privacidade dos utilizadores. Contudo, é precisamente esta geração e armazenamento de dados que é essencial para que os algoritmos de AI obtenham um bom desempenho, garantindo os melhores resultados para diferentes tarefas. Os sistemas de recomendação são, por exemplo, sistemas nos quais padrões de comportamento dos utilizadores são explorados de forma a poder ser recomendado o melhor serviço, seja o melhor restaurante para um dado utilizador ou pesquisas relacionadas com o que pesquisou anteriormente [84]. Desta forma, no presente e num futuro próximo, iremos presenciar cada vez mais a utilização de sistemas inteligentes, dispositivos inteligentes que recolhem dados permanentemente que poderão depois ser usados para executar funções (de recomendação).

Já se verifica a utilização de AI em sistemas de defesa de cibersegurança para melhoria de resiliência dos mesmos. De acordo com algumas observações feitas no ano de 2021, a AI ainda não tem um papel determinante nos ataques realizados contra as organizações, no entanto é expectável que isso se venha a tornar uma realidade [86]. Por outro lado, embora a evolução dos algoritmos de AI se possa

tornar uma mais-valia na deteção de ataques, também poderá contribuir fortemente para uma maior automação de ataques informáticos mais eficientes.

Paralelamente, o futuro da AI passará também por uma necessidade urgente de regulamentação no que diz respeito à integração de sistemas inteligentes na sociedade. O nível de supervisão regulamentar (incluindo aspetos éticos) existente em áreas tecnológicas é frequentemente difícil de implementar em sistemas de AI, dada a opacidade final do sistema, onde não é discernível a relação entre o resultado e a forma como foi atingido. Em alternativa, e de forma mais simples, poderão ser estabelecidos requisitos em relação à forma como os algoritmos são treinados e testados. Desta forma, **o futuro passará também por haver uma garantia de qualidade e usabilidade** estabelecida com base em alguns tipos de parâmetros [87].

Um outro aspeto para o futuro prende-se com o relacionamento da AI com a própria sociedade e os humanos em geral. A recente popularidade dos modelos conversacionais generativos (e.g. GPT-3) trouxe este problema para a ribalta. Os riscos inerentes para a sociedade face à exposição dos utilizadores a sistemas de AI têm vindo a ser discutidos devido essencialmente a fatores como a probabilidade de sofrerem ataques informáticos que podem comprometer a sua segurança, privacidade e em casos extremos como colocar a vida dos cidadãos em risco, por exemplo, por falhas em carros autónomos.

Independentemente destes aspetos, é expectável que haja uma mudança nas estratégias de marketing bem como, por exemplo, nos comportamentos dos clientes. De forma ilustrativa e recorrendo ao setor dos transportes, temos o conceito dos carros autónomos, isto é, sem motorista e incorporando AI, que podem vir a fazer parte do futuro; mas tal exigirá uma modernização de muitos serviços de transporte e uma adaptação dos clientes à nova realidade. Além disso, a condução autónoma poderá influenciar, ainda que indiretamente, hotéis ou comércio relacionado por não haver necessidade de pausas por parte dos condutores. Ou, noutro exemplo, poderemos ter os vendedores em lojas substituídos/auxiliados por algoritmos de AI para prestar auxílio aos consumidores: com recursos avançados de análise de voz, um agente de AI poderá inferir pelo tom de um cliente que um problema não mencionado existe ou persiste e fornecer feedback em tempo real para orientar a próxima abordagem do vendedor (humano). Nesse sentido, a AI pode aumentar as capacidades dos vendedores, mas também pode desencadear consequências negativas não intencionais, especialmente se os clientes se sentirem desconfortáveis com tais sistemas [88], algo que pode até ser dependente de aspetos como género, raça ou condição social, ou do tipo de dados usados para o treino dos sistemas. Numa linha paralela, a introdução crescente de AI/ML poderá levar a substituição de postos de trabalho, ou levar a sérias falhas associadas a proteção intelectual ou privacidade (como se tem visto com os modelos conversacionais generativos) podendo originar reações sociais. Exemplos incipientes de todos estes aspetos já se podem encontrar em produtos atuais.

Os sistemas de AI são muitas vezes confrontados com numerosas ameaças, de diferentes ordens, em termos de cibersegurança. Essas ameaças podem incidir sobre o sistema de informação que suporta a plataforma de AI/ML (p.ex., uma vulnerabilidade do Sistema Operativo também conhecido por SO), sobre o sistema de AI/ML em si (p.ex., explorar uma vulnerabilidade numa das funções), sobre a cadeia de fornecimento do sistema, ou pela interceção/análise/manipulação do tráfego de rede que comunica com o sistema de AI/ML. Além disso, os próprios resultados de um algoritmo de AI devem ser corretos, isto é, estarem de acordo com o esperado pelo modelo e serem não manipuláveis, uma vez que já foram relatados casos de ataques maliciosos a sistemas baseados em AI, levando a resultados inesperados. Por norma, os mais conhecidos ataques exploram vulnerabilidades como falhas no código fonte ou existência de erros nas interfaces que permitam um acesso direto ao sistema. A utilização de AI tem riscos e preocupações justificadas.

Através de reconhecimento de padrões e respetiva alteração dos padrões de dados de entrada num modelo é possível alterar o comportamento de um sistema baseado em AI, mesmo sem afetar diretamente o computador: um modelo de ML pode ser projetado para reconhecer, por exemplo, sinais de trânsito, extraindo padrões como cores e formas para reconhecer o que o sinal representa. Uma pequena alteração num sinal pode ser suficiente para que o modelo associe a entrada a um outro padrão e produza um resultado de saída diferente do expectável podendo efetuar uma má classificação.[6] Esse é um problema praticamente indetetável se não se utilizarem técnicas de *Explainable* AI [85] que, justamente, têm recebido atenção crescente. Estas técnicas permitem validar o processo de tomada de decisão de um sistema inteligente.

Os ciber-criminosos também recorrem a ataques inteligentes que se propagam automaticamente num sistema ou numa rede. O *malware* inteligente pode, por exemplo, explorar vulnerabilidades não mitigadas, levando a um aumento da probabilidade de alvos totalmente comprometidos. Além disso, a AI pode aprender a detetar comportamentos e aprender a reconhecer padrões dos mesmos e desta forma convencer de forma mais eficiente os utilizadores de que aquilo que lhes é apresentado é benigno mesmo não o sendo [86].

A utilização de sistemas de AI sem compreender o seu funcionamento, pode por si só, constituir um problema de segurança. Tipicamente, a informação sobre o processamento dos dados e a forma como os dados são guardados está descrita nas políticas de privacidade que são apresentadas aos utilizadores antes de ser possível usar o sistema, sendo expectável que o utilizador esteja informado e dê consentimento para o processamento dos seus dados. Estas políticas de privacidade são, contudo, documentos extensos e complexos, dificilmente apreendidos por todos os utilizadores. Assim, a não adaptação e simplificação dos documentos referentes às políticas de privacidade — ou a sua deliberada complexificação — faz com que os utilizadores forneçam consentimento para o processamento dos seus dados sem estarem devidamente informados sobre o que efetivamente estão a consentir,

6 Este pode ser um problema, p.ex., na utilização de carros autónomos em que confundir por exemplo um sinal de STOP com um semáforo verde pode ser catastrófico para vidas humanas [59].

podendo suscitar uma violação de privacidade. A recolha de dados pessoais como dados biométricos e de localização são problemas de privacidade que podem afetar a segurança dos cidadãos. A utilização deste tipo de dados por parte dos algoritmos de AI pode constituir sérios riscos para os cidadãos na medida em que em cenário de ataque informático todos estes dados possam ser expostos ou a sua integridade possa ser comprometida.

Para aumentar a maturidade da cibersegurança em sistemas AI/ML, é necessária uma visão holística do ambiente cibernético das organizações, na qual a AI é combinada com o discernimento humano, uma vez que nem as pessoas, nem a AI, denotam por si só capacidade de resolução de todos os problemas. Portanto, o uso responsável das técnicas de AI, e a escolha de técnicas de AI que sejam auditáveis por um humano, será essencial para mitigar ainda mais os riscos e as preocupações relacionados. É, assim, necessário ter uma base comum e unificadora para compreender potenciais ameaças e, consequentemente, realizar avaliações de risco específicas para cada sistema. Desta forma, é possível apoiar a implementação de medidas e controlos de segurança direcionados e proporcionais de forma a combater as ameaças relacionadas com AI.

A AI permite uma tomada de decisão automática e facilita muitas tarefas que fazem parte de uma rotina diária, fornecendo melhorias das operações e inúmeros outros benefícios. Um aumento da dependência da tecnologia para o funcionamento da sociedade origina maiores riscos, com uma maior exposição a ciberataques, erros de programação, disrupção de cadeias de fornecimento/falta de componentes, entre outros eventos adversos e outras eventuais consequências que vão para além da tecnologia, potencialmente afetando a sustentabilidade e a segurança social.

Numa outra dimensão, além das implicações face à exposição a ataques informáticos e problemas de privacidade, surgem problemas relacionados com a forma como os algoritmos de AI podem afetar o comportamento dos cidadãos Casos específicos, como os sistemas de recomendação, assentam na recolha de dados relativos às preferências dos utilizadores e consequente previsão de opções semelhantes para sugestão. Este tipo de sistemas é fortemente usado em estratégias de marketing, interferindo no comportamento dos utilizadores - as plataformas de venda online, em que após a pesquisa por um determinado produto são disponibilizados produtos semelhantes ao utilizador, é um dos exemplos mais conhecidos deste modelo.

OPORTUNIDADES

Quando os sistemas de segurança convencionais são lentos e insuficientes, as técnicas de AI podem melhorar o seu desempenho ao nível de segurança e fornecer uma melhor proteção contra o número crescente de ameaças cibernéticas sofisticadas [89].

As áreas de cibersegurança onde são frequentemente usados algoritmos de AI e/ou ML são normalmente conhecidos como *intrusion detection*, *malware*, *ransomware*, *Denial of Service* e *phishing*. Além disso, as técnicas de AI consideradas promissoras e que são atualmente foco de investigação para cibersegurança são Natural Language *Processing*, automatização e robótica. Os algoritmos de *Natural Language Processing* são essencialmente usados em intrusion detection, *ransomware* e *phishing*, enquanto

que os algoritmos de automatização e robótica são normalmente usados em ataques de *malware* .

A relação entre AI e cibersegurança pode ser vista de duas formas diferentes:

1. Uma delas, relaciona-se com a utilização de técnicas de AI para a resolução ou prevenção de ataques. Na Tabela 2, são apresentados possíveis problemas na área de cibersegurança, e como técnicas de AI podem solucionar ou prever o problema de forma a evitá-lo.

2. Outra abordagem (que não iremos elaborar) enfatiza a utilização das técnicas de AI para criar ataques.

Tabela 4 – AI e áreas de cibersegurança

		Incidências em Cibersegurança				
		Intrusion detection	*Malware*	*Ransomware*	*Denial of Service*	*Phishing*
Técnicas de AI	Artificial *Immune Systems*	(1)				
	Deep Learning	(2)		(7)		(11)
	Artificial Neutral Network	(3)				
	Machine Learning	(4)	(6)	(8)	(10)	(12)
	Natural *Language Processing*	(5)		(9)		(13)

(1) *Artificial Immune Systems* & *Intrusion Detection*

Os *Artificial Immune Systems* (AIS) podem ser utilizados para resolver questões relacionadas com intrusões, nomeadamente na deteção de intrusões. Estes sistemas são conhecidos como *Intrusion Detection Systems* (IDS) e são úteis para identificar atividades maliciosas existentes na rede, tal como, o uso indevido ou não autorizado. Contudo, têm uma capacidade limitada em termos de deteção de ataques distribuídos. Estes sistemas exploram características como a capacidade de aprender, de forma a possibilitar a resolução de diversos problemas. Assim, são uma excelente abordagem para a resolução de problemas, ao nível de segurança, existentes nas redes de computadores. [90][91]

(2) *Deep Learning* & Deteção de intrusão

Diferentes técnicas de *Machine Learning* podem desempenhar um papel importante contra ameaças em termos de cibersegurança. Contudo, o *Deep Learning* facilita o processo por não ser necessário uma extração explícita de características. O *Deep Learning* consegue detetar correlações não lineares inerentes aos dados, suporta qualquer tipo de ficheiros e permite detetar ataques

desconhecidos, tornando-se assim uma vantagem ao nível de segurança. É baseado em aprendizagem e pode ser usado em sistemas autónomos devido às vantagens que apresenta ao nível da otimização, discriminação e previsão. Assim, a este nível é possível considerar sistemas como IDS, Network Intrusion Detection System (NIDS), *Host Intrusion Detection System* (HIDS) ou *Intrusion Detection and Prevention Systems* (IDPS). A utilização de *Deep Learning* em IDS, na deteção e resistência a intrusões, denota maior precisão, apresentando assim melhores resultados e melhorando o desempenho.[92][93][94]

(3) *Artificial Neural Network* & Deteção de intrusão

As Artificial Neural Network (ANN) são um modelo estatístico de aprendizagem que se inspira na estrutura de funcionamento do cérebro humano ajudando a aprender e a resolver problemas, especialmente em ambientes onde as regras e os algoritmos para resolução de problemas são difíceis de explicitar ou são desconhecidos. Os *Intrusion Detection Prevention Systems* (IDPS) são usados para proteger um sistema ou redes inteiras e já demonstraram ao longo do tempo ser uma ferramenta útil para a cibersegurança. Estes sistemas podem identificar atividade maliciosa através da definição de padrões de comportamento incomum da rede e/ou do sistema ou podem estabelecer uma definição de padrões de comportamento comum da rede e/ou do sistema. Desta forma, é conseguida uma otimização de desempenho, máxima proteção e minimização do erro. No entanto, têm a sua capacidade limitada no que toca à deteção de atividade maliciosa e demonstram uma falha ao nível de escalabilidade, resiliência e automatismo. Quando os ANN são integrados nos IDPS, se for detetada alguma irregularidade na informação, a mesma é classificada como maliciosa e é rejeitada. Enquanto os IDPS trabalham essencialmente contra intrusões conhecidas, a abordagem dos ANN está protegida contra instâncias de intrusões que são ainda desconhecidas [116]. Esta abordagem protege com sucesso o sistema contra possíveis intrusões, na medida em que torna o IDPS mais robusto, adaptável e preciso. A utilização de ANN nos IDPS não limita a sua utilização e pode ser inclusive utilizada em qualquer sistema que monitoriza atividades de redes, além de permitir que sejam detetados ataques em tempo real [89][116].

(4) *Machine Learning* & Deteção de intrusão

Os algoritmos de *Machine Learning* focam-se essencialmente na classificação e regressão, podendo ser utilizados para a deteção de anomalias ou intrusões de forma eficiente, uma vez que são preparados e posteriormente aplicados em parâmetros de entrada usualmente invisíveis pelo processo normal de deteção de intrusões. Utilizando os algoritmos de *Machine Learning* e começando com uma pré-preparação dos dados, seguido de uma conversão e otimização, conseguimos classificar se existe ou não uma possível intrusão. [95][96]

(5) *Natural Language Processing* & Deteção de intrusão.

A *Natural Language Processing* (NLP) captura a relação entre as palavras e a forma como foram expressas, e dispõe de vários métodos para automatizar a análise de grandes volumes de texto. Além disso, abrange áreas específicas como análise probabilística, resolução de ambiguidades, extração de informações ou análise de discurso. Todas estas áreas podem ser aplicadas à análise de registos de acesso ao sistema, detetando potenciais intrusões.

Pode-se ainda automatizar o processo de extração da informação significativa, usando para isso modelos semânticos, existente no sistema de rastreio de problemas, tendo a informação extraída uma elevada probabilidade de relacionamento com a tentativa de intrusão. [97][98]

(6) *Machine Learning & Malware*

Malware é considerado qualquer *software* com intenções maliciosas, isto é, todo o *software* com capacidade para explorar vulnerabilidades do sistema operativo e de aplicações computacionais. As técnicas de ML desempenham um papel fundamental no desenvolvimento de sistemas inteligentes, pois conseguem distinguir entre o que é definido como malicioso e o que é benigno. A *Machine Learning* pode ser aplicada de forma efetiva em situações em que se verifica uma ameaça de *malware*, nomeadamente na sua deteção e identificação, ajudando assim na diminuição dos ataques por *malware* de que os sistemas sejam alvo. A utilização de *Machine Learning* geralmente foca-se em encontrar possíveis ligações em dados observados e minimização de relações, e como tal provou ser capaz de detetar possíveis variações de *malware*, além de que consegue compreender o comportamento do *malware* e analisar como o mesmo evolui. [99][100]

(7) *Deep Learning & Ransomware*

Ransomware consiste em provocar a indisponibilidade do sistema e dados da vítima, e usualmente os ataques têm início na cifragem de ficheiros importantes, como fotografias e documentos. Após a realização do ataque é feito um pedido de resgate para que a vítima consiga recuperar o sistema e os dados. Um ataque de *ransomware* pode ocorrer de várias formas por exemplo, através de downloads em páginas maliciosa ou em e-mails de *phishing*. A partir do momento em que se acede ao sistema do utilizador, o *ransomware* começa a agir, conseguindo obter informação acerca do utilizador, bem como informação sobre o sistema a que acedeu. O Deep Learning tem sido usado na deteção de *ransomware*, pois permite que se aprenda a representação abstrata de dados, como imagens e discursos. Como tal, de forma intuitiva e prática, é possível criar um classificador que permite detetar possíveis ataques de *ransomware*. [101][102]

(8) *Machine Learning & Ransomware*

A deteção de *ransomware* utilizando ML é possível com um modelo híbrido de regressão e um algoritmo baseado em regras. O algoritmo de regressão permite construir o modelo de previsão baseado na relação entre prognósticos e resultados, enquanto o algoritmo baseado em regras irá gerar um conjunto de regras para o modelo de previsão. Esta combinação permite a criação de um modelo robusto que segue um conjunto de regras, que serão fortalecidas com a formulação do relacionamento com o algoritmo de regressão.[103][104] O modelo de regressão oferece uma maior adaptabilidade que não é possível apenas com um modelo de regras estáticas.

(9) *Natural Language Processing & Ransomware*

A utilização de *Natural Language Processing* para combater ataques de *ransomware* mostra-se eficiente, pois permite que sejam verificados comportamentos diferentes no sistema e ajuda no seu combate. [105][106]

(10) *Machine Learning & Denial of Service*

Os ataques de *Distributed Denial of Service* (DDoS) são lançados através de computadores geridos remotamente. São bem organizados e amplamente distribuídos, tendo como objetivo sobrecarregar os recursos da Internet, de forma a deixar determinados serviços inacessíveis, fazendo os utilizadores enviarem um largo número de pedidos dispendiosos de processar pelos sistemas.. As abordagens defensivas com recurso a AI têm aumentado de forma bem-sucedida. A grande vantagem da utilização de *Machine Learning* na deteção de ataques de DDoS centra-se na flexibilidade inerente ao ML, que vai alterar o seu desempenho com base nos dados recolhidos. [107][108]

(11) *Deep Learning & Phishing*

O *phishing* é um tipo de ataque em que se usam técnicas de engenharia social para capturar informação sensível de uma vítima. Pode ser utilizado através de correio eletrónico ou de sites contrafeitos para roubar informações sensíveis aos utilizadores, como o número do cartão de crédito, ou dados para início de sessão, entre outros. Para o efeito, o atacante simula uma marca credível ou personifica alguém de confiança. Apresenta um elevado risco para instituições que gerem o seu negócio online, pois diminui a confiança do consumidor, além do elevado dano financeiro que ocorre com a realização de um ataque de *phishing*. O Deep Neural Network (DNN) é uma técnica de DL, suportando grandes volumes de dados, que consegue aprender sobre recursos com múltiplos níveis de abstração, o que permite ao sistema aprender funções complexas de mapeamento para, através dos dados da entrada, obter diretamente os dados de saída, sem depender de recursos humanos. É utilizado para classificar os URLs enquanto URLs de *phishing* ou legítimos. A utilização de Deep Learning para detetar e combater possíveis ataques de *phishing* é eficiente pela sua elevada precisão; é ainda possível utilizar diferentes algoritmos de Deep Learning para tornarem a defesa do sistema mais forte, visto que os algoritmos se complementam. [109][110]

(12) *Machine Learning & Phishing*

Os sistemas tradicionais de ML, de sua natureza mais simples, quando usados para a deteção de *phishing* podem falhar por vários motivos. Esta imprecisão ocorre quando estes modelos são apenas treinados com os detalhes de um URL. Para tal, podem ser utilizados algoritmos ML como *Random Forest*, mais complexos e capazes de inferências mais precisas. Uma das grandes vantagens deste modelo é a utilização de um sistema de voto interno que permite agregar a tomada de decisão através de múltiplos modelos. Sistemas de deteção baseados em *Random Forest* são bastante capazes na identificação de *phishing*. [111][112]

(13) *Natural Language Processing & Phishing*

Recorrendo a técnicas de NLP é possível evitar ataques de *phishing*. É possível detetar os diferentes contextos e conteúdos num e-mail padrão, ajudando na identificação[113][114]. No entanto, o desenvolvimento recente de modelos baseados em *Large Language Models* (dos quais so ChatGPT é o exemplo mais conhecido) tem tornado o uso de NLP uma técnica muito eficaz também usada em ataques de *phishing*.

POTENCIAIS INDICADORES DA ÁREA

O número crescente de ataques informáticos que tem vindo a acontecer nos últimos 5 anos refletem uma necessidade de adaptação por parte das empresas ou serviços de forma a robustecer a sua defesa contra este tipo de ataques, podendo para tanto recorrer a tecnologias associadas a AI. Dado a falta de normas para o desenho e implementação de modelos da AI/ML é sempre complexo definir métricas para avaliar os impactos da área. No entanto existem duas direções que podem indicar a evolução da área: i) a legislação que está a ser considerada para legislar o uso de AI/ML em serviços com impacto para o público (e abordada na secção final de Legislação Adicional), ii) os movimentos de XAI (*explainable* AI) que ambicionam de alguma forma facilitar a compreensão do processo de tomada de decisão (auxiliando a atribuição de responsabilidades e a auditoria de processos).

De acordo com um relatório da ENISA sobre AI [115], interessa considerar nestes casos:

- A autenticidade dos dados pode ser afetada quando a integridade é comprometida, uma vez que os dados ou resultados podem ser afetados.
- A autorização que pode ser afetada quando a confidencialidade e a integridade são afetadas, dado que a legitimidade da operação possa ser prejudicada.
- O não repúdio pode ser afetado quando a integridade é afetada.
- Robustez de um sistema baseado em AI pode ser afetado quando a disponibilidade e integridade são afetadas.
- A confiança num sistema baseado em AI pode ser afetada quando a integridade, confidencialidade e disponibilidade são afetadas, porque o sistema pode ser operado com dados corrompidos ou com baixo desempenho.
- A segurança pode ser afetada quando a integridade ou disponibilidade são afetadas, uma vez que estas propriedades podem afetar negativamente a operação adequada de um sistema de AI.
- A transparência pode ser afetada quando a confidencialidade, integridade ou disponibilidade são afetadas comprometendo a informação sobre como o sistema se comportou e os respetivos fundamentos.
- A explicabilidade pode ser afetada quando a confidencialidade, integridade ou disponibilidade são afetadas, uma vez que dificulta a inferência de explicações adequadas sobre o comportamento de um sistema baseado em AI.
- A proteção de dados pessoais pode ser afetada na medida em que a confidencialidade, disponibilidade e integridade dos dados podem ser afetados, e uma exposição de dados pessoais a terceiros ser suscetível de constituir violação de privacidade.

Assim, de uma forma pragmática, os principais indicadores de segurança em AI baseiam-se essencialmente em três pilares: Prevenção, Deteção e Resposta. A obtenção de valores quantitativos é difícil, dada a opacidade dos algoritmos em si, bem como a sua dependência dos dados. No entanto, podem ser identificados alguns indicadores que aferem a evolução dos problemas de segurança da área. Esses indicadores nesta área poderão incluir [117]:

Tabela 5 - Métricas potenciais para avaliação societal de segurança no uso de Inteligência Artificial

Métrica	Significado	Mecanismo de obtenção
Atribuição de responsabilidade (sistema inteligente, quem o desenvolveu ou quem o usa)	É necessário compreender de quem é a responsabilidade em caso de falha e como atribuir essa responsabilidade	A responsabilidade em caso de falha deve ser atribuída a quem o desenvolveu ou a quem usa o sistema inteligente, mediante circunstâncias específicas a cada caso concreto.
Transparência no processamento dos dados e nos algoritmos usados, incluindo evidências de preocupações éticas no uso da tecnologia	A forma como os dados são processados, os algoritmos usados e o uso dos dados deve ser transparente para o sujeito de dados, isto é, o sistema baseado em AI deve fornecer este tipo de informação ao sujeito de dados de forma simples e clara.	Definição, uniformização e normalização dos processos de aprendizagem e inferências dos modelos de AI/ML
Capacidade de resposta em caso de deteção de anomalia no algoritmo	Avaliar a capacidade de resposta a uma eventual anomalia no algoritmo poderá prevenir a ocorrência de acidentes ou resultados indesejáveis por parte do sistema baseado em AI. Além disso torna o algoritmo muito mais robusto e otimizado.	Definição, uniformização e normalização das implementações de AI/ML validando a sua atuação de forma controlada e sistemática.
Conhecimento do nível de confiança dos algoritmos de AI/ML	Diferentes modelos de AI/ML possuem diferentes capacidades de aprendizagem. Numa instanciação é normal o uso de múltiplos modelos para a concessão de um sistema mais inteligente. No entanto, é necessário perceber o impacto de cada um dos modelos de aprendizagem.	Definição, uniformização e normalização das implementações de AI/ML principalmente ao nível de combinação de múltiplos modelos num sistema inteligente complexo. Deve ser possível identificar a contribuição de cada modelo para a decisão final.

Portugal tem vindo a demonstrar bons resultados de inovação, estando bem posicionado em termos de colaborações internacionais de investigação e inovações de produtos ou processos nas Pequenas e Médias Empresas (PME). Assim, é possível assumir que Portugal tem desenvolvido um ambiente favorável à inovação na área da AI [118]. Em Portugal há muitas empresas que se têm destacado pelo desenvolvimento de produtos inovadores baseados em sistemas inteligentes. Algumas das empresas nacionais com maior projeção tecnológica utilizam técnicas de AI como uma componente essencial para o seu modelo de negócio. Em ambiente académico, são várias as universidades e institutos de investigação associados que têm vindo a promover projetos de investigação em AI e ML aplicados a medicina, redes, serviços, robótica e condução autónoma, originando frequentemente *spin-offs* comerciais.

Como vimos, a AI apresenta diversos benefícios para a nossa sociedade, e Portugal encontra-se integrado nas tendências mundiais. Contudo, a opacidade de muitos algoritmos pode comprometer a sua coexistência com utilizadores comuns. Isto significa que devem ser mantidos os requisitos em termos de segurança e dos direitos fundamentais.

Entre os direitos fundamentais importantes, neste contexto, é possível destacar o direito à privacidade, onde o utilizador deve estar informado acerca de tudo o que envolve o processamento dos seus dados pessoais. De acordo com o regulamento em vigor na União Europeia (Regulamento Geral de Proteção de Dados, também conhecido por RGPD), o processamento de dados pessoais deve ser realizado com base no consentimento dado pelo proprietário dos dados sendo que este consentimento deve ser atribuído de forma clara e inequívoca estando o utilizador informado sobre as condições do mesmo. O utilizador deve estar informado sobre que tipo de processamento vai ser realizado sobre os seus dados, quem irá poder aceder aos seus dados e qual o propósito para recolha e tratamento dos mesmos. Além disso, deverá ser capaz de exercer o seu direito ao esquecimento pedindo para que os dados sejam apagados do sistema. O RGPD inclui também a classificação dos dados como pessoais ou não pessoais, sendo que dentro da categoria de dados pessoais alguns são considerados como dados pessoais sensíveis. Desta forma, para o processamento de dados por algoritmos inteligentes é fundamental que os dados pessoais sejam tratados com garantias de privacidade face aos dados não pessoais, assim como, os dados pessoais sensíveis devem ser tratados com mais cuidado face aos dados pessoais.

Assim, uma primeira recomendação para qualquer sistema, e em especial para um sistema de AI, passa pelo cumprimento estrito do RGPD e dos conceitos gerais preconizados pelo mesmo, desde a fase inicial de desenvolvimento do sistema (em contexto de salvaguarda da privacidade do utilizador). Além disso, um sistema de AI deverá primeiramente certificar-se de que antes de qualquer processamento de dados ser efetuado deve ser dado o consentimento para tal, bem como garantir que o regulamento é cumprido.

Uma das componentes tecnológicas que carecem de regulamentação transversal são os desafios colocados pelas novas tecnologias, cada vez mais integradas. Estando a AI a tomar uma posição predominante nos nossos dias,

em diversos ambientes e tendo cada vez mais recursos como o caso de plataformas de *IoT* e dispositivos inteligentes para recolher mais dados, **torna-se essencial a regulamentação deste tipo de serviços** para que possam ser atribuídas responsabilidades em caso de violação da privacidade e da segurança do sujeito de dados não limitando o desenvolvimento e aplicabilidade da AI. Aspetos de processamento e armazenamento de dados, bem como a transparência de todos os processos e a capacidade de toda a cadeia de informação poder ser auditada, carecem de uma reflexão profunda, requerendo especialistas legais e informáticos para estabelecer bases bem fundamentadas, que promovam o uso das tecnologias, protegendo a sociedade em geral e os direitos dos cidadãos em particular. Há uma questão adicional sobre a exploração dos dados para treino, que carece de reflexão separada.

Em termos de defesa das organizações, recomenda-se que **haja uma alteração nas estratégias usadas para prevenir ataques**, explorando as oportunidades fornecidas pela AI, como descritas atrás. A abordagem de defesa atual é um modelo de organização seguro a partir do exterior, ou seja, como uma barreira de forma a impedir que a organização seja comprometida. Uma melhor abordagem será considerar que os atacantes vão encontrar lacunas (sejam atacantes internos, ou produtos comprometidos dentro da organização), e é necessário que as organizações estejam preparadas para a defesa nesses casos, pelo que se torna necessário adicionar uma camada de monitorização. Desta forma, serão três as camadas principais: deteção, proteção e resposta. Toda a parte de monitorização pode ser feita com recurso a algoritmos de AI facilitando o processo e melhorando a capacidade de resposta e rapidez. Novos modelos podem passar por um sistema inteligente que, para além de monitorizar, possa até responder de forma autónoma e resolver o problema ao qual a organização foi exposta, podendo evitar um comprometimento dos dados.

O aparecimento de sistemas baseados em AI torna importante uma abordagem diferente em termos de segurança das organizações, dado os perigos de cibersegurança (e a opacidade) inerentes à tecnologia. Torna-se essencial **estabelecer uma abordagem baseada no risco** uma vez que diferentes sistemas de AI apresentam diferentes níveis de risco para o utilizador final e para as organizações. Em abril de 2021 foram propostas novas regras e ações (denominado "Novas regras para a inteligência artificial") [119] para promoção da AI, respondendo à crescente presença ativa da AI na sociedade. Como tal, é necessário que haja uma legislação aplicável de forma a garantir fiabilidade. Estas propostas visam primeiramente definir o risco que determinado sistema apresenta e dessa forma poder estabelecer uma proteção eficaz:

- Tornam claro que sistemas que representam uma clara ameaça à segurança e aos direitos das pessoas não deverão poder existir na nossa sociedade. Um caso específico deste tipo de ameaças refere-se a sistemas de AI acessíveis por crianças, grupo desde logo mais vulnerável. Existem brinquedos, por exemplo, que através de assistência de voz podem manipular o comportamento das crianças, podendo levar a situações de alto risco. Devem ainda ser considerados os sistemas de risco elevado quando a AI é usada de forma indevida e possa pôr a vida e saúde dos cidadãos em causa, restringir o acesso à educação ou acesso a trabalho, a serviços públicos e privados essenciais, na gestão da migração, asilo

ou controlo de fronteiras, a interferir na administração da justiça e processos democráticos. Além disso, devem também ser considerados os componentes de segurança de produtos como a utilização de AI em cirurgia assistida por robots como se considera possível com o 5G. Assim, esta utilização de sistemas que podem comprometer o acesso a direitos, beneficiar/prejudicar os cidadãos devido à automatização de tarefas ou até mesmo colocar a saúde ou a vida dos cidadãos em perigo, devem ser estritamente avaliados através de sistemas adequados de validação; deve haver um registo de toda a atividade de forma a ser possível recuar no tempo e aceder a todo o histórico de informação podendo em alguns casos atribuir-se uma responsabilidade civil; deve haver um total conhecimento sobre o funcionamento do sistema de AI por todas as entidades envolvidas e elevado nível de transparência devendo a informação ser clara e adequada para o utilizador; deverá ser possível que o sistema seja auditado por um humano para minimizar os riscos; e deve existir um elevado nível de solidez, segurança e exatidão.

- Em sistemas de risco limitado deve ser garantido um elevado nível de transparência para que os utilizadores tenham a perceção de que estão a lidar com um sistema inteligente e possam decidir se pretendem continuar a interação ou não. Este caso pode ocorrer, por exemplo, com robots de conversação.

- Por fim, alguns sistemas de AI podem ser considerados sistemas de risco mínimo, ou seja, sistemas que não interferem com a segurança e privacidade dos utilizadores. Possíveis exemplos de sistemas de risco mínimo são os algoritmos inteligentes usados em jogos ou em deteção de SPAM.

No entanto, o **problema dos dados e do treino** não tem recebido suficiente atenção. Os algoritmos de AI e os modelos de ML dependem de dados: sem uma base de dados para treino de alta qualidade, mesmo os algoritmos mais eficientes serão inúteis. Estes dados — conhecidos como dados de treino — referem-se aos dados iniciais usados para desenvolver um modelo de ML, a partir do qual o modelo cria e melhora as suas regras. O resultado de modelos robustos de ML pode ser bastante prejudicado quando os dados de treino são inadequados, imprecisos ou irrelevantes na fase de treino. A qualidade desses dados tem implicações profundas para o desenvolvimento subsequente do modelo, estabelecendo um precedente para todas as aplicações futuras que usam os mesmos dados de treino. Desta forma, as fases de aquisição, identificação e preparação dos dados são cruciais para uma boa classificação. Os dados rotulados são anotados para mostrar o resultado que o modelo deve prever. O processo de rotulagem de dados envolve a marcação de um conjunto de dados para ajudar a treinar o algoritmo. A precisão do algoritmo depende da forma como os dados são rotulados e do peso atribuído a cada rótulo [120].

Atendendo a que os dados não são todos iguais, devem ser aplicados mecanismos de segurança que permitam garantir alguma proteção para que não ocorra uma violação de privacidade ou que os dados fiquem comprometidos. Em parte, isto relaciona-se também com a forma como os dados são armazenados — antes e após o processamento. Técnicas de controlo de acesso permitem também gerir quem tem permissões para aceder aos dados e quando. Além disso, facilitam a identificação de quem acedeu aos dados e quando através dos *logs* dos serviços. Algumas abordagens passam pela anonimização dos dados antes do seu processamento para evitar que os mesmos possam identificar um sujeito específico, contudo, pode ocorrer a perda de características úteis para um bom resultado do treino com os dados anonimizados. Estudos científicos recentes comprovam que têm vindo a ser investigadas técnicas [121][122][123] que permitem anonimizar dados com preservação da privacidade dos utilizadores, mantendo uma boa qualidade dos dados para processamento, com resultados favoráveis na fase de classificação ou decisão. Contudo, o impacto computacional deste tipo de abordagens passa, neste caso, a ser uma possível preocupação.

5G e tecnologias subsequentes

O 5G representa a mais recente geração das redes móveis, melhorando a capacidade das mesmas em oferecer novos serviços. Ao contrário das tecnologias anteriores, muito centradas nos serviços ao consumidor, o 5G foi desenvolvido de forma a facilitar o desenvolvimento de serviços a empresas e à sociedade em geral.

A tecnologia expande a filosofia das gerações anteriores, fornecendo um amplo leque de evoluções ao nível da tecnologia rádio, como forma de fornecer melhor desempenho. Em concreto pode salientar-se: i) o uso generalizado de "Multiple Input Multiple Output" (MIMO), que visa melhorar a eficiência espectral através do uso de um grande número de antenas, e oferecendo a sua variante "Multiple User" (MU-MIMO) em que as estações base conseguem comunicar em múltiplos fluxos de dados com múltiplos terminais móveis na mesma frequência; ii) o "beamforming", que permite reduzir a interferência, capitalizando a existência do MIMO, para emitir o mesmo sinal utilizando múltiplas antenas, usando reflexão e difusão do sinal, concentrando a sua transmissão até ao receptor; iii) o futuro uso de ondas milimétricas, que permitem capitalizar de uma parte do espectro entre os 24 GHz e os 100 GHz, particularmente no uso das bandas 26GHz (Europa e China) e 28 GHz (EUA, Japão e Coreia do Sul) para atingir velocidades com desempenho superiores a 1 Gbps; iv) a partilha dinâmica de espectro que permite ao 5G ser disponibilizado em simultâneo com o 4G e coexistirem numa única portadora e v) a capacidade de gestão de redes heterogéneas compondo células móveis macro, micro, sistemas de antenas distribuídas e "hotspots" Wi-Fi quando disponíveis.

No entanto, sendo uma tecnologia já na era da nuvem, o 5G também se distingue das gerações anteriores pela incorporação de mecanismos e estratégias comumente usados em ambientes de centros de dados. O 5G recorre a virtualização da rede e dos sistemas, o que permite desacoplar o hardware e o *software* da rede. Numa arquitetura de redes virtualizadas, uma rede corre sob forma virtual em cima da infraestrutura física da rede. Tal resulta num sistema mais dinâmico e facilmente configurável, permitindo às diferentes funções de rede correrem em servidores computacionais em vez de hardware dedicado. Esta capacidade permite dividir os recursos de hardware em funções, compondo um sistema denominado por Funções de Rede Virtualizadas (*Network Function Virtualization*). Adicionalmente, são aplicados também mecanismos de redes definidas por software, onde o plano de controlo e o de dados são estruturalmente separados, interligados por uma vista centralizada da rede.

A conjugação destas evoluções ao nível da rede de acesso e da virtualização de funções de rede permitem ao 5G implementar novas capacidades, com vista à sua aplicação num leque de novos cenários, e suportar diferentes cenários de uma forma estruturalmente isolada. Em concreto, o *slicing* da rede permitirá dividir e isolar os recursos da mesma em função dos casos de uso que decorrem em simultâneo sobre a mesma. Tal permite ao mesmo hardware servir diferentes casos de uso com necessidades específicas de funcionamento da rede. Assim, torna-se possível fornecer, em simultâneo, serviços com muito baixa latência e muito alta largura de banda para diferentes cenários. Esta plasticidade da tecnologia levou ao desenvolvimento de terminologia específica para identificar diferentes classes de serviços:

- eMBB (*enhanced Mobile Broadband*), serviços fundamentalmente associados a grandes larguras de banda (e.g. vídeo streaming de UHD)
- URLLC (*Ultra Reliable Low Latency Communications*), serviços associados a grandes requisitos de fiabilidade e baixa latência (e.g. controlo remoto de um robot)
- mMTC (*massive Machine Type Communications*), serviços associados a grandes redes de sensores (e.g. medidores de energia eléctrica)

A Figura 9 representa esquematicamente estas grandes linhas de serviços, e ilustra como diferentes tipos de serviços apresentam requisitos que podem conjugar diferentes aspetos destas três grandes linhas.

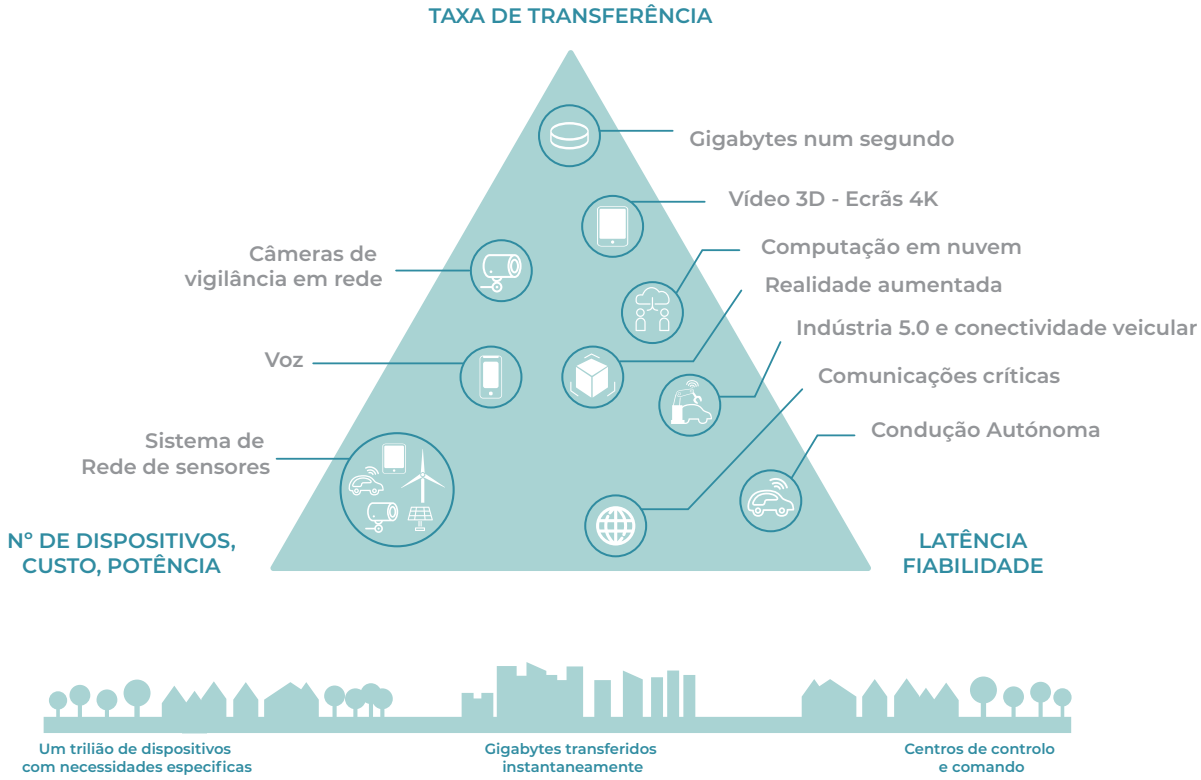


Figura 9 – Serviços potencialmente oferecidos em redes 5G

Adicionalmente, esta conjugação de vertentes tecnológicas permite também a integração de modelos de desenvolvimento distintos, por exemplo com tecnologias mais abertas, tais como o Open RAN [124], que permite aos operadores combinarem componentes de diferentes fabricantes em todo o subsistema de rádio e de acesso à rede. Fica assim possibilitado um maior nível de inovação e opções para o operador, podendo também contribuir para a implantação das redes 5G de forma mais célere, à custa de menor eficiência operacional. Contribui ainda para que qualquer solução 5G possua um maior grau de independência de um fornecedor especifico.

BREVE RESENHA HISTÓRICA

O 5G prossegue a evolução tecnológica das redes móveis, que começou com a primeira geração nos anos 1980. De uma forma geral, e em função de compromissos técnicos e sustentabilidade económica, observa-se o lançamento de uma nova geração a cada 10 anos, tal como definidas pelas normas do 3GPP (3rd Generation Partnership Project, a associação mundial responsável pela uniformização das comunicações móveis) associadas às inerentes inovações e melhorias tecnológicas. A primeira geração (1G) permitiu o estabelecimento de chamadas de voz móveis analógicas, sendo que a segunda geração (2G) trouxe a digitalização da voz e permitiu o uso de mensagens de texto. Nesta segunda geração começou a transição para os serviços digitais, com o desenvolvimento do 2.5G, a tecnologia GPRS. A terceira geração (3G) permitiu aos utilizadores utilizarem de base serviços digitais on-line com velocidades (inicialmente) até aos 384 Kbps. A quarta geração (4G) foi lançada na primeira década do século XXI, onde as suas velocidades de receção de dados estavam tipicamente situadas entre os 10 e os 20 Mbps, mas evoluindo gradualmente até 100Mbps.

A quinta geração (5G) iniciou o seu trabalho normativo no início da década passada, com as primeiras especificações a serem publicadas entre 2017 e 2018 [125]. Tal como as gerações anteriores, **o 5G tem um processo evolutivo em que vai incorporando novas características, e que neste caso se irá estender até meados desta década**. No fim de 2019, a denominada Release 16 foi lançada [126], focando as necessidades das indústrias verticais (os ecossistemas associados a sectores económicos específicos), tais como o setor automóvel, a Internet das Coisas Industrial, e a operação em espetro não licenciado. Em março de 2022 foi terminada a Release 17 [127], que se tem focado na operação dos casos de uso diversificados, mas fundamentalmente associados a URLLC (serviços de resposta crítica) e mMTC (*IoT* generalizada), suportando o crescimento esperado no tráfego de dados móveis, bem como a customização do fornecimento de serviço aos setores automóvel, logística, proteção civil, media e manufatura. A *Tabela 3 – Evolução da tecnologia 5G ao longo dos anos* sumaria as principais características das diferentes versões do 5G.

De notar que as tecnologias associadas ao 5G não pararam a sua evolução, e novas versões estão planeadas para os próximos anos. Resulta desta tabela que as capacidades da rede serão diferentes dependendo da versão que estiver a ser instalada - e há sempre um atraso de pelo menos dois anos entre a normalização de uma versão e a sua instalação. Em diferentes alturas dos próximos anos, diferentes setores de atividades terão de se adaptar a diferentes

(e melhores) caraterísticas da rede de comunicações (dependendo até do operador subscrito!), criando novos perigos de cibersegurança, em ambientes muito mais dinâmicos e imprevisíveis.

Embora o 5G almeje velocidades de comunicação de dados na ordem dos 10 Gigabits, em 2021 as velocidades médias efetivas estão a ser medidas no utilizador final com valores entre 400 a 600 Mbps. Estas velocidades significam que o 5G pode ser já um concorrente aos serviços de banda larga doméstica, oferecendo uma versão bastante melhorada dos Acessos Fixos Sem-fios disponíveis com o 4G. Adicionalmente, as redes 5G apresentam melhor desempenho em termos de latência, representando esta o tempo que demora a transmitir cada pacote de dados. Concretamente, no 4G a latência variava habitualmente entre os 60 e os 100ms, mas o 5G tem como objetivo fornecer valores na gama dos poucos milissegundos. Este aspeto permite a implantação de casos de uso onde respostas próximas do instantâneo são necessárias, tais como o controlo remoto de maquinaria industrial ou "*massive gaming online*". O 5G também permite uma forma melhorada de fornecer serviços de conectividade a um vasto número de dispositivos na mesma localização, permitindo a implantação plena da Internet das Coisas.

Tabela 6 - Evolução da tecnologia 5G ao longo dos anos

R#	Taxa máx. (UL)	Taxa máx. (DL)	Latência	Características	Cenários	Referência
15 (2018)	10Gbps	20Gbps	4ms	Foca essencialmente o eMBB · 6GHz · *Network Slicing* · Beamforming · Service Based Architecture · Exposição de APIs	Realidade Virtual *Smart Cities*	3GPP TR 38.913 3GPP TR 21.915
16 (2019)	10Gbps	20Gbps	0.5ms	Foca essencialmente o URLLC · 24.25—52.6 GHz · Transmissão redundante para comunicações com alta fiabilidade · Monitoria de QoS · Delay Budget dinâmico · Melhorias ao nível da continuidade de sessão · Suporte de NR *IIoT* · 5G V2X com NR sidelink · Service Enabler Architecture Layer para as Verticais · Precisão de posicionamento abaixo de 1 metro · Network Slice-Specific Authentication and Authorization (NSSAA)	Realidade aumentada e-Health *IIoT* Internet Táctil Controlo robot remoto	3GPP TR 21.916
17 (2022)	10Gbps	20Gbps	0.5ms	· Até 71 GHz · Localização até ao nível do centímetro · Introdução de gestão de computação no edge (ECM) · Suporte de redes não terrestres (NTN) · *Broadcast and unicast* · Melhoria do feedback da para latências mais baixas · Suporte de dispositivos com capacidades reduzidas (*enhanced* MTC) · Ponto de transmissões e recepções múltiplas (mTRP) · *Backhaul* de acesso móvel integrado (IAB)	Rastreamento de ativos Serviços de broadcast 5G Cirurgia remota Automação fabril	3GPP TR 21.917

Devido ao interesse e oportunidades comerciais associadas, houve uma pressão para a implementação rápida de serviços 5G. Existiram muitas iniciativas nacionais que foram politicamente aceleradas, quer nos EUA [128] e na Coreia do Sul [129] seguidos da China [131], expondo a oferta de serviço de forma condicionada e em algumas cidades. No espaço Europeu, os esforços de implantação da rede estiveram centrados no âmbito do "5G Action Plan" [132], iniciativa que foi criada em 2016 com o objetivo de fomentar a implantação do 5G na Europa. Esta encadeou esforços de forma propriamente dita em 2019, com muitos países Europeus nessa altura a oferecer serviços limitados em algumas cidades [133]. Este desenvolvimento avançou durante 2020, tendo até ao fim desse ano sido lançados serviços 5G em quase todos os países da UE, tendo recentemente Portugal ingressado nesse grupo.

FUTURO A 5 E 10 ANOS

O 5G já tem um fim previsto, no tocante a esta primeira fase de inovação. Concretamente, as especificações da Release 17 estão essencialmente concluídas, terminando brevemente a implementação das interfaces programáticas associadas. Com a próxima Release 18, dar-se-á início a uma evolução do 5G, sendo nessa Release dado início à normalização do que será chamado 5.5G, ou 5G-Advanced. Neste momento, encontram-se a ser concluídos os pontos de estudo e de trabalho do 3GPP, dando início ao longo de 2022 ao primeiro estágio do processo de normalização. O segundo estágio, que descreve a organização das funções de rede necessárias para esta nova instância da tecnologia, será concluído em março de 2023, sendo este seguido dos trabalhos de definição da sinalização necessária, previsivelmente em dezembro desse mesmo ano. Os processos de implementação das interfaces programáticas serão finalizados em março de 2024. Este é o trajeto inicial que se cruza também com a preparação para o 6G. De uma forma mais genérica, o denominado 6G será analisado primeiramente sob o ponto de vista de tendências tecnológicas, culminando com a fomentação da visão e indicadores de desempenho para a nova geração, a começar formalmente em junho de 2022. No ano seguinte, ocorrerá a 23ª Conferência Mundial de Comunicações Rádio da ITU (WRC-23), que definirá também a discussão sobre o espectro a ser utilizado pelo 6G, e terá as discussões finais sobre a alocação do mesmo em 2027, a WRC-27. Será antes desta altura, nomeadamente no fim de 2025 ou início de 2026, que o 3GPP iniciará os trabalhos de estudo do 6G (nomeadamente os seus requisitos, e artigos de estudo e trabalho), com a primeira especificação prevista vir a estar finalizada antes de 2030. Assim, resulta que **o 5G é uma tecnologia que tem objetivos temporais muito bem definidos**.

Para preparação do 6G, decorrem estudos importantes, resultantes da análise do uso de tecnologias potencialmente candidatas à concretização de novos casos de uso. Em concreto, seguindo a tendência de evolução da largura de banda operável em cada geração de redes móveis (i.e., 200 KHz no 2G, os 5 MHz no 3G, os 20 MHz no 4G e até aos 100MHz no 5G), o 6G pretende ser o palco para a exploração do uso das bandas THz (que poderão ir além dos 100Mhz de largura de banda), sendo um potencial fornecedor de soluções para requisitos de larguras de banda entre os 500MHz e os 1GHz. Neste sentido, decorrem estudos desencadeados pelo ITU, sobre a viabilidade do uso de

frequências acima dos 100GHz, cujo relatório está previsto para meados de 2023. Esta vertente permite ir além dos conceitos de "Coisas Interligadas" que fomentam os casos de uso associados a URLLC e mMTC, passando a oferecer a largura de banda e latência necessárias para uma verdadeira experiência de "Inteligência Interligada", onde a AI e a sensorização são combinadas para o fornecimento de serviços de reconhecimento, proteção, observação e posicionamento em tempo real, e com alta precisão, até agora impossíveis. Com estas possibilidades tecnológicas, vislumbra-se a possibilidade de ir mais além nos grandes cenários cujo trilho foi talhado pelo 5G (eMBB, URLLC e mMTC), não só melhorando os mesmos (eMBB+, URLLC+ e mMTC+), mas também criando novas vertentes (i.e., Sensorial e AI), que ainda estão a ser discutidos [130], mas que podem ser ilustrados como:

- **eMBB+** - Realidade virtual imersiva através da *cloud*; comunicações hápticas e multi-sensoriais; mostradores holográficos e sem-ecrã; acesso sem-fios de banda larga para os infoexcluídos;
- **URLLC+** - As fábricas do futuro; Controlo de movimento ciber-físico em tempo real; Robots colaborativos em grupo; Ciborgues (inteligência independente);
- **mMTC+** - Transportes inteligentes e veículos autónomos; edifícios inteligentes; prestação de cuidados de saúde inteligente; serviços inteligentes fornecidos por veículos aéreos não-pilotados; serviços *IoT* em áreas telco-excluídas;
- **Sensorial** - Localização e monitorização de alta precisão; captura de imagem, mapeamento e localização simultâneas; sensorisação humana; reconhecimento gestual e de atividades; navegação e posicionamento de alta precisão; proteção e observação da terra em tempo real
- **AI** - Automação da rede suportada por AI; redes para transferência de dados ou modelos de AI; redes para aprendizagem distribuída.

Genericamente, podemos concluir que os desafios e oportunidades postos pelas tecnologias 5G irão sendo crescentes e a sociedade terá de estar preparada para ir respondendo a todas estas potenciais mudanças durante os próximos anos. **Não será possível adotarmos uma estratégia passiva pelo facto de "estarmos sempre a falar de redes 5G**": as redes irão melhorando, evoluindo na direção de redes 6G ao longo dos anos.

DESAFIOS DE CIBERSEGURANÇA

Com a expectável crescente dependência que os sistemas e infraestruturas críticas irão ter das redes móveis de 5ª geração, verifica-se que a integridade e disponibilidade das mesmas irão tornar-se alvo de grandes preocupações de segurança nacional, assim como um dos principais desafios de segurança sob a perspetiva da União Europeia. As infraestruturas de telecomunicações são sistemas físicos, cibernéticos e organizacionais complexos.

Tipicamente, os operadores de telecomunicações centram a sua atenção em aspetos de resiliência e segurança, utilizando ferramentas consagradas e coordenando as suas defesas a partir de centros de operações altamente sofisticados. No entanto, estas infraestruturas estão continuamente sujeitas a uma variedade de ataques oriunda de um vasto espectro de ameaças, e verifica-se o contínuo crescimento de novos desafios com base nos avanços tecnológicos e da complexidade da arquitetura [135]. Aqui, no âmbito do 5G, são importantes as novas superfícies de ataque tornadas possíveis pela integração de novos mecanismos (tais como os mecanismos de virtualização exemplificados por ambientes de centros de dados), bem como a aplicação das telecomunicações 5G em cenários que anteriormente não eram considerados em redes móveis públicas. Concretamente, a abertura à pervasividade das plataformas programáveis na era do 5G acarreta uma nova frente de ataques cibernéticos. Do ponto de vista físico, estes problemas também aumentam com a maior complexidade da arquitetura no suporte da Internet das Coisas, do ponto de vista da monitorização e proteção eficientes das partes mais remotas da infraestrutura (i.e., armários, mastros, entre outros).

As infraestruturas críticas de comunicação são um alvo determinante para ataques (quer físicos, quer cibernéticos) uma vez que exibem um fator multiplicativo. Um bom exemplo são os ataques de "botnet" (tal como o que sucedeu em 2016 na Alemanha, focado na Deutsche Telekom) [136] que criou problemas de conectividade à Internet para quase um milhão de utilizadores, tendo-se distribuído por dispositivos móveis, routers, câmaras de vigilância e gravadores de vídeo digitais, ou o ataque à Vodafone Portugal [137], realizado a nível da infraestrutura central. Ao nível de ataques físicos verifica-se também como alvos os mastros das antenas das redes móveis, infraestrutura "backbone", bem como ativos da infraestrutura de acesso física. De facto, o movimento "anti-5G" gerou algumas dessas situações, incluindo em Portugal [138], que (erradamente) argumentava com malefícios de saúde associados a sistemas 5G.

Adicionalmente, segundo o relatório da UE sobre a avaliação coordenada de riscos em cibersegurança em redes de quinta geração lançado pela Comissão Europeia em outubro de 2019 [139], como parte do esforço de implementação da sua recomendação de março de 2019 com vista ao estabelecimento de um elevado nível de cibersegurança nessas redes pelo espaço Europeu, verifica-se também que o papel dos fornecedores de soluções 5G (quer ao nível do seu desenvolvimento e fabrico, quer ao nível da sua operação) é preponderante face ao grau de dependência sobre os operadores individuais (esta consideração é também sustentada de acordo com a "5G Toolbox" de conectividade que suporta os estados-membros com as melhores práticas de implantação do 5G, referenciada nos "Potenciais Indicadores da área", desta secção do documento). Concretamente, com o crescimento das funcionalidades associadas aos diferentes componentes de uma rede 5G, os operadores de telecomunicações tornam-se mais dependentes dos fabricantes e fornecedores, levando a um aumento do número de vias e severidade dos ataques que podem ser explorados, em sistemas cada vez mais complexos. Neste sentido, existe a noção de os ataques em 5G poderem ser inerentes aos próprios produtos desenvolvidos pelos fornecedores dos operadores, devido ao seu posicionamento na cadeia de valor de fornecimento de serviços de telecomunicações. Torna-se assim necessário endereçar de forma individual o perfil de risco de cada produto introduzido na infraestrutura, focando sobretudo a sua capacidade de ser sujeito a

interferências nefastas. Tais riscos acarretam situações como a potencial interrupção no fornecimento resultante de falha comercial, que toma especial relevo se houver grande dependência de fornecedores individuais.

Numa visão de rede 5G tradicional, um operador de telecomunicações mantém a sua estrutura de operações baseada num pequeno conjunto de fornecedores de soluções de hardware e software, apoiadas por um também reduzido número de integradores de sistema e operadores. Neste contexto, podemos sumariar as considerações sobre a cibersegurança nas novas redes 5G na tabela seguinte.

Tabela 7 - Considerações sobre cibersegurança em redes 5G de operadores tradicionais

Tema	Consideração
Ameaças	Associado ao aumento dos ataques às cadeias de valor associadas à implantação globalizada das redes 5G, será de esperar um maior impacto de falhas nas mesmas. A maior dependência de sistemas críticos (i.e., societais e económicos) em redes 5G poderá piorar as consequências das perturbações criadas;
Ativos	No contexto de redes de telecomunicações, o 5G partilha da criticidade das funções da rede "core", rede de acesso, sistemas de gestão, funções de transporte/transmissão e trocas inter-redes*, nomeadamente: • **das funções da rede "core"** · Categoria: Software, hardware, dispositivos de rede · Funções: diversas, assegurando o controlo e operação da rede · Localização: infraestrutura da rede · Criticidade: imprescindível · Dependências: rede de acesso, sistemas de gestão, funções de transporte/transmissão • **rede de acesso,** · Categoria: Software, hardware, dispositivos de rede · Funções: diversas, assegurando a transmissão de dados entre a rede e os dispositivos móveis dos utilizadores · Localização: orla da infraestrutura da rede · Criticidade: imprescindível · Dependências: rede core, sistemas de gestão, funções de transporte/transmissão · **sistemas de gestão,** · Categoria: Software, hardware, dispositivos de rede · Funções: diversas, assegurando a correta operação da rede, sua monitorização e controlo · Localização: infraestrutura da rede · Criticidade: imprescindível · Dependências: rede core, rede de acesso, funções de transporte/transmissão • **funções de transporte/transmissão e trocas inter-redes** · Categoria: Software, hardware · Funções: permitir e assegurar a transmissão de dados na infraestrutura e entre esta e elementos externos · Localização: infraestrutura da rede · Criticidade: imprescindível · Dependências: rede core, rede de acesso a sistemas de gestão, funções de transporte/transmissão No entanto, as características (e possibilidades) tecnológicas do 5G levam a que surjam elementos de sensibilidade crítica no tocante à gestão e orquestração de funções de redes virtualizadas ("*Management and Orchestration*", ou MANO). Apesar destes sistemas não transportarem tráfego efetivo, controlam elementos importantes da rede e podem assim ser utilizados para conduzir atos maliciosos, tais como sabotagem ou espionagem. Assim podemos considerar para estes elementos: · Categoria: Software, hardware · Funções: gestão e orquestração de serviços de rede, compostos pelo encadeamento de máquinas virtuais ou containers, com o propósito de instanciar uma funcionalidade na rede · Localização: infraestrutura da rede · Criticidade: atualmente grande, mas imprescindível a curto prazo · Dependências: infraestrutura de virtualização, sistemas de gestão

* E como tal, devendo refletir preocupações identificadas no https://www.cncs.gov.pt/docs/cncs-quadrodeavaliacao.pdf.

Tema	Consideração
Vulnerabilidades	Geralmente, as redes 5G podem ser associadas a vulnerabilidades que podem afetar *software*, *hardware* ou surgir de deficiências existentes em processos de segurança. Adicionalmente, na fase inicial de implantação, as vulnerabilidades associadas ao 3G e ao 4G continuam a ser alvo de consideração. Novos tipos de vulnerabilidades técnicas associadas a tecnologias 5G específicas são passíveis de surgir (e.g., as tecnologias SDN, NFV e incluindo os sistemas *cloud*). Verifi-cam-se também várias funções a transitarem de *hardware* para *software* (i.e., interceção legal de dados) que, se não forem devidamente geridas, podem ser utilizadas para levar a cabo ações maliciosas. Um exemplo, com especial relevo associado a uma utilização mais massiva por parte dos já mencionados ambientes verticais advém da possibilidade de passagem de dados entre diferentes ambientes virtualizados, uma vez que o isolamento de "*slices*" (isolamento completo de diferentes serviços sobre a mesma infraestrutura) é um problema identificado pela indústria e em amplo desenvolvimento tecnológico ainda. As redes 5G irão ser compostas por uma grande quantidade de dispositivos virtualizados, que podem ser acedidos remotamente através da rede, tornando-se uma vulnerabilidade com a capacidade de se tornar mais acutilante em casos em que a manutenção das redes é realizada por terceiros. Em concreto, o crescente papel do *software* e dos ser-viços fornecidos por terceiros em redes 5G levam a uma maior exposição face a múltiplas vulnerabilidades que podem derivar do perfil de risco dos fornecedores.
Cenários de risco	ID.AR-1 - Má configuração de redes, falta de controlos de acesso Ameaça - Com a introdução das redes 5G, soluções técnicas complexas irão requerer suporte adicional de diferentes tipos de fornecedores, a quem deverá ser concedido acesso remoto ou até mesmo on-site. Tal possibilita manipular certas funcionalidades, ou intercetar e encaminhar tráfego de dados, ultrapassando mecanismos de auditoria de uma forma não detetável pelo operador. Vulnerabilidade - Sim Confidencialidade - Sim Integridade - Sim Disponibilidade - Sim Impacto - 4 - Catastrófico Probabilidade - 3 - Muito Provável Nível do Risco - 12 - Alto Estratégia - Proteger e Detetar Ações (referenciadas dos níveis de capacidade do Quadro de Avaliação de Capacidades de Cibersegurança) - PR.SD-1, PR.SD-2, PR.SD-3, PR.SD-4, PR.SD-5, PR.SD-6, PR.SD-7, PR.SD-8, DE.MC-6, DE.MC-7
	ID.AR-2 - Qualidade dos produtos e dependências Ameaça - A maior complexidade dos sistemas das redes 5G aumenta o risco da existência de defeitos significativos no equipamento fornecido, bem como nos processos de suporte. A consequente dependência em terceiros, sobretudo nos casos em que há o foco em apenas um fornecedor ou quando existe um fornecedor dominante, expõe múltiplas vulnerabilidades. Vulnerabilidade - Sim Confidencialidade - Sim Integridade - Sim Disponibilidade - Sim Impacto - 4 - Catastrófico Probabilidade - 2 - Provável Nível do Risco - 8 - Alto Estratégia - Detetar Ações (referenciadas dos níveis de capacidade do Quadro de Avaliação de Capacidades de Cibersegurança) - DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.MC-1, DE.MC-2, DE.MC-4, DE.MC-8, DE.PD-1, DE.PD-2, DE.PD-4, DE.PD-5

Tema	Consideração
Cenários de risco	ID.AR-3 - Interferência estatal ou exploração criminal das redes 5G Ameaça - Pode ser colocada pressão sobre um fornecedor sob sua jurisdição, para que seja providenciado acesso a ativos de rede sensíveis. Igualmente, atividade criminal pode fazer refém dados associados a serviços comprometidos. Vulnerabilidade - Sim Confidencialidade - Sim Integridade - Sim Disponibilidade - Sim Impacto - 4 - Catastrófico Probabilidade - 2 - Provável Nível do Risco - 8 - Alto Estratégia - Monitorização contínua da segurança e mitigar Ações (referenciadas dos níveis de capacidade do Quadro de Avaliação de Capacidades de Cibersegurança) - DE.MC-1, DE.MC-2, DE.MC-3, DE.MC-4, DE.MC-5, DE.MC-6, DE.MC-7, DE.MC-8, RS.MI-1, RS.MI-2, RS.MI-3.
	ID.AR-4 - Disrupção de infraestrutura ou serviços críticos e falha massiva de redes devido a falha de fornecimento elétrico ou outros sistemas de suporte Ameaça - Motivados pela ação de hackers ou catástrofes naturais. Vulnerabilidade - Sim Confidencialidade - Sim Integridade - Sim Disponibilidade - Sim Impacto - 4 - Catastrófico Probabilidade - 2 - Provável Nível do Risco - 8 - Alto Estratégia - Detetar, mitigar e recuperar Ações (referenciadas dos níveis de capacidade do Quadro de Avaliação de Capacidades de Cibersegurança) - DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.MI-1, RS.MI-2, RS.MI-3, RC.PR-1.
	ID.AR-5 - Exploração *IoT* Ameaça - Ataques tomam controlo de dispositivos *IoT* de baixa segurança (i.e., sensores) de forma a atacar a rede Vulnerabilidade - Sim Confidencialidade - Sim Integridade - Sim Disponibilidade - Sim Impacto - 3 - Elevado Probabilidade - 3 - Muito Provável Nível do Risco - 9 - Alto Estratégia - Proteger, Detetar e Mitigar Ações (referenciadas dos níveis de capacidade do Quadro de Avaliação de Capacidades de Cibersegurança) - PR.SD-1, PR.SD-2, PR.SD-3, PR.SD-4, PR.SD-5, PR.SD-6, PR.SD-7, PR.SD-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.MC-1, DE.MC-2, DE.MC-4, DE.MC-8,RS.MI-1, RS.MI-2, RS.MI-3.

Há, no entanto, também que ter em conta aspetos de situações específicas sobre vulnerabilidades acrescidas, resultantes da integração de outras tecnologias no seio do funcionamento das redes 5G. O conceito das redes Open RAN permite aos operadores de telecomunicações utilizar soluções de hardware e *software* de diferentes fabricantes, ao invés de obrigar à adoção de um sistema completamente integrado, que foi desenvolvido por um único (ou poucos) fabricante(s). Para tal, é fundamental que as interfaces (normalizadas) entre os diferentes componentes da rede sejam implantadas de acordo com as normas estabelecidas pelo 3GPP. Adicionalmente, as soluções Open RAN suportam-se de mecanismos de "*cloud*ificação", "*softwarização*" e virtualização para conseguirem virtualizar funções da rede de acesso, desagregando o *software* do hardware (daí a origem do termo "open"), passando assim a poder operar em hardware genérico. Por fim, o conceito das redes Open RAN assenta também na utilização de mecanismos de automação da rede, onde controladores inteligentes permitem realizar processos de orquestração e gestão das funções, abrindo o caminho para a introdução de funcionalidades de inteligência artificial e aprendizagem automática. Consequentemente, as superfícies de ataque associadas a este conceito podem introduzir ainda um outro conjunto de riscos adicionais [133], nomeadamente:

- Pontos de entrada adicionais resultantes da interligação de componentes de rede pertencentes a diferentes fabricantes;
- Além da superfície de ataque maior, também aumenta a complexidade de configuração e gestão do sistema, levando a um maior número de riscos de vulnerabilidade, de falhas e de problemas de configuração da rede;
- Atualmente, as especificações para o conceito Open RAN (perseguidas pela "O-RAN Alliance") são ainda imaturas no tocante à segurança como requisito fundamental da arquitetura das mesmas;
- A dependência de mecanismos de *cloud* introduzida pelo Open RAN representa um potencial ponto de sujeição a terceiros, que obriga a definir critérios e mecanismos de segurança e proteção de dados, oriundos da partilha de recursos de computação onde estão alojadas as funções de rede virtualizadas.

OPORTUNIDADES

As infraestruturas e serviços de telecomunicações detêm um papel fulcral (e crescente) na economia digital. Concretamente, no continente europeu, as tecnologias e serviços móveis representaram 3,3% do produto interno bruto regional em 2017, sendo expectável que esse valor ultrapasse os 4% em 2022. Adicionalmente, a região representa a maior taxa de penetração móvel mundial, com 85% registados em 2017, e com um potencial de crescimento para 88% até 2025 [139]. O 5G será então um alicerce nesta nova era de conectividade inteligente, contribuindo para acelerar a transformação industrial e dar novo fôlego à digital. É também reconhecido que o 5G irá permitir criar novas áreas de negócio, permitindo às redes móveis fomentar o crescimento de produtividade nas indústrias tradicionais. A título de exemplo, o plano de ação 5G

da União Europeia evidencia a necessidade de cobertura ininterrupta de 5G nas principais estradas e ferrovias até 2025 [133].

Além da melhoria do desempenho da rede como observado nas anteriores gerações, com o 5G irão também emergir outras tecnologias complementares. A computação na fronteira da rede (ou "edge") irá permitir transferência de dados e segurança de perímetro mais eficientes, auxiliando os operadores de telecomunicações na redução do congestionamento da rede e na redução da latência. A virtualização de funções de rede irá suportar uma gestão mais dinâmica dos recursos de rede, auxiliando nos custos de operação (OPEX) e de investimentos (CAPEX). Adicionalmente, novos paradigmas de operação da rede e criação de serviços poderão surgir, capitalizando da análise de dados, inteligência artificial e aprendizagem automática. Com este suporte adicional, é conferido aos operadores de telecomunicações um papel mais assertivo na cadeia de valores industrial, fomentando relações mais próximas com os seus clientes, com vista a desenvolver novas experiências e monetização de serviços [143].

Na Europa o 5G foi universalmente identificado como uma oportunidade de fomentar a criação da economia e sociedade digitais para a próxima década, tomando medidas significativas para tornar a Europa num líder no desenvolvimento estratégico global tecnológico. O plano de ação 5G [132] tem como objetivo impulsionar a implantação de infraestrutura e serviços 5G, tendo iniciado em setembro de 2016. As seguintes medidas foram propostas pela Comissão Europeia:

- estabelecer uma ação coordenada de implantação do 5G entre os estados-membros, alinhando os seus roteiros e prioridades, assim como o aprovisionamento das bandas associadas e promoção nas principais áreas urbanas e vias de comunicação (aspetos que já ocorreram ou estão a decorrer);
- promover ensaios pan-Europeus envolvendo múltiplos atores, de forma a catalisar a transformação de inovação tecnológica em soluções de negócio completas;
- facilitar a implementação de programas de financiamento liderados pela indústria no suporte à inovação 5G;
- unificar atores líderes para a promoção de normas globais.

Na sequência da pandemia da Covid19 foram disponibilizados investimentos associados ao 5G (e comunicações em geral), tida como uma área de investimento chave nas medidas de recuperação e resiliência, com vista a uma recuperação digital e verde, incluindo ecossistemas *IoT*, o desenvolvimento de cidades inteligentes e investimento em inteligência artificial.

Neste contexto, existe uma expectativa da sociedade que o 5G suporte uma grande variedade de aplicações, incluindo [144]:

- Comunicações máquina-a-máquina em larga escala, tais como os sensores numa linha de produção fabril;
- Aplicações inovadoras em realidade aumentada e virtual;
- Veículos ligados e autónomos para utilização individual e corporativa, incluindo transportes e distribuição;
- Inovações em inteligência artificial e robótica;
- Ferramentas para cidades inteligentes e domótica;
- Aplicações no setor da saúde tais como monitorização de saúde e bem-estar, dispositivos de fornecimento de medicação e expansão da telemedicina;
- Transição acelerada para tecnologias de produção da Indústria 4.0;
- Aplicações na agricultura tais como uma aplicação mais focada de fertilizantes, pesticidas e nutrição, levando a uma redução dos custos e melhoria ambiental.

Adicionalmente, foram identificadas atividades económicas chave com a capacidade de liderar a integração das capacidades do 5G na melhoria dos seus processos [144][145][146], cruzando o mundo do *IoT* com as novas capacidades de comunicação e computação introduzidas pelo 5G. Destes ecossistemas podemos ilustrar as evoluções em cinco áreas, que de alguma forma espelham os pontos salientados na secção 5: a energia, a indústria, os transportes/mobilidade, a eletrónica de consumo, e a saúde.

Tabela 8 - Ilustração das oportunidades abertas pelo 5G noutras indústrias

Energia
• Os quatro principais cenários de aplicação do 5G na indústria da energia são os serviços de controlo (i.e., de carga e de proteção diferencial para a rede de distribuição), os serviços de coleção (i.e., monitoria automática do consumo energético), aplicações móveis (i.e., inspeção móvel) e novos serviços das grelhas energéticas (i.e., integração de multi-estações em cenários de *smart grids*); • As grelhas energéticas inteligentes poderão ajustar o fornecimento (e procura) energética à medida que aumenta a quantidade de máquinas e dispositivos ligados à rede; • A integração de mecanismos 5G no seio desta indústria implica oportunidades de cooperação entre as empresas de energia, fabricantes e operadores, em situações de normalização, propriedade intelectual, recursos (i.e., zonas e áreas) para implantação de base stations, planeamento e construção de infraestrutura, e na compreensão das exigências de energia dos consumidores.
Transportes/mobilidade
• Veículos ligados irão permitir a recolha de dados do ambiente em redor, tais como as luzes de trânsito, outros veículos e sensores nas vias, com vista à melhoria da eficiência e capacidade dos sistemas de transportes; • Consequentemente, torna-se possível melhorar a eficiência e economia dos transportes por estrada (incluindo fretes), através da circulação em pelotão; • Adicionalmente, reduz-se o trânsito, permitindo melhorias nos tempos de viagem, com impacto na fiabilidade dos serviços de transporte de mercadorias, bem como redução das emissões; • Criação de sistemas de gestão de frota e logística inteligentes, além de melhores serviços de correio e emergência; • Os carros autónomos irão também contribuir para melhorar a mobilidade (i.e., transporte de terceira idade ou deficientes), e aumento da segurança por eliminação do erro humano.

Cidades inteligentes e domótica

- A capacidade de ligar um número cada vez maior de dispositivos à Internet em simultâneo é uma componente chave da *IoT*, que por sua vez irá alimentar a inovação necessária à criação de cidades e casas verdadeiramente inteligentes;
- À medida que as zonas urbanas se expandem e aumentam de densidade populacional, cresce a importância de termos uma capacidade mais inteligente de gerir recursos, melhorar a segurança pública, fornecer serviços tais como recolha dos resíduos urbanos, reduzir o trânsito e o resultante impacto ambiental.

Eletrónica de Consumo

- Após um custo inicial grande dos módulos 5G no arranque da primeira onda de aplicações, é expectável que os preços entrem em declínio e, posteriormente, estabilizem. Estas condições permitem expor a eletrónica de consumo a um maior potencial de integração de comunicações 5G nas suas operações e funcionalidades;
- A primeira onda de aplicações 5G transformou o segmento B2C, permitindo às diferentes empresas adquirirem experiência neste contexto. Consequentemente, tal irá permitir-lhes capitalizar dessas interações B2C para lançarem também parcerias ao nível do B2B;
- Existe um grande potencial para casos de uso B2B para os fabricantes que pretendam capitalizar do 5G. No entanto, o alcance e a complexidade das aplicações associadas requerem (e fomentam) o desenvolvimento de parcerias para assegurar o melhor ROI. E.g., fornecedores de módulos de *IoT* ou automação industrial são excelentes parceiros potenciais quando já tiverem desenvolvido também hardware 5G e produtos que suportem 5G).

Saúde

- O 5G irá acelerar o desenvolvimento e expansão dos sensores biométricos, conferindo-lhes a capacidade de monitorizar a saúde além do bem-estar, sendo aplicados à monitorização da administração de fármacos, ou em doentes crónicos;
- O 5G irá também suportar análise de grandes dados (i.e., *Big Data*), reduzindo o tempo de disponibilização no mercado de novos tratamentos e reduzindo os enormes custos associados à investigação e desenvolvimento na atividade farmacêutica;
- A melhoria das comunicações irá auxiliar no desenvolvimento e disseminação de programas de telemedicina, onde pacientes com condições não críticas podem realizar consultas através de videochamada com grande clareza, promovendo diagnósticos mais precisos;
- A longo-prazo, o 5G promoverá a inovação noutras tecnologias médicas, tais como a utilização de *robots* em cirurgia.

Além dos setores supracitados, o 5G irá também dinamizar a produtividade e a participação laboral. Em concreto, os trabalhadores poderão colaborar de forma mais eficaz não só dentro da sua organização, mas também com parceiros, contribuindo para uma melhoria dos serviços aos clientes. O facto de ser possível fornecer ligações com melhor desempenho e fiabilidade aumentará também a possibilidade de teletrabalho, permitindo poupanças nas deslocações e consequentemente baixando o impacto da densidade populacional sobre os transportes em estrada e ferrovia. Em resultado, os trabalhadores poderão realizar o seu trabalho de forma mais eficaz e móvel, contribuindo para a remoção de barreiras no acesso a trabalho e carreiras por parte de pessoas sediadas em casa ou com dificuldades de mobilidade, bem como trabalhadores de idade mais avançada (um aspeto que adquire maior significância com o aumento da idade de reforma).

Estruturalmente, e de acordo com os seus objetivos de desenvolvimento, **o 5G abre um mundo de oportunidades para a transição digital**, permitindo a integração de TICs avançadas em ofertas de novas soluções competitivas para diferentes indústrias.

POTENCIAIS INDICADORES DA ÁREA

Entre os dias 20 de março e 27 de maio de 2016, o projeto H2020 5G-Ensure [147] lançou uma consulta pública [148] sobre segurança em 5G, conduzida de forma anónima. A consulta procurou recolher informação dos peritos de segurança, bem como das principais partes interessadas, para obter os diferentes pontos de vista sobre os desafios e prioridades de segurança e privacidade, bem como do seu impacto devido à adoção dos avanços tecnológicos associados ao 5G, e as ações em vista à normalização de segurança nesse contexto. A consulta visava assim tecer considerações gerais sobre os principais tópicos de segurança em 5G, nomeadamente segurança, privacidade, confiança, virtualização de redes e normalização. Aos participantes foi pedido que, i) indicassem quais eram os principais desafios numa rede 5G, ii) se a segurança associada deveria ser erguida sobre as redes anteriores, e iii) quais as novas prioridades de segurança para o 5G. No primeiro caso, não foram evidenciadas diferenças marcantes nas respostas, significando que os múltiplos facilitadores que compõem a arquitetura 5G (i.e., arquitetura de segurança, virtualização de redes, modelo de confiança, privacidade, AAA – autenticação, autorização, e contabilização, monitorização) são todos relevantes para a segurança do 5G. No segundo caso foi evidenciado que a segurança das redes anteriores é considerada suficientemente boa, e que mais aspetos podem ser reutilizados em 5G, tais como algoritmos de blockchain e mecanismos de autenticação e negociação de chaves. No último aspeto, sobressaem os mecanismos de segurança para infraestrutura de funções de redes virtualizadas, suporte de confiabilidade-integridade-autenticidade em dispositivos de recursos reduzidos, e autenticação transparente entre diferentes redes. **A conclusão global foi a de que o 5G, evoluindo sobre as redes 4G, poderá ter mecanismos adequados para as considerações tradicionais de segurança de redes de comunicações.**

Desde então foram colocadas em prática na Europa várias políticas de fomento à implantação do 5G no mercado digital, tais como o Plano de Ação 5G (lançado a 14 de setembro de 2016), o quadro de condições do Código de Comunicações Eletrónico Europeu [140] (em vigor em 21 de dezembro de 2018), e a designada "toolbox" de conectividade que suporta os estados-membros com as melhores práticas nessa implantação [141]. A problemática dos parâmetros de segurança foi revista durante este processo, desenvolvendo-se o conceito de Indicadores-chave de valor ("Key Value Indicators" ou KVIs), a refletir o impacto/relevância social da tecnologia. Os KVIs oferecem um ponto de partida para a definição, medição e avaliação do impacto social das novas tecnologias, permitindo a sua comparação, bem como a introdução de outras métricas mais amplas que as tradicionais métricas de sistemas de comunicação, envolvendo aspetos societais e tecnológicos (e de forma similar, apresentando mecanismos de intervenção técnicos e sociais).

A seguinte tabela, extraída do relatório de outubro de 2021 do 5G Observatory [149], sumariza o desempenho geral da Europa dos 27 face aos objetivos relevantes do 5G fomentados pela reinterpretação das métricas de segurança em termos de novos KVIs, que cruzam aspetos de segurança de infraestrutura com o conceito de segurança e fiabilidade das infraestruturas críticas para a transição digital.

Tabela 9 - Objectivos do plano de ação 5G, integrados pelos parâmetros da toolbox de cibersegurança

Objetivos	Desempenho/Estado
Lançamento comercial de serviços 5G em pelo menos uma grande cidade em todos os países da União Europeia	Até 2021 terão ocorrido lançamentos 5G comerciais em todos os países da União Europeia, com duas exceções: Lituânia e Portugal, cujo lançamento foi um pouco mais tarde. A maioria das implementações até ao momento ao longo dos 25 estados membros cobrem as principais cidades e áreas urbanas.
Cobertura ininterrupta 5G sem fios em banda larga para todas as áreas urbanas e principais estradas e ferrovias.	Com a base em dados colhidos pela Comissão Europeia em 2020, a linha base para a cobertura populacional na UE está estimada em 14%. Dados fragmentados sobre a cobertura em áreas urbanas por estados-membros estão disponíveis. Informação sobre cobertura 5G em estradas e ferrovias é praticamente não-existente (exceto na Finlândia) [150].
"Tecnologias digitais incluindo 5G", no núcleo de novos produtos, novos processos de fabrico e novos modelos de negócio	A disponibilização de redes 5G privadas está ainda numa fase de relativo crescimento inicial, mas será um contribuinte importante para a produtividade dos estados-membro e para a adoção de novas tecnologias para empresas, e que irá suportar o desenvolvimento contínuo do ecossistema 5G. A maioria dos ensaios parecem ocorrer dentro de redes privadas, apesar de existirem alguns exemplos com verticais que utilizam em redes públicas.
Autorização de bandas de espectro 5G	A banda 3.6 GHz foi a mais atribuída, em que 19 dos 27 estados-membros já atribuíram esta banda. A segunda banda mais popular é a dos 700 MHz, que foi atribuída em 17 dos 27 estados-membros. A banda menos popular é a dos 26GHz, que apenas foi atribuída em 7 estados-membros. Uma tendência crescente entre os estados-membros é a disponibilização de porções da banda-C a empresas privadas, tais como a porção dedicada de 100MHz disponível a verticais na Alemanha ou em países como a Suécia e a Holanda, permitindo a partilha de espectro para suportar implantações locais de rede.
Promoção de ensaios pan-Europeus com múltiplas-partes (corredores 5G)	12 "corredores digitais transfronteiriços" foram estabelecidos para acomodar testes reais de 5G para Mobilidade Automatizada e Ligada de forma Cooperativa. Adicionalmente, pelo menos 8 estados-membros referem a implantação Europeia de corredores 5G ao longo de redes TEN-T no interesse do Mercado Comum e de coesão nos seus planos de recuperação [151].
Implementação da "toolbox" 5G	A maioria dos estados-membros encetou as principais medidas para implementar as várias medidas técnicas e estratégicas. [151]

REALIDADE NACIONAL E RECOMENDAÇÕES

O leilão para acesso às frequências em Portugal terminou a 27 de outubro de 2021, após 1727 rondas concretizadas durante 200 dias. Neste processo estiveram em disputa 58 lotes que foram atribuídos a seis operadores distintos, com modelos de negócios diferenciados. A longa duração do processo, e o número de empresas interessadas, mostra como o 5G suscitou interesse em Portugal.

Atualmente a oferta do 5G disponibilizada por estes operadores apresenta o mesmo serviço móvel comumente utilizado da mesma forma que o 4G, considerando essencialmente um serviço do tipo eMBB. A oferta de outras funcionalidades, nomeadamente aquelas mais associadas ao setor industrial (i.e., URLLC e mMTC), poderão ser oferecidas aquando da implantação de soluções das próximas releases do 5G.

No contexto de recomendações associadas à disponibilização de redes 5G fiáveis e com segurança, Portugal contribuiu para o processo europeu de desenvolvimento da toolbox de cibersegurança, e desenvolveu as suas estratégias internas como resposta à mesma. Foram desenvolvidos internamente Análises de Risco e

Planos de Ação, que foram utilizados para a formação de politicas nacionais de segurança, junto das entidades reguladoras adequadas. No âmbito desse trabalho, as análises de risco foram referenciadas na componente "Desafios de cibersegurança" nesta secção do documento. Ainda nesse âmbito importa salientar o trabalho desenvolvido também sobre o caminho a seguir, nomeadamente:

- O novo paradigma de segurança criado pelo 5G requer uma reapreciação da atual política e enquadramento de segurança aplicado ao setor das comunicações, sendo necessário tomar medidas de mitigação;
- Torna-se necessário identificar omissões nos atuais mecanismos de aplicação de segurança, desde a legislação em cibersegurança, o papel de supervisão das autoridades públicas, assim como as obrigações e responsabilização por parte dos operadores e fornecedores.
- Os aspetos técnicos de segurança das gerações anteriores que permaneçam em funcionamento após a implantação do 5G requerem também medidas de mitigação, que deverão também determinar se a sua resolução é endereçada apenas do ponto de vista técnico, ou também do ponto de vista estratégico;
- Deverá também ser facilitada a coordenação de processos de normalização e certificação entre estados membros.

Além disso, olhando para o 5G como uma tecnologia crítica que irá agregar múltiplas tecnologias (como discutidas nos capítulos anteriores), poder-se-á adicionar um conjunto de linhas gerais adicionais a considerar.

É essencial garantir que as infraestruturas críticas estejam sempre disponíveis, independentemente de ataques, problemas de fabricantes, atualizações de *software*, suporte técnico, ou qualquer outra razão. Para tal, importa que todo o território nacional esteja coberto de uma forma heterogénea, no sentido de em qualquer ponto do território termos pelo menos duas ofertas de comunicação que sejam tecnologicamente independentes, i.e., não tenham elementos comuns nas suas cadeias de fornecimento.

Além deste aspeto de resiliência, a integração de novas tecnologias complementares às operações fundamentais das redes móveis no âmbito do 5G deve ser controlada. A inclusão de mecanismos de AI e de "*cloud*ificação" permitem (e.g.) automatizar aspetos de operação e otimização das redes, e melhorar significativamente o custo operacional da rede, bem como a sua capacidade de adaptação, respetivamente. No entanto, os aspetos de aplicação destas tecnologias mandatam considerações importantes sobre a transparência dos dados (desde a sua proveniência, processamento e armazenamento), em que os principais agentes de operações dos mesmos deverão ser incentivados (ou até mesmo instruídos) na divulgação de quais as práticas para assegurar a segurança desses mecanismos, e na transparência de todos os processos de decisão e controlo.

As tecnologias 5G trazem desafios estruturais para o país, e perigos de cibersegurança que, em última instância, tocam nos múltiplos problemas de diferentes tecnologias, como a *cloud* e a AI, ou as tecnologias de *IoT*. Os reguladores, as empresas e os utilizadores deverão estar cientes destes novos perigos nestes novos ambientes, sendo essencial educação de todos os atores envolvidos.


Tecnologias
Quânticas

As tecnologias anteriores implementam mecanismos de segurança em diferentes níveis, mas sempre recorrendo a algum tipo de método criptográfico baseado em complexidade computacional. A criptografia pública atual, aqui designada por criptografia clássica de chave pública, é baseada no pressuposto que existem problemas matemáticos fáceis de resolver num sentido e incrivelmente difíceis de resolver na direção contrária[7]. Existem diversos algoritmos criptográficos que implementam protocolos de chave pública entre os quais são de salientar: RSA (*Rivest-Shamir-Adleman*), *Diffie-Hellman key exchange*, *El-Gamal*, *DAS* (*Digital Signature Algorithm*), e *Criptografia de Curvas Elípticas* [153].

Atualmente, a segurança e a privacidade dos nossos dados, em transito ou armazenados, é em grande medida assegurada pela dificuldade em fatorizar números muito grandes, i.e. encontrar números parcelares cuja multiplicação seja um determinado número. Isto é, se é fácil multiplicar dois números, mesmo que sejam números muito grandes, é muito difícil decompor um número muito grande em números mais pequenos, e, em particular, nos seus fatores elementares, isto é, em números primos. De facto, se foram escolhidos dois números primos muito longos e se estes forem depois multiplicados, o que é uma operação relativamente simples e rápida, é muito demorado usando apenas um computador clássico obter os números primos originais a partir do resultado da multiplicação. Esta realidade matemática está por trás dos processos matemáticos que asseguram muita da segurança da nossa infraestrutura de comunicações.

No entanto, existem diversas situações em que a segurança e privacidade dos dados digitais deve ser mantida por períodos longos, e em alguns casos dezenas de anos. Como exemplo de tais situações temos os nossos dados genéticos e os nossos registos médicos, dados governamentais associados por exemplo ao cartão do cidadão, os registos digitais do ministério da justiça, e todos os setores do Estado ligados às funções de soberania. Todos estes dados digitais que de alguma forma são transportados em redes de comunicação e armazenados em bases de dados têm de ser preservados de forma inviolável, não podendo uma terceira entidade não autorizada ter acesso à informação.

Uma vez que a segurança dos protocolos criptográficos clássicos de chave pública usados para tornar a informação impercetível a um atacante no canal de comunicação se baseia fundamentalmente no poder computacional disponível e não em provas matemáticas, não é possível garantir a segurança e/ou privacidade dos dados digitais a uma escala temporal compatível com os requisitos impostos pela sensibilidade da informação em causa. Deve-se ainda salientar que mesmo a informação encriptada pode ser copiada sem que as partes interessadas tenham conhecimento de tal. Após copiada por uma terceira entidade não autorizada, esta poderá ter o tempo necessário para tentar desencriptar a informação. Este tipo de ataques é designado por "*intercept now, decrypt later*", e são complexos de se contornar uma vez que não é possível de forma clara saber qual será o poder computacional disponível

7 Um exemplo é a multiplicação e a factorização. A multiplicação é uma operação fácil de realizar mesmo para grandes números; mas já não é conhecido nenhum algoritmo que possa ser implementado num computador clássico capaz de resolver a operação inversa, ou seja a factorização, de forma que a complexidade não cresça exponencialmente, com o tamanho do número a fatorizar.

no futuro. Isto sugere que a informação encriptada atualmente, e considerada segura, corre o risco de ser tornada pública num prazo temporal relativamente pequeno, dispondo-se de maiores capacidades computacionais. Obviamente, estas situações não são compatíveis com a confidencialidade e criticidade de dados sensíveis que requerem medidas especiais de segurança.

Atualmente, uma forma prática de contornar este problema de criptografia pública é simplesmente usar chaves criptográficas cada vez mais longas para encriptar a informação, tornando-a impraticável para um atacante com grande capacidade computacional no futuro. O uso destas chaves criptográficas longas impõe constrangimentos importantes relacionados com a capacidade de gerar em tempo útil ("*real time*") essas chaves criptográficas e a capacidade de processar toda a informação gerada. Deve-se salientar que a geração de um número primo longo pode demorar vários minutos (dependendo do seu tamanho) antes de ser usado nos protocolos criptográficos. Isto impede o uso massivo de chaves criptográficas longas para encriptar e desencriptar a informação em muitas situações. Para além disso e como referido anteriormente, nada impede que daqui a 5-10 anos não haja poder computacional suficiente, que mesmo com o uso de chaves criptográficas longas, a informação atual não possa ser tornada pública em tempos úteis.

Uma outra forma sugerida de contornar este problema seria usar criptografia de chave simétrica. O protocolo de chave de uso único resolveria o problema de segurança associado aos dados digitais. No entanto, os requisitos de tal protocolo de criptografia pública impedem o seu uso nas redes de comunicação, uma vez que este protocolo exige que se partilhe e mantenha secreta uma chave criptográfica de igual tamanho à mensagem a transmitir, e que a chave só seja usada uma única vez e gerada de forma completamente aleatória.

Mesmo protocolos bem estabelecidos de chaves criptográficas simétricas, tais como o AES, podem num futuro próximo estar em risco. Esses protocolos necessitam de uma chave criptográfica pré-partilhada entre os utilizadores do canal de comunicação, usualmente distribuída usando criptografia de chave pública.

Este tipo de discussão sobre complexidade computacional está na base de toda a criptografia clássica de chave pública, e é um aspeto dominante de todas as discussões de cibersegurança na área. Contudo grandes avanços científicos e tecnológicos na área da computação vieram questionar esta abordagem, pois existem problemas que, embora sejam muito complexos de resolver num computador clássico, tornam-se de fácil resolução num computador quântico. A computação quântica, que tem princípios fundamentais completamente distintos da computação clássica, permite resolver algumas classes de problemas matemáticos muito complexos em tempo muito reduzido. Dois destes problemas matemáticos são precisamente a factorização e o problema do logaritmo discreto, dois conceitos que estão na base dos sistemas de distribuição de chaves criptográficas públicas hoje em uso. Apesar de avanços científicos potencialmente significativos (por exemplo na área da saúde) associados ao desenvolvimento da computação quântica, no caso da criptografia de chave pública a computação quântica é claramente um problema, e não uma solução.

A tecnologia quântica baseia-se no uso de dois princípios fundamentais da física quântica: a superposição quântica e o entrelaçamento quântico. A unidade fundamental é definida como sendo o qubit, e este representa a superposição de dois bits clássicos, o bit "0" e o bit "1", cada um com diferentes probabilidades de ocorrerem. Isto indica que um qubit pode ser simultaneamente o bit "0" e o bit "1". Por outro lado, o entrelaçamento quântico, propriedade física sem possibilidade de comparação no mundo clássico, permite descrever duas partículas distintas numa única função de onda (estado quântico). Alterar o estado de uma das partículas muda instantaneamente o estado da outra de maneira previsível. O uso destes estados entrelaçados permite aumentar exponencialmente a capacidade de processamento da computação. Se olharmos para o protocolo clássico de chave pública RSA-230, a factorização de 230 dígitos em dois primos de 115 dígitos cada necessita de 1023 operações num computador clássico. Num computador quântico são necessárias apenas 36 operações, numa aceleração de várias ordens de grandeza. Olhando para estes números, é fácil compreender como a computação quântica coloca em risco as garantias até agora fornecidas pela criptografia clássica de chave pública.

É previsível o aparecimento na próxima década de um computador quântico plenamente funcional, ou seja, um computador capaz de operar com um número elevado de *qubits*, com uma taxa de erro baixa e capaz de resolver problemas complexos tais como a factorização de números primos longos. Neste cenário deve-se abordar a questão da segurança da informação, não num contexto de poder computacional disponível, mas do ponto de vista matemático. Ou seja, devemos implementar protocolos criptográficos em que seja possível quantificar os seus limites de segurança, sendo que dentro desses limites de segurança os protocolos criptográficos devem ser incondicionalmente seguros, isto é, independentes do poder computacional atual e futuro.

Como referido anteriormente, pode-se tirar proveito das tecnologias quânticas para aumentar de forma exponencial a capacidade de computação. No entanto, os mesmos princípios da física quântica podem e devem ser usados para criar sistemas criptográficos incondicionalmente seguros. Este novo tipo de tecnologia baseia-se nos princípios da não clonagem, da superposição e do entrelaçamento. Estes são princípios físicos conhecidos há quase um século, mas a sua utilização em sistemas práticos só agora é tecnologicamente possível. O princípio da não clonagem diz-nos que considerando um sistema quântico, se à partida não conhecermos este estado não é possível replicá-lo com 100% de fidelidade. Uma consequência direta deste princípio implica que um atacante que esteja num canal de comunicação não conseguirá copiar de forma exata a informação que é codificada em estados quânticos. Mais ainda, a perturbação que a presença de um atacante introduz no canal de comunicação é mensurável e os legítimos proprietários da informação ficam a par da sua presença.

Nesse sentido, a utilização destes princípios permite também resolver problemas criptográficos prescindindo da complexidade computacional, o que faz com que as tecnologias quânticas deixem de constituir uma ameaça à segurança dos sistemas, e possam ainda fornecer mecanismos para aumentar a segurança dos mesmos. Atualmente encontramos na literatura protocolos quânticos capazes de gerar e distribuir chaves criptográficas de

forma incondicionalmente segura (descritos nas páginas seguintes) [153]. Protocolos como o BB84 representam uma forma prática de distribuir chaves criptográficas simétricas de forma segura, mesmo considerando que o atacante tem acesso a um computador quântico. Para além disso, o protocolo quântico de geração e distribuição de chaves criptográficas BB84 permite detetar a presença de um espião no canal de comunicação, por partes dos legítimos utilizadores do canal.

As tecnologias quânticas estão numa fase de intenso desenvolvimento. O impacto das tecnologias quânticas é muito abrangente e irão certamente ter um forte impacto na área da segurança dos sistemas de informação, nomeadamente na salvaguarda da informação que requer medidas especiais de segurança, embora tal impacto seja progressivo e será sentido de forma gradualmente crescente durante os próximos anos. As tecnologias quânticas irão trazer grandes riscos ao nível da segurança da informação, e potencialmente poderão expor vulnerabilidades, mas também poderão oferecer soluções que permitirão tornar os sistemas mais seguros. A forma como irão sendo introduzidas em cada sistema em particular irá ditar se o balanço será positivo em termos de aumentar a segurança dos sistemas, ou se, pelo contrário, irá ser no sentido de aumentar as vulnerabilidades.

BREVE RESENHA HISTÓRIA

Uma das primeiras referências relacionadas com a possibilidade de usar-se os princípios da mecânica quântica na área da computação foi feita por Benioff [154] em 1980. Esse trabalho pioneiro demonstrou a possibilidade teórica de computadores quânticos, descrevendo o primeiro modelo de mecânica quântica de um computador. Benioff mostrou que um computador poderia operar sob as leis da mecânica quântica, descrevendo dessa forma uma versão quântica das máquinas de Turing, baseando-se na descrição clássica de máquinas de Turing reversíveis[155].

No entanto, o conceito de computação quântica em si só foi introduzido por Feynman [156] em 1982. Este conceito surgiu como resposta à pergunta que computadores iremos usar para simular a física. Nesse trabalho pioneiro, Feynman também demonstrou que é impossível representar os resultados da física quântica num dispositivo clássico universal. Esta ideia original de Feynman fez germinar o conceito da computação quântica junto da comunidade científica, e em 1985 David [157] expandiu o conceito de computador quântico, mostrando ser em princípio possível construir um computador universal tendo por base os princípios da mecânica quântica e que essa máquina seria capaz de tratar problemas que são intratáveis num computador clássico. Contudo, o primeiro algoritmo (sem interesse prático) capaz de demonstrar a superioridade de um computador quântico face a um computador não quântico surgiu apenas em 1992, proposto por Deutsch and Jozsa [158].

Um marco histórico nesta área surgiu em 1994 quando Shor propôs um algoritmo quântico capaz de fatorizar números primos longos de forma eficiente [159]. Este algoritmo resolve tanto o problema de factorização quanto o problema de logaritmo discreto. Este enorme marco histórico colocou a computação quântica, assim como a segurança fornecida pela criptografia,

no centro da atenção da comunidade científica. Deve-se salientar que o conceito de qubit, que representa a unidade básica da informação quântica, foi introduzido em 1995 por Schumacher [160]. No seguimento destes trabalhos, em 1996 foi proposto um novo algoritmo quântico para procura não estruturada em base de dados, referido na literatura como algoritmo de Grover [161]. Ao contrário de outros algoritmos quânticos, como por exemplo o algoritmo de Shor, que podem fornecer aceleração exponencial sobre as suas contrapartes clássicas, o algoritmo de Grover fornece apenas uma aceleração quadrática.

A primeira implementação física com interesse prático aconteceu em 1998 [162] onde os autores implementaram o algoritmo de Deutsch and Jozsa usando ressonância magnética nuclear, num sistema de 2-*qubits*. Nesse mesmo ano, e usando a mesma interface física, foi implementado o algoritmo de Grover [163]. Mais recentemente (em 2001), o algoritmo de Shor foi implementado com sucesso e o número 15 foi fatorizado no IBM's Almaden Research Center e Stanford University [164]. Hoje em dia, o maior número primo fatorizado num computador quântico é o 21, usando o computador quântico da IBM com 16 *qubits* [165]. Deve-se salientar que devido à propagação de erro nas gates do circuito quântico não foi possível por exemplo fatorizar o número 35. De referir que para a factorização do protocolo criptográfico RSA-2048 seria necessário pelo menos 20 milhões de *qubits*, sendo necessárias 8 horas de computação [12], ou 13 436 *qubits* mas requerendo 177 dias de computação [166]. A título de exemplo, o computador quântico da IBM opera atualmente com 127 *qubits* [167], sendo que o roteiro dessa empresa para o desenvolvimento da computação quântica prevê o desenvolvimento de chips de 1000 *qubits* em 2023 [168].

Os desenvolvimentos tecnológicos associados à computação quântica foram sempre acompanhados por grandes avanços na área da criptografia quântica. Deve-se salientar primeiramente o trabalho pioneiro de Wiesner em 1968 [169] que propôs um método criptográfico para criar notas bancárias impossíveis de falsear, usando os princípios da mecânica quântica [170]. No entanto, os fundamentos para a criptografia quântica foram lançados posteriormente, nomeadamente o "*the no-go theorem*" [171] e o teorema da não-clonagem [172]. O "*the no-go theorem*" restringe o uso de variáveis escondidas em mecânica quântica, ao passo que o teorema da não clonagem afirma que é impossível criar uma cópia independente e idêntica de um estado quântico arbitrário desconhecido. A partir destes teoremas podemos afirmar que é impossível criar uma cópia independente e idêntica de um estado quântico desconhecido arbitrário. Com base nesses trabalhos, em 1984, Bennett e Brassard propõem o primeiro protocolo quântico para distribuição de chaves criptográficas, tipicamente designado por BB84 [173]. Nesse mesmo trabalho os autores introduzem o conceito de taxa de erro quântica para quantificar o impacto de um agente externo no canal de comunicação, estabelecendo dessa forma limites de segurança para o protocolo, isto é, a presença de um agente externo passou a poder ser detetado. O protocolo BB84 foi testado experimentalmente pela primeira vez em 1989 pelos mesmos autores [174], usando a polarização de fotões únicos como meio para transmitir informação. No seguimento destes trabalhos acerca de criptografia quântica, em 1991 Ekert descreveu um protocolo quântico (E91) usando um método alternativo para implementação dos sistemas de distribuição de chaves quânticas [175].

O E91 usa estados entrelaçados como forma de transmitir informação, e como forma de detetar a presença de um agente externo no canal de comunicação [176]. Sendo baseado em princípios fundamentais da física, o protocolo E91 é incondicionalmente seguro. O facto de este protocolo usar pares de fotões ao invés de fotões únicos permite um alcance superior. Apesar do protocolo BB84 e E91 fornecerem uma solução para o problema de distribuição de chaves criptográficas, existem variadíssimos problemas criptográficos que não podem ser resolvidos usando sistemas de distribuição de chaves quânticas simétricas tais como autenticação, e serviços de computação segura multiagente. Nesse sentido, protocolos quânticos para compromisso de bit [177][178], transferência oblívia [179] "*coin tossing*" [173][180] foram também desenvolvidos. No entanto, dada a particularidade desses protocolos envolvendo duas ou mais entidades que não confiam mutuamente, não foi possível demonstrar a segurança incondicional para tais protocolos usando apenas os princípios da física quântica. No entanto, usando por exemplo fundamentos da física relativista [181][182], ou funções criptográficas unidirecionais é possível estabelecer segurança do ponto de vista prático [183]. De notar que a prova de segurança para o protocolo BB84, admitindo que a capacidade de um atacante é apenas limitada pela física quântica, surgiu apenas em 2000 [184].

Após ser demonstrada a fiabilidade de implementação do protocolo BB84 em diversas experiências laboratoriais, uma das primeiras demonstrações em campo aconteceu em 1996 numa distância de 23 km em fibra ótica ao redor do lago de Genebra, Suíça, demonstrando a potencialidade prática desta tecnologia [185]. Por outro lado, devido à sua maior complexidade de implementação, apenas em 2004 foi efetuada a primeira demonstração em campo associada à utilização de estados entrelaçados (na polarização de pares de fotões) para distribuição de chaves criptográficas [186]. A viabilidade dos sistemas de distribuição de chaves quânticas entre dois utilizadores tem sido extensivamente estudada [187][188], por exemplo, em canais de comunicação de espaço livre [189], em fibras óticas [190] e ligações terra-satélite [191]. Estas experiências pioneiras permitiram o desenvolvimento de redes de distribuição de chaves criptográficas usando tecnologias quânticas. Diversas redes óticas têm sido desenvolvidas e implementadas em campo ao longo dos últimos anos, capazes de distribuir chaves criptográficas por vários utilizadores, incluindo a rede de três nós nos EUA designada por DARPA em 2003 [192], a rede SECOQC de seis nós na Europa em 2008 [193], a rede SwissQuantum desenvolvida e implementada na Suíça em 2009 [194], e a rede USTC10 de seis nós em Tóquio (2011) [195]. Recentemente (2021), foi reportada a implementação de uma rede ótica para distribuição de chaves quânticas que combina mais de 700 ligações em fibra ótica e duas ligações satélite-terra [196]. Atualmente, a rede quântica terrestre cobre uma distância superior a 2000 km, ao passo que a ligação satélite-terra em espaço livre permite ligar locais remotos separados por 2600 km [197]. Na Europa encontra-se a decorrer o projeto OPENQKD [198] com o objetivo demostrar e promover a integração das tecnologias quânticas com as infra-estruturas existentes de telecomunicações. Simultaneamente, no âmbito da Iniciativa Infraestrutura Europeia de Comunicação Quântica (EuroQCI) [199], têm sido implementadas redes quânticas nacionais no espaço europeu.

Em Portugal e no âmbito da iniciativa EuroQCI está a ser implementada a rede quântica PTQCI. Ainda no âmbito da iniciativa EuroQCI, está a iniciar-se uma segunda fase que tem como objetivo interligar as diferentes redes naconais no espaço europeu, usando ligações por fibra ótica e ligações por satélite, dotando assim a Europa de uma quântica segura.

FUTURO A 5 E 10 ANOS

Atualmente existem várias empresas internacionais tais como IBM, Microsoft, Google Research, D-Wave Systems, QuTech, Xanadu, IONQ e Zapata Computing, que estão ativamente a desenvolver chips e *software* para computação quântica. Particularmente a IBM e a Google ultrapassaram a barreira do desenvolvimento de chips operando com mais de 100 *qubits*. De salientar que a complexidade de representação de 100 *qubits* de um computador quântico do ponto de vista de computação clássica exigiria mais bits do que número de átomos no planeta Terra [200]. A expectativa, de acordo com o roteiro das várias empresas envolvidas nesta área, é a passagem dos 1000 *qubits* já em 2024, e nos próximos 10 anos termos chips capazes de operarem com mais de um milhão de *qubits*. No entanto deve-se salientar dois aspetos fundamentais: (i) os inúmeros desenvolvimentos nesta área tecnológica ocorrem a um ritmo sem precedente sendo por isso difícil consensualizar um roteiro preciso; (ii) o facto do desenvolvimento na área da computação quântica estar centrado em grandes empresas torna difícil de perceber o nível de desenvolvimento em que os seus produtos, de facto se encontram, podendo encontrar-se num nível tecnológico superior. Apesar disso, é expectável que no prazo de uma década esteja disponível para computação na *cloud* computadores quânticos completamente funcionais a operarem com mais de um milhão de *qubits*, já incluindo APIs para projeto de circuitos para programação do computador quântico.

Por outro lado, e como referido na secção anterior, as tecnologias quânticas para distribuição de chaves simétricas são atualmente por si mesmas uma tecnologia madura. Várias redes de teste já foram implementadas para demonstrar a potencialidade e fiabilidade desta tecnologia. Atualmente encontramos estes sistemas de distribuição de chaves simétricas recorrendo a tecnologias quânticas do ponto de vista comercial em empresas tais como a Id Quantique, Toshiba, QuintessenceLabs, LuxQuanta, e MagiQ. É expectável que num prazo de 5-10 anos esteja disponivel uma infraestrutura de comunicação quântica segura que abrangerá toda a União Europeia (a iniciativa EuroQCI). Esta futura rede europeia baseada em tecnologias quânticas tem como objetivo primordial proteger os dados que requeiram medidas especiais de segurança (governamentais e dos cidadãos) e infraestruturas críticas (redes digitais governamentais, redes elétricas, gás, água, entre outras). Para tal o objetivo a 10 anos passa pela integração dos sistemas baseados em tecnologias quânticas nas infraestruturas de comunicação existentes, fornecendo uma camada de segurança adicional.

É reconhecido pela comunidade científica que a computação quântica será na próxima década o principal inimigo da criptografia clássica. Atualmente, um agente externo acede (ou tenta aceder) a informação confidencial usando estratégias para obter senhas de autenticação ou instalando *software* malicioso em servidores e computadores. Ataques diretos às fragilidades dos protocolos criptográficos são bastante raros devido à complexidade e poder computacional necessários para efetuar este tipo de ataques. Contudo, **no dia em que o primeiro computador quântico ficar disponível, alguns dos protocolos criptográficos cruciais, que garantem a confidencialidade dos dados digitais, tornar-se-ão obsoletos.** A título de exemplo, um relatório do NIST (o norte americano National Institute of Standards and Technology) resumiu o impacto da computação quântica na criptografia de chave pública numa tabela única [47], apresentada na Tabela 10.

De salientar que os vários algoritmos de chave pública analisados se tornam inseguros perante a presença de um computador quântico. Por outro lado, os protocolos de chaves simétricas permanecem robustos, se adaptados: por exemplo no protocolo AES é recomendando a norma AES-256. Neste ponto é também importante referir que o protocolo criptográfico TLS (*Transport Layer Security*) usado em larga escala na Internet, usa também variantes do protocolo RSA, tais como o DHE-RSA e o ECDH-RSA. Esta realidade demonstra claramente o perigo global para a cibersegurança dos desenvolvimentos na área da computação quântica. Por outro lado, ataques à pré-imagem das funções de *hash* usando algoritmos quânticos, tal como o algoritmo de Groover, permite reduzir significativamente o tempo computacional para encontrar a pré-imagem de funções de *hash*, ou seja, tenta encontrar uma mensagem que seja um valor específico da função de *hash*. Nesse sentido pode afirmar-se que o algoritmo de Grover reduz a segurança de bits de tais funções para metade, ou seja, uma função de 128 bits oferece apenas segurança de 64 bits perante tal ataque.

Tabela 10 - Computação quântica e o seu impacto em criptografia [47]

Protocolo criptográfico	Tipo	Objectivo	Impacto da computação quântica
SHA-2, SHA-3	---	Funções de Hash	Requer o uso de chaves mais longas
AES	Chave simétrica	Encriptação	Requer o uso de chaves mais longas.
RSA	Chave pública	Assinaturas, Geração de chaves criptográficas	**Protocolo inseguro**
ECDSA, ECHD (Elliptic Curve Cryptography)	Chave pública	Assinaturas, Geração de chaves criptográficas	**Protocolo inseguro**
DSA (Finite Field Cryptography)	Chave pública	Assinaturas, Geração de chaves criptográficas	**Protocolo inseguro**

Dada a prática tecnológica atual, e as expectativas da computação quântica, é expectável que **a segurança das futuras redes de telecomunicações e sistemas de armazenamento de dados só seja possivel recorrendo a múltiplas camadas e que englobando complementarmente tecnologias clássicas e quânticas.**

OPORTUNIDADES

As infraestruturas de telecomunicações são elementos fundamentais da nossa sociedade. Isto é válido para uso civil, militar ou governamental. Em todos esses cenários, dados digitais confidenciais circulam nas infraestruturas de telecomunicações. Esses dados são protegidos de utilizadores não autorizados usando métodos criptográficos. No entanto, a resiliência desses métodos criptográficos perante o surgimento de um computador quântico é muito limitada, como vimos acima. Nesse sentido, a Comissão Europeia tem lançado vários programas de investigação na área da criptografia quântica com particular foco a partir do programa H2020, estendendo-se e reforçando-se no atual quadro Horizon Europe 2021-2027. O enquadramento político subjacente é a necessidade dos estados-membros iniciarem o processo de tornar os seus sistemas digitais resilientes num mundo pós-quântico. Nesse sentido uma *quantum flagship*[8] foi lançada em 2018 para apoiar o desenvolvimento de tecnologias quânticas ao longo de 10 anos, com um orçamento previsto (EU) de mil milhões de euros, e onde a criptografia quântica tem sido um dos maiores pilares. Esta *flagship* tem como objetivo apoiar a transformação da investigação europeia em aplicações comerciais que utilizem plenamente o potencial disruptivo das tecnologias quânticas. No entanto, as oportunidades não se limitam ao apoio através desta *flagship*. Dentro do programa H2020 foi financiada uma *test-bed* europeia[9] que permitiu a instalação de redes piloto quânticas em vários países europeus com o objetivo de testar a funcionalidade das tecnologias quânticas, nomeadamente criptografia. Este projeto encontra-se atualmente a decorrer e permitiu (num dos vários projetos envolvendo grupos de investigação nacionais) o teste de novos protocolos e aplicações usando tecnologias quânticas capazes de suportarem computação segura multiagente na área da medicina genómica.

Para além disto a Comissão Europeia tem promovido a incorporação de tecnologias quânticas no âmbito da defesa, através do programa *EDIDP - European Defence Industrial Development Programme*. Deve-se ainda salientar que recentemente a Comissão Europeia no âmbito do novo programa-quadro irá investir mais 154 milhões de euros, tendo em vista a instalação de infraestruturas quânticas, focando-se na implementação de projetos nacionais e em preparar a infraestrutura de teste e certificação dos sistemas de distribuição de chaves quânticas em larga escala. Um dos objetivos para este programa-quadro passa por reforçar a proteção das instituições governamentais da Europa, os seus centros de dados, hospitais, redes de energia entre outras infra-estruturas críticas, tornando-se um dos principais pilares da nova Estratégia de Cibersegurança da União para as próximas décadas.

8 https://qt.eu/

9 https://openqkd.eu/

POTENCIAIS INDICADORES DA ÁREA

Atualmente as tecnologias quânticas são uma área de investigação muito ativa a nível nacional e internacional. O número de artigos científicos publicados assim como o número de patentes aceites têm vindo a aumentar consideravelmente nos últimos cinco anos. Este desenvolvimento tem sido suportado por várias iniciativas mundiais com investimentos nacionais e regionais em investigação e tecnologia quântica atingindo quase 25 mil milhões de dólares em 2021 [202]. Este investimento global tem atraído jovens investigadores para esta área de investigação o que tem contribuído para o aumento do número de artigos publicados, assim como o número de patentes. Este investimento associado aos objetivos calendarizados pela Comissão Europeia desencadeou o surgimento de várias empresas (maioritariamente *spinoffs*) na União Europeia e por variadíssimos países fora da Europa. Em Portugal, empresas como a Altice, Warpcom, IPTelecom, Deimos, ou Capgemini recentemente criaram grupos de trabalhos ou departamentos na área das tecnologias quânticas participando em projetos científicos em conjunto com institutos de investigação e/ou universidades, ou até participando em demonstrações da fiabilidade e impacto das tecnologias quânticas em experiências realizadas em campo. Deve-se salientar ainda o interesse particular da defesa nacional na área da criptografia quântica como meio para fornecer chaves criptográficas às máquinas de cifra.

Como demonstrativo do impacto das tecnologias quânticas na indústria, deve-se salientar que há cinco anos o mercado europeu era essencialmente dominado por apenas duas empresas (Toshiba e IdQuantique) que forneciam equipamentos para sistemas criptográficos, particularmente sistemas de distribuição de chaves quânticas. Hoje em dia a lista de fornecedores oficiais da União Europeia inclui mais de 30 empresas.

Identificam-se na tabela seguinte um conjunto de indicadores que podem permitir um quadro situacional da adoção das tecnologias quânticas. Dada a forte dependência entre valores numéricos e aspetos de praticabilidade e de impacto em cibersegurança, estes indicadores têm necessariamente de refletir essa dimensionalidade intrínseca ao estado atual das tecnologias quânticas.

Tabela 11 - Métricas potenciais para avaliação societal de segurança no uso de tecnologias quânticas

Métrica	Valor	Mecanismo de obtenção
Número de empresas que comercializam sistemas de comunicação/informação recorrendo tecnologia quântica	31	De acordo com a lista de fornecedores disponibilizada pela EU no âmbito da call EuroQCI
Números de redes quânticas em funcionamento	8	Análise do estado da arte
Número de empresas que declaram desenvolvimento em computação quântica	25	Análise do estado da arte
Número máximo de quibts disponíveis para computação quântica	127	Estado da indústria, e.g. IBM roadmap
Taxa de geração chaves quânticas sistemas variáveis discretas	1 kbps @ 24dB	ITU-T Focus Group on Quantum Information Technology for Networks D2.5
Taxa de geração chaves quânticas sistemas variáveis contínuas	25 kbps@10 dB; 1 kbps@20 dB	ITU-T Focus Group on Quantum Information Technology for Networks D2.5
Taxa de geração chaves quânticas sistemas baseados em entrelaçamento	40 bps @ 8dB	ITU-T Focus Group on Quantum Information Technology for Networks D2.5
Maior número fatorizado recorrendo a computação quântica	21	Análise do estado da arte
Número de códigos RSA fatorizados usando computação clássica	23	Análise do estado da arte

Portugal tem vindo a demonstrar bons resultados em termos de inovação nesta área extremamente competitiva a nível internacional. O estudo e desenvolvimento de tecnologias quânticas em Portugal com aplicação em cibersegurança tem tido o envolvimento de diferentes grupos de investigação em comunicação, criptografia e computação quântica. Deve-se ainda salientar o muito recente envolvimento em Portugal de empresas privadas nesta área de investigação. Universidades, institutos de investigação e empresas têm participado em projetos de investigação científica com particular foco para o desenvolvimento de tecnologias quânticas na área da segurança e privacidade dos dados digitais.

No âmbito do projeto nacional QSCRIPT, foi feita uma primeira experiência de distribuição de chaves quânticas envolvendo entidades militares, de soberania, a academia e a indústria. No âmbito do projeto europeu DISCRETION, que tem uma forte participação nacional, estão a ser desenvolvidos sistemas de distribuição de chaves criptográficas, e maquinas de cifra. No âmbito do projeto PTQCI, com cofinanciamento nacional e europeu, estão a ser instalados os primeiros nós e ligações da futura rede quântica nacional, perspetivando-se já a sua interligação a outras redes quânticas já instaladas ou a instalar no espaço europeu. Nesta linha, a rede nacional quântica arranca em inícios de 2023.

Uma primeira recomendação em termos de cibersegurança perante o surgimento de um computador quântico funcional durante a próxima década **é a criação de uma análise crítica dos protocolos usados em serviços de autenticação e assinaturas digitais**, quer do ponto de vista de uso, quer de armazenamento de dados. Nesse sentido, dotar infraestruturas críticas de protocolos associados a tecnologias quânticas é um passo essencial para garantir a segurança e privacidade dos dados digitais. Já foram reportados diversos ciberataques bem-sucedidos explorando debilidades associadas aos geradores de números aleatórios, expondo publicamente, por exemplo, informação (chaves criptográficas) dos cartões de identificação dos cidadãos de Taiwan [203]. Nesse sentido, o uso de geradores quânticos de números aleatórios deve ser incorporado na infraestrutura protocolar associada a sistemas críticos (e.g. o cartão de cidadão), pois permitirá não só gerar números verdadeiramente aleatórios, como também números primos longos essenciais para protocolos como RSA.

Uma segunda recomendação em termos de cibersegurança é o uso de **redes quânticas para a distribuição de chaves criptográficas simétricas** entre entidades e serviços governamentais onde seja necessário garantir segurança particularmente elevada dos dados digitais. De particular interesse serão áreas da soberania nacional, administração pública e serviços diplomáticos. Deve-se salientar que os sistemas de distribuição de chaves quânticas podem ser usados em encriptadores clássicos tais como máquinas de cifras, ou protocolos criptográficos simétricos, como por exemplo o AES. Isto oferece uma camada adicional de segurança na qual o sistema de distribuição de chaves quânticas continuamente atualiza as chaves criptográficas usadas nesses encriptadores clássicos.

Notas Conclusivas

A nossa sociedade vive um período transformativo, com as denominadas tecnologias de informação e comunicação a permearem todos os aspetos da vida social e económica. Vivemos uma época singular, em que diversos modelos tecnológicos estão a tornar-se comuns, penetrando a nossa vida frequentemente de uma forma sub-reptícia. Neste mesmo contexto, e também potenciados pelas capacidades tecnológicas que se vão implementando, os desafios de cibersegurança ganham uma nova expressão, não só pelos novos mecanismos de ataque que aparecem, mas também pelas capacidades crescentemente destrutivas para a sociedade que os novos ataques poderão representar.

Este documento faz uma súmula, necessariamente incompleta, de alguns dos desafios que a introdução de novas tecnologias irá trazer. Essencialmente, o documento aborda um conjunto grande de novas tecnologias, mas numa perspetiva englobadora, tal como se perspetiva com os novos modelos associados às comunicações móveis da tecnologia 5G. Nesse sentido, os aspetos de computação na nuvem, o uso de inteligência artificial ou a expansão de modelos de Internet das Coisas, são conceitos que não podem deixar de ser abordados para uma análise consistente dos desafios que enfrentamos. Todas estas tecnologias, que apresentam uma dinâmica de implementação independente entre si mesmo, são peças importantes de uma sociedade tecnologicamente avançada, suportada em processos integrados pela tecnologia 5G. Assim, pese o levantamento de desafios deste documento ter sido feito de uma forma isolada, **os desafios de cibersegurança que enfrentaremos no futuro efetivamente serão o resultado cumulativo do uso de todos estes conceitos tecnológicos.**

Adicionalmente o documento aborda a questão da tecnologia quântica, dada a sua relevância para os aspetos mais fundamentais de criptografia, usados em todas estas tecnologias mencionadas. Embora seja a tecnologia mais emergente de todas as cobertas pelo documento, é a tecnologia que potencialmente poderá questionar todos os modelos de segurança em vigor neste momento, em todos os outros domínios mencionados.

Globalmente, há um conjunto de preocupações que são transversais a todo o documento. **É necessário colmatar o *deficit* de conhecimento quanto aos aspetos de cibersegurança** associados a todas estas tecnologias. Esse *deficit* começa no cidadão comum, mas também nas empresas e organizações, tocando inevitavelmente órgãos de governança. Não poderemos ultrapassar os desafios que se perspetivam sem endereçar este problema de conhecimento.

Um outro problema transversal prende-se com o dinamismo destas tecnologias. É claro que todas estas tecnologias estão em processos de evolução rápida, quer em questões de detalhe tecnológico, quer em questões de modelos (e disseminação) de utilização. Os problemas presentes hoje não serão os problemas existente daqui a dois anos, embora continuemos a falar dos mesmos conceitos. **Não poderemos ter uma abordagem reativa para a minimização de todos os riscos** que irão aparecer, sob pena de dedicarmos a próxima década a responder tardiamente a problemas de cibersegurança com potencial impacto devastador para a nossa sociedade. Todos os envolvidos no problema devem desenvolver estratégias que permitam precaver os potenciais problemas futuros, com uma natural razoabilidade temporal.

Uma nota adicional sobre este documento: ele não ambiciona ser a palavra final sobre os problemas mencionados. Há diferentes aspetos que foram ou abordados muito sumariamente, ou até foram simplesmente excluídos para não densificar desnecessariamente o essencial fluxo da discussão. O que é claro é a necessidade de, através de documentos enquadradores (separada ou conjugadamente), desenvolver abordagens que permitam promover boas práticas no uso destas tecnologias – documentos que provavelmente terão de ser atualizados com regularidade. Esses documentos deverão agregar considerações legais, regulamentares, económicas e sociais, e envolver as entidades com responsabilidades na prevenção e respostas nos processos de cibersegurança de todas estas áreas, cobrindo assim de uma forma integrada os aspetos legais e tecnológicos, garantido uma efetiva resiliência da nossa sociedade e contribuindo para uma maior autossuficiência tecnológica nacional.

Em termos de conclusão, não podemos deixar de terminar com uma mensagem positiva do ponto de vista da cibersegurança. Pese todos os perigos associados a estas tecnologias, elas encerram inerentemente potencialidades de uso para minorar os perigos de ciberataques, e o desenvolvimento atempado de respostas globais no país para toda esta problemática poderá colocar as instituições e empresas nacionais na liderança internacional de cibersegurança.

Legislação Adicional

Para diversos casos abordados neste documento existem enquadramentos regulatórios e legais em termos internacionais, que são indicativos de boas práticas nas áreas.

Nesta seção apresentamos algumas das mais relevantes.

COMPUTAÇÃO NA NUVEM

A área da cloud computing é um setor já bem estabelecido, com importância estratégica reconhecida. Assim, não é de estranhar que exista uma panóplia de recomendações e regulamentos associados, embora não existam ainda considerações adequadas para as novas tendências identificadas no Capítulo 2.

Nos EUA, atualmente as leis governamentais do *PATRIOT Act* [208] e *CLOUD Act* [209] permitem ao governo acesso a dados de utilizadores que usam serviços que estão sob a jurisdição dos EUA. Indiretamente estas peças regulatórias estão a incentivar os fornecedores de serviços a adotar medidas de criptografia e segurança, pese embora o impacto das considerações de segurança nacional em toda a atividade americana. No entanto, não há uma legislação no contexto de recomendações de segurança para fornecedores de Cloud.

Em termos europeus, temos diversas iniciativas do ponto de vista da regulação. São exemplos disso a proposta legislativa *Digital Services Act* [16] da Comissão Europeia e a estratégia European Data Strategy [17]. Já no que respeita à cibersegurança, o *EU Cybersecurity Act* [204] também inclui a Cloud como um dos serviços constituintes deste quadro regulatório. O ato delega na ENISA a criação e manutenção de um framework de certificação de cibersegurança para Cloud, baseado nas melhores práticas atuais e com o objetivo de aumentar a transparência e garantir a cibersegurança destes serviços. São definidos diferentes níveis (alto, substancial e básico) de regras que devem ser seguidas para obter a certificação. Em Portugal, a diretiva SRI (Segurança das Redes e da Informação) [205] estabelece requisitos particulares para os operadores de serviços digitais, onde se inserem os prestadores de serviços de cloud, nomeadamente no que concerne à segurança, ao tratamento de incidentes, à gestão da continuidade das atividades, às auditorias e à conformidade com normas internacionais.

Em dezembro de 2020 um rascunho do quadro regulatório de certificação para Cloud [206] foi publicado pela ENISA para revisão externa. Este quadro regulatório pretende, não só definir os critérios de certificação de serviços cloud mas, acima de tudo, a harmonização a nível europeu para incentivar o desenvolvimento do mercado. Alguns países como França, Alemanha e Espanha já publicaram seus próprios frameworks de certificação para cloud [207]. No que respeita a referências internacionais, as normas da família ISO/IEC 17000, em concreto a ISO/IEC 17788 e a ISO/IEC 17789 representam dois marcos normativos reconhecidos e que são usados no quadro regulatório de certificação da ENISA [210].

O RGPD (Regulamento Geral de Proteção de Dados [211]) traz também requisitos especiais ao nível da privacidade, em particular em ambientes cloud (ex: artigos 25, 30 e 32), dada a sua distribuição geográfica e jurisdicional, com diferentes regras, exigências e legislações a nível global. Estas implicações são agravadas pelo caso Shremms II [212] e consequentes decisões do Tribunal de Justiça da União Europeia sobre a conformidade legal das prorrogativas das agências, no caso dos Estados Unidos, poderem intercetar e vigiar comunicações e informação.

O Decreto-Lei 65/2021 [217] introduz o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019. Este decreto-lei aplica-se às entidades previstas nas alíneas a) a d) do n.º 1 do artigo 2.º do Regime Jurídico da Segurança do Ciberespaço, o que inclui os fornecedores de serviços digitais e em particular os fornecedores de computação cloud. Outras entidades como a Administração Pública e fornecedores de Serviços Críticos, frequentes utilizadores de ambientes cloud (público ou privado), devem igualmente respeitar esta lei. Constitui um ponto importante para a segurança das instituições nacionais ao definir procedimentos mínimos a considerar, tais como a existência de um ponto de contacto, um responsável de segurança, a existência de um processo de gestão de risco com identificação dos serviços críticos, inventário de ativos e um plano de segurança.

Mais recentemente, foi publicada a diretiva NIS 2 (2022/2555) [218], que deve ser transposta até Outubro de 2024. A nova diretiva visa harmonizar a gestão de segurança entre todos os Estados-membros, reforçando as obrigações em termos de cibersegurança e de notificação em caso de incidentes. Além de estabelecer um referencial mínimo para a gestão da segurança, também obriga vários fornecedores de serviços, onde se incluem os fornecedores de Cloud, a incluir equipas de CSIRT com processos padronizados. De notar que a diretiva também inclui clientes destes serviços, caso prestem serviços críticos ou outros como investigação.

INTELIGÊNCIA ARTIFICIAL

É expectável que os sistemas baseados em AI continuem o seu desenvolvimento bem como a sua crescente integração na sociedade. Desta forma, é também expectável que a legislação evolua no sentido de criar um meio justo e equilibrado para que os cidadãos consigam viver mantendo a qualidade de vida que os sistemas inteligentes conseguem proporcionar, mas também garantido os seus direitos.

A vice-presidente executiva para uma Europa adequada para a era digital, Margrethe Vestager afirmou: "On Artificial Intelligence, trust is a must, not a nice to have", o que valoriza a questão da confiança durante a utilização de AI em qualquer tipo de ambiente. A diretiva europeia [119] ambiciona estabelecer novos padrões globais para uma inteligência artificial confiável, salvaguardando-se a segurança e os direitos fundamentais dos cidadãos. O novo regulamento será aplicado diretamente da mesma forma, em todos os estados-membros fazendo com que os sistemas de AI de risco inaceitável sejam banidos, isto é, aqueles que representam uma clara ameaça à segurança, à subsistência e aos direitos das pessoas, nomeadamente sistemas de AI que manipulem o

comportamento, ou que permitam que os governos atribuam "pontuações sociais" às pessoas [213]. Além disso, de acordo com a Lei n.º 27/2021, de 17 de maio (Carta Portuguesa de Direitos Humanos na Era Digital), "A República Portuguesa participa no processo mundial de transformação da Internet num instrumento de conquista de liberdade, igualdade e justiça social e num espaço de promoção, proteção e livre exercício dos direitos humanos, com vista a uma inclusão social em ambiente digital"[214] valorizando portanto as questões de liberdade, igualdade e justiça social durante a utilização da internet o que inclui a AI.

Os vários artigos que compõem a Carta Portuguesa de Direitos Humanos na Era Digital incluem direitos em ambiente digital, de acesso e à proteção contra a desinformação, incluindo direitos à privacidade em ambiente digital, à neutralidade da lei, desenvolvimento das competências digitais, direito ao esquecimento e à cibersegurança. Embora alguns pontos mencionados ao longo do documento possam também ser aplicados ao processamento de dados por parte de algoritmos inteligentes ou ML, o artigo 9.º menciona explicitamente aspetos relacionados com AI nomeadamente: " A utilização da inteligência artificial deve ser orientada pelo respeito dos direitos fundamentais, garantindo um justo equilíbrio entre os princípios da explicabilidade, da segurança, da transparência e da responsabilidade, que atenda às circunstâncias de cada caso concreto e estabeleça processos destinados a evitar quaisquer preconceitos e formas de discriminação"; "As decisões com impacto significativo na esfera dos destinatários que sejam tomadas mediante o uso de algoritmos devem ser comunicadas aos interessados, sendo suscetíveis de recurso e auditáveis, nos termos previstos na lei"; e finalmente, "São aplicáveis à criação e ao uso de robôs os princípios da beneficência, da não-maleficência, do respeito pela autonomia humana e pela justiça, bem como os princípios e valores consagrados no artigo 2.º do Tratado da União Europeia, designadamente a não discriminação e a tolerância".

Esta carta é um conjunto de normas programáticas, em grande parte redundantes em relação às já existentes no ordenamento jurídico, desde logo na Constituição da República Portuguesa. Contudo, o capítulo relativo à AII, embora seja mencionada, resume-se a apenas três números do artigo 9.º, não sendo, portanto, completa para assegurar um ambiente seguro no que diz respeito à utilização de AI nos nossos dias. De qualquer forma, trata-se de um importante passo para a sua regulamentação visto que desta forma estes temas passam a ser discutidos mais assertivamente. Um exemplo concreto é o facto de ser mencionada a necessidade de haver transparência, segurança e responsabilidade. Contudo, este ponto não prevê como tal deve ser garantido devido por exemplo à partilha de dados com terceiros, o próprio sistema pode garantir todos estes requisitos, mas nada estará relacionado com subprodutos que façam parte da arquitetura final. Além disso, não prevê uma solução para atribuição de responsabilidades em caso de falha. Menciona que deve ser atribuída uma responsabilidade, mas não refere a quem ou o quê. Note-se que é referido que deve ser garantido um "justo equilíbrio", o que poderá indicar que o desenvolvimento de AI não será comprometido desde que garanta segurança, privacidade e proteção de dados.

De acordo com o Regime Jurídico das Decisões Automatizadas, o artigo 22.º está relacionado com a criação de perfis e decisões automatizadas, contudo alguns autores questionam o conceito de decisão presente no RGPD: "Se a decisão não for propriamente uma decisão final, mas antes um passo intermédio num procedimento de tomada de decisão, ou até mesmo numa atividade de definição de perfis, poderá considerar-se abrangida pelo âmbito do artigo?" [215]. Assumindo que o ponto 2 do artigo 9.º da Carta Portuguesa de Direitos Humanos na Era Digital tenta endereçar esta questão das decisões automatizadas, alguns problemas práticos podem ser evidenciados como é caso de partilha de ambientes de *IoT* dotados de AI em que várias pessoas usam o ambiente sem necessidade de se identificarem. Contudo, uma auditoria sobre as decisões tomadas é essencial para se poder rever quais foram as bases para uma decisão e como ocorreu, e os enquadramentos legais em jogo aparentam revelar-se insuficientes para as múltiplas situações que se perspetivam para o futuro.

REDES 5G

As redes 5G são um dos ambientes mais regulamentados do mundo.

Em termos dos objetivos políticos estruturais para a Europa, incluindo os objetivos digitais para a Europa 2030, podem ser consultadas [132][150][151]. Na Europa foi desenvolvido o denominado 5GObservatory, que produz relatórios periódicos trimestrais[10], entre outros documentos (e.g [134]).

Do ponto de vista de recomendações de investimento, a EU formalizou a diretiva 2018/1972 [140] que estabelece as regras e objetivos comuns europeus para a regulação da indústria das telecomunicações, definindo a forma como os fornecedores de redes e/ou serviços poderão ser regulamentados pelas autoridades nacionais, no tocante ao 5G. Uma compilação dos principais resultados da adoção dessa regulamentação é facultada por representantes dos diversos estados-membros, sob alçada do Grupo Especial de Conetividade, cujos resultados foram compilados num relatório conjunto [141]. Em termos de cibersegurança, ainda temos diversas iniciativas no contexto Europeu, coordenadas pelo Grupo de Cooperação em Sistemas de Informação e Redes da Comissão Europeia, cobrindo aspetos como OpenRAN [133], avaliação de risco [139] e utilização de ferramentas de segurança estratégica [151]. A European Union Agency for Cybersecurity (ENISA) tem identificado ao longo dos últimos anos vários riscos de segurança associados à implementação de 5G na Europa, e produzido um conjunto continuado de documentos em coordenação com os estados-membros, incluindo aspetos tão vastos como confiança na cadeia de fornecimento, fiabilidade de soluções e auditoria de processos. Este trabalho é regulamente atualizado em diferentes aspetos.

As normas técnicas associadas ao 5G estão regulamentadas pelo 3GPP, podendo ser consultadas como: Release 15 [125]; Release 16 [126]; e Release 17 [127].

Em Portugal, parte dos aspetos de cibersegurança dos sistemas e redes de comunicação está coberta na transposição nacional de diretivas europeias relevantes, na Lei das Comunicações Eletrónicas, Lei nº 16/2022 de 16 de Agosto, e legislação associada.

10 https://5gobservatory.eu/observatory-overview/observatory-reports/

Nota Metodológica

O documento foi construído com base nas contribuições de um conjunto alargado de peritos, entre os quais se incluem: Rui Luis Aguiar (editor), Mário Antunes, João Paulo Barraca, Paulo Bartolomeu, Daniel Corujo, Vitor Cunha, Rafael Direito, Diogo Gomes, Leonardo da Cruz Marcuzzo, Ricardo Martins, Paulo Mateus, Armando Nolasco Pinto e Nuno Silva.

A metodologia utilizada para este documento foi baseada no uso extensivo de pesquisa bibliográfica, incluindo aspetos académicos e de mercado, bem como documentação regulamentar e decisões políticas relevantes. Acessoriamente foram consultados peritos internacionais, representando agências de normalização, academia e indústria na área da segurança como elementos de validação das principais conclusões do documento.

10
Referências Principais

[1] Zhao, G., Liu, J., Tang, Y., Sun, W., Zhang, F., Ye, X., & Tang, N. (2009). Cloud Computing: A Statistics Aspect of Users. In M. G. Jaatun, G. Zhao, & C. Rong (Reds), Cloud Computing (bll 347–358). Berlin, Heidelberg: Springer Berlin Heidelberg.

[2] https://www.darpa.mil/about-us/timeline/project-mac

[3] https://www.darpa.mil/about-us/timeline/arpanet

[4] https://www.dataversity.net/brief-history-*cloud*-computing

[5] https://www.c-sharpcorner.com/article/top-10-*cloud*-service-providers/

[6] https://digital-strategy.ec.europa.eu/en/policies/*cloud*-computing

[7] https://eufordigital.eu/

[8] [https://ec.europa.eu/eurostat/en/web/products-eurostat-news/-/ddn-20211209-2

[9] https://www.alliedmarketresearch.com/*cloud*-services-market

[10] Gartner says four trends are shaping the future of public cloud. Gartner. Retrieved February 16, 2022, from https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud

[11] AI market size 2018-2025. (2022). Retrieved 16 February 2022, from https://www.statista.com/statistics/607716/worldwide-artificial-intelligence-market-revenues/

[12] Panetta, K. (2019). Is The *Cloud* Secure. Retrieved 16 February 2022, from https://www.gartner.com/smarterwithgartner/is-the-*cloud*-secure

[13] F.Bonomi, R.Milito, J.Zhu, and S.Addepalli, "Fog computing and its role in the Internet of Things," in ACM SIGCOMM Workshop on Mobile cloud Computing, Helsinki, Finland, 2012, pp. 13--16

[14] Firdhous, Mohamed & Ghazali, Osman & Hassan, Suhaidi. (2014). Fog Computing: Will it be the Future of Cloud Computing?.

[15] https://www.gartner.com/smarterwithgartner/is-the-*cloud*-secure

[16] https://ec.europa.eu/info/digital-services-act-ensuring-safe-and-accountable-online-environment_en

[17] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

[18] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[19] https://www.pcisecuritystandards.org/document_library

[20] https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996

[21] https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

[22] https://www.checkpoint.com/cyber-hub/*cloud*-security/what-is-*cloud*-security/

[23] Huizenga, R. (2021, October 1). Ten *cloud* opportunities you may not have fully exploited. Retrieved February 16, 2022, from https://www.capgemini.com/2021/09/ten-*cloud*-opportunities-you-may-not-have-fully-exploited/

[24] Gartner Magic Quadrant for WAN Edge Infrastructure, September 2020.

[25] https://empresite.jornaldenegocios.pt/Actividade/*cloud-computing*

[26] https://www.datamation.com/trends/cloud-computing-job-market-trends/

[27] https://tic.gov.pt/pt/web/tic/estrategia-para-a-transformacao-digital-da-administracao-publica-2021-2026

[28] https://eco.sapo.pt/2021/09/17/vantagens-da-cloud-convencem-e-servicos-crescem-20-em-portugal/

[29] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises

[30] Cloud Computing Market In Portugal, 2018 – 2022

[31] https://tic.gov.pt/documents/37177/0/CTIC+Estrate%CC%81giaCloud+-+novembro2020.pdf/4c7b4f4f-4647-a6d8-b6a5-a988ae133c95

[32] Tarkoma, Sasu, and Artem Katasonov. 2011. Internet of Things Strategic Research Agenda (IoT-SRA). Finnish Strategic Centre for Science, Technology, and Innovation: For Information and Communications (ICT) Services, Businesses, and Technologies, Finland.

[33] Tzafestas, Spyros G. "Ethics and law in the internet of things world." Smart cities 1.1 (2018): 98-120.

[34] Statista, "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (Online)

[35] Michael Chui, Mark Collins, Mark Patel. The Internet of Things: Catching up to an accelerating opportunity, McKinsey & Company, 2021.

[36] Silva BN, Khan M, Han K. 2018. Internet of Things: a comprehensive review of enabling technologies, architecture, and challenges. IETE Technical Review 35(2):205–220

[37] Lynn, T.; Endo, P.T.; Ribeiro, A.M.N.C.; Barbosa, G.B.N.; Rosati, P. The Internet of Things: Definitions, Key Concepts, and Reference Architectures. In The Cloud-to-Thing Continuum; Lynn, T., Mooney, J., Lee, B., Endo, P.T., Eds.; Palgrave Macmillan: London, UK, 2020.

[38] Wollschlaeger M, Sauter T, Jasperneite J. 2017. The future of industrial communication: automation networks in the era of the Internet of Things and industry 4.0. IEEE Industrial Electronics Magazine 11(1):17–27.

[39] Mancini, Mônica. "Internet das Coisas: História, conceitos, aplicações e desafios." Project Management Institute–PMI (2017).

[40] Kuyoro, Sade, Folasade Osisanwo, and Omoyele Akinsowon. "Internet of things (IoT): an overview." Proc. of the 3th International Conference on Advances in Engineering Sciences and Applie) Technologies and Innovation. CITI 2021. Communications in Computer and Information Science, vol 1460. Springer, Cham. https://doi.org/10.1007/978-3-030-88262-4_14

[41] Gackowiec, Paulina, i Marta Podobińska-Staniec. "*IoT* Platforms for the Mining Industry: An Overview". Inżynieria Mineralna, t. 21, nr 1, Polskie Towarzystwo Przeróbki Kopalin d Mathematics (ICAESAM). 2015

[42] Yerovi, E., Delgado-Vera, C., Molina-Oleas, W., Ortega-Ponce, L. (2021). A Brief Systematic Review of the Latest Advances in IOT Platforms in Agriculture. In: Valencia-García, R., Bucaram-Leverone, M., Del Cioppo-Morstadt, J., Vera-Lucio, N., Jácome-Murillo, E. (eds) 2019, s. 267–72.

[43] https://www.sam-solutions.com/blog/top-iot-platforms/

[44] Kumar, Sachin, Prayag Tiwari, and Mikhail Zymbler. "Internet of Things is a revolutionary approach for future technology enhancement: a review." Journal of Big data 6.1 (2019): 1-21.

[45] Palo Alto Networks, "Unit 42 IoT Threat Report", 2020, Online [Consultado em 06/2022].

[46] Ericson, "Ericsson Mobility Report", November 2020, Online [Consultado em 06/2022].

[47] VisionMobile , "The Essencial Guide to Open Source in IoT" Whitepaper, 2016, [Consultado em 06/2022]

[48] Synopsis, "2022 Open Source Security and Risk Analysis", 2022, Online [Consultado em 06/2022]

[49] Noopur Davis, "2020 Xfinity Cyber Health Report", COMCAST, 2020, Online [Consultado em 06/2022]

[50] Brandan Schondorfer, Nader Zaveri, Tyler Mclellan, Jennifer Brito, "Old Services, New Tricks: Cloud Metadata Abuse by UNC2903", May 2022, Online [Consultado em 06/2022]

[51] National Institute of Standards and Technology, "Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products", February 2022, Online [Consultado em 06/2022].

[52] European Union Agency For Network And Information Security , "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures", 2017, Online [Consultado em 06/2022].

[53] European Union Agency For Network And Information Security , "GUIDELINES FOR SECURING THE INTERNET OF THINGS: Secure supply chain for IoT", Novembro 2020, Online [Consultado em 06/2022].

[54] European Union Agency For Network And Information Security , "ENISA Good practices for IoT and Smart Infrastructures Tool", 2022, Online [Consultado em 06/2022].

[55] Drummond Reed, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, Markus Sabadello, "Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations", W3C Proposed Recommendation, August 2021, https://w3c.github.io/did-core/ Online, [Consultado em 06/2022].

[56] Manu Sporny, Dave Longley, David Chadwick, "Verifiable Credentials Data Model v1.1", W3C Recommendation, March 2022, https://www.w3.org/TR/vc-data-model/ Online, [Consultado em 06/2022].

[57] Ricardo S. Alonso, Inés Sittón-Candanedo, Óscar García, Javier Prieto, Sara Rodríguez-González, "An intelligent Edge-IoT platform for monitoring livestock and crops in a dairy farming scenario", Ad Hoc Networks, Volume 98, 2020, 102047, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2019.102047.

[58] Nurgazina, J.; Pakdeetrakulwong, U.; Moser, T.; Reiner, G. Distributed Ledger Technology Applications in Food Supply Chains: A Review of Challenges and Future Research Directions. Sustainability 2021, 13, 4206. https://doi.org/10.3390/su13084206

[59] P. Nikander, J. Autiosalo and S. Paavolainen, "Interledger for the Industrial Internet of Things," 2019 IEEE 17th International Conference on Industrial Informatics (INDIN), 2019, pp. 908-915, doi: 10.1109/INDIN41052.2019.8972167.

[60] IOTA Foundation, "An Open, Feeless Data And Value Transfer Protocol", https://www.iota.org/get-started/what-is-iota, Online, [Consultado em 06/2022].

[61] Hedera, "HBAR: Incredibly fast. Predictably low fees. Finality in seconds", https://hedera.com/hbar, Online, [Consultado em 06/2022].

[62] Autoridade Nacional de Comunicações (ANACOM), "Utilização da Internet das Coisas: Segmento residencial e empresarial", Relatório, 2021, Online, [Consultado em 07/2022].

[63] CMMI Institute, "Capability Maturity Model-Integration (CMMI)", https://www.cmmiinstitute.com/, Online, [Consultado em 07/2022].

[64] Tecnalia, "IT-Mark", http://it-mark.eu/, Online, [Consultado em 07/2022].

[65] Instituto Nacional de Estatística (INE), "Empresas em Portugal - 2020", 2022, ISSN 0872-9514, https://www.ine.pt/xurl/pub/15413305, Online, [Consultado em 07/2022].

[66] Philip, Nada Y., et al. "Internet of Things for in-home health monitoring systems: current advances, challenges and future directions." IEEE Journal on Selected Areas in Communications 39.2 (2021): 300-310.

[67] Ali O, Ishak MK, Bhatti MKL. 2021. Emerging IoT domains, current standings and open research challenges: a review. PeerJ Computer Science 7:e659

[68] Qu Z, Zhang G, Cao H, Xie J. 2017. LEO satellite constellation for Internet of Things. IEEE Access 5:18391–18401

[69] Akyildiz IF, Kak A. 2019. The Internet of Space Things/CubeSats: a ubiquitous cyber-physical system for the connected world. Computer Networks 150(3):134–149

[70] Li S, Qu W, Liu C, Qiu T, Zhao Z. 2019. Survey on high reliability wireless communication for underwater sensor networks. Journal of Network and Computer Applications 148(3):102446.

[71] B. Atakan, S. Galmes and O. B. Akan, "Nanoscale Communication With Molecular Arrays in Nanonetworks," in IEEE Transactions on NanoBioscience, vol. 11, no. 2, pp. 149-160, June 2012.

[72] Petermann, T.; Bradke, H.; Lüllmann, A.; Poetzsch, M.; Riehm, U. What Happens during a Blackout: Consequences of a Prolonged and Wide-Ranging Power Outage; BoD: Norderstedt, Germany, 2014.

[73] E-ISAC. Analysis of the Cyber Attack on the Ukrainian Power Grid. Available online: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf (acedido em Março 2022).

[74] Radoglou-Grammatikis, P.; Sarigiannidis, P.; Giannoulakis, I.; Kafetzakis, E.; Panaousis, E. Attacking IEC-60870-5-104 SCADA Systems. In Proceedings of the 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 8–13 July 2019; Volume 2642.

[75] D. J. S. Cardenas, A. Hahn and C. -C. Liu, "Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations," in IEEE Access, vol. 8, pp. 61161-61173, 2020.

[76] E. Sisinni, A. Saifullah, S. Han, U. Jennehag and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," in IEEE Trans. on Industrial Inf., vol. 14, no. 11, pp. 4724-4734, Nov. 2018.

[77] T. M. F.-Caramés and P. F.-Lamas,"A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories," in IEEE Access, vol. 7, pp. 45201-45218, 2019.

[78] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K. F. Tsang and J. Rodriguez, "Massive Internet of Things for Industrial Applications: Addressing Wireless IIoT Connectivity Challenges and Ecosystem Fragmentation," in IEEE Industrial Electronics Magazine, vol. 11, no. 1, pp. 28-33, March 2017.

[79] McKinsey & Company, "Cybersecurity in automotive", 2020. Acedido online em 18/02/2022.

[80] Chalermpong Senarak, "Port cybersecurity and threat: A structural model for prevention and policy development, The Asian Journal of Shipping and Logistics", Volume 37, Issue 1, 2021, Pages 20-36, ISSN 2092-5212. doi: 10.1016/j.ajsl.2020.05.001.

[81] Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, Prakash Ranganathan, "Cybersecurity challenges in vehicular communications", Vehicular Communications, Volume 23, 2020, 100214, ISSN 2214-2096. doi: 10.1016/j.vehcom.2019.100214.

[82] Schank, Roger C. "What is AI, anyway?." AI magazine 8.4 (1987): 59-59.

[83] Chaudhary, Harsh, et al. "A review of various challenges in cybersecurity using artificial intelligence." 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS). IEEE, 2020.

[84] Tewari, Anand Shanker, et al. "User-centric hybrid semi-autoencoder recommendation system." Multimedia Tools and Applications (2021): 1-14

[85] Holzinger, Andreas, et al. "Explainable AI methods-a brief overview." International Workshop on Extending Explainable AI Beyond Deep Models and Classifiers. Springer, Cham, 2022

[86] Security, IT. "Inteligência Artificial: A Cibersegurança Para Além Dos Humanos". IT Security, 2022, https://www.itsecurity.pt/news/analysis/inteligencia-artificial-a-ciberseguranca-para-alem-dos-humanos.

[87] Haenlein, Michael, and Andreas Kaplan. "A brief history of artificial intelligence: On the past, present, and future of artificial intelligence." California management review 61.4 (2019): 5-14.

[88] Davenport, Thomas, et al. "How artificial intelligence will change the future of marketing." Journal of the Academy of Marketing Science 48.1 (2020): 24-42.

[89] Bertino, Elisa. "Attacks on Artificial Intelligence [Last Word]." IEEE Security & Privacy 19.1 (2021): 103-104.

[90] Timmis, Jon, et al. "An overview of artificial immune systems." Computation in cells and tissues (2004): 51-91.

[91] Aickelin, U., Dasgupta, D. (2005). Artificial Immune Systems. In: Burke, E.K., Kendall, G. (eds) Search Methodologies. Springer, Boston, MA. https://cije.up.pt/client/doi.org/10.1007/0-387-28356-0_13

[92] LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton. "Deep learning." nature 521.7553 (2015): 436-444.

[93] Liu, Hongyu, and Bo Lang. "Machine learning and deep learning methods for intrusion detection systems: A survey." applied sciences 9.20 (2019): 4396.

[94] Javaid, Ahmad, et al. "A deep learning approach for network intrusion detection system." Eai Endorsed Transactions on Security and Safety 3.9 (2016): e2.

[95] Ahmad, Zeeshan, et al. "Network intrusion detection system: A systematic study of machine learning and deep learning approaches." Transactions on Emerging Telecommunications Technologies 32.1 (2021): e4150.

[96] Maseer, Ziadoon Kamil, et al. "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset." IEEE access 9 (2021): 22351-22370.

[97] A. Stone, "Natural-Language Processing for Intrusion Detection," in Computer, vol. 40, no. 12, pp. 103-105, Dec. 2007, doi: 10.1109/MC.2007.437.

[98] Chowdhary, KR1442. "Natural language processing." Fundamentals of artificial intelligence (2020): 603-649

[99] Kouliaridis, Vasileios, and Georgios Kambourakis. "A comprehensive survey on machine learning techniques for android malware detection." Information 12.5 (2021): 185.

[100] Singh, Jagsir, and Jaswinder Singh. "A survey on machine learning-based malware detection in executable files/0000000001/4-ines-costa_1677.pdf." Journal of Systems Architecture 112 (2021): 101861.

[101] Hemalatha, Jeyaprakash, et al. "An efficient densenet-based deep learning model for malware detection." Entropy 23.3 (2021): 344.

[102] Yadav, Balram, and Sanjiv Tokekar. "Recent innovations and comparison of deep learning techniques in malware classification: a review." International Journal of Information Security Science 9.4 (2021): 230-247.

[103] Masum, Mohammad, et al. "Ransomware classification and detection with machine learning algorithms." 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2022.

[104] Urooj, Umara, et al. "Ransomware detection using the dynamic analysis and machine learning: A survey and research directions." Applied Sciences 12.1 (2021): 172.

[105] Poudyal, Subash, et al. "A multi-level ransomware detection framework using natural language processing and machine learning." 14th International Conference on Malicious and Unwanted Software" MALCON. No. October 2015. 2019.

[106] Qin, Bin, Yalong Wang, and Changchun Ma. "API call based ransomware dynamic detection approach using TextCNN." 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE). IEEE, 2020.

[107] Barati, Mehdi, et al. "Distributed Denial of Service detection using hybrid machine learning technique." 2014 International Symposium on Biometrics and Security Technologies (ISBAST). IEEE, 2014.

[108] Imamverdiyev, Yadigar, and Fargana Abdullayeva. "Deep learning method for denial of service attack detection based on restricted boltzmann machine." Big data 6.2 (2018): 159-169.

[109] Somesha, M., et al. "Efficient deep learning techniques for the detection of phishing websites." Sādhanā 45.1 (2020): 1-18.

[110] Yi, Ping, et al. "Web phishing detection using a deep learning framework." Wireless Communications and Mobile Computing 2018 (2018).

[111] Basnet, Ram, Srinivas Mukkamala, and Andrew H. Sung. "Detection of phishing attacks: A machine learning approach." Soft computing applications in industry. Springer, Berlin, Heidelberg, 2008. 373-383.

[112] Kiruthiga, R., and D. Akila. "Phishing websites detection using machine learning." International Journal of Recent Technology and Engineering 8.2 (2019): 111-114.

[113] Peng, Tianrui, Ian Harris, and Yuki Sawa. "Detecting phishing attacks using natural language processing and machine learning." 2018 IEEE 12th international conference on semantic computing (icsc). IEEE, 2018.

[114] Salloum, Said, et al. "Phishing email detection using natural language processing techniques: a literature survey." Procedia Computer Science 189 (2021): 19-28

[115] https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges/at_download/fullReport

[116] Baylon, Caroline et al. Artificial Intelligence Cybersecurity Challenges. 2020, https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges. Accessed 20 Jan 2022.

[117] "Proteger O Futuro Da AI E O ML Na Microsoft - Security Documentation". Docs.Microsoft.Com, 2022, https://docs.microsoft.com/pt-pt/security/engineering/securing-artificial-intelligence-machine-learning.

[118] "AI PORTUGAL 2030" Portugal Incode.2030, 2022, https://www.incode2030.gov.pt/en/ai-portugal-2030

[119] https://ec.europa.eu/commission/presscorner/detail/pt/qanda_21_1683

[120] https://www.cloudfactory.com/training-data-guide

[121] Olatunji, Iyiola E., et al. "A review of anonymization for healthcare data." Big Data (2022).

[122] Majeed, Abdul, and Sungchang Lee. "Anonymization techniques for privacy preserving data publishing: A comprehensive survey." IEEE Access 9 (2020): 8512-8545.

[123] Senavirathne, Navoda, and Vicenç Torra. "On the role of data anonymization in machine learning privacy." 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2020

[124] https://www.o-ran.org/

[125] 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, Release 15 Description, Summary of Rel-15 Work Items (Release 15), 3GPP TR 21.915, v0.0.1, março 2018

[126] 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, Release 16 Description, Summary of Rel-16 Work Items (Release 16), 3GPP TR 21.916, v0.1.0, setembro 2019

[127] 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, Release 17 Description, Summary of Rel-17 Work Items (Release 17), 3GPP TR 21.917, v0.1.0, novembro 2021

[128] https://www.verizon.com/about/our-company/5g/when-will-verizon-have-5g

[129] https://www.sktelecom.com/en/press/press_detail.do?page.page=13&idx=1388&page.type=all

[130] Tong, W., & Zhu, P. (Eds.). (2021). 6G: The Next Horizon: From Connected People and Things to Connected Intelligence. Cambridge: Cambridge University Press. doi:10.1017/9781108989817

[131] https://www.bbc.com/news/business-50258287

[132] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 5G for Europe: An Action Plan, 14 de setembro de 2016, Bruxelas, Bélgica

[133] NIS Cooperation Group, "Report on the cybersecurity of Open RAN", 11 May 2022, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks

[134] https://5gobservatory.eu/market-developments/5g-services/#:~:text=At%20the%20end%20of%20March%202021%2C%205G%20commercial%20services%20had,%2C%20Slovenia%2C%20Spain%20and%20Sweden.

[135] ENISA Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends, Final Version 1.0, ETL 2016, janeiro 2017

[136] https://www.reuters.com/article/us-deutsche-telekom-outages-idUSKBN13O0X4

[137] https://www.itsecurity.pt/news/x-ray/o-que-se-sabe-ate-ao-momento-sobre-o-ciberataque-a-vodafone

[138] https://electrosmogportugal.weebly.com/

[139] NIS Cooperation Group, EU coordinated risk assessment of the cybersecurity of 5G networks, 9 October 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

[140] Council of the European Union, European Parliament, "Directive (EU) 2018/1972 establishing the European Electronic Communications Code", Official Journal of the European Union, L 321, 17/12/2018, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018L1972&from=EN

[141] Connectivity Special Group, "Summary Report of Best Practices - Outcome of phase 1 of the work of the Special Group for developing a common Union Toolbox for connectivity - 16/10/2020-20/12/2020", 20/12/2020, https://ec.europa.eu/information_society/newsroom/image/document/2020-51/compilation_report_special_group_-_summary_and_annex_002_A201FFA5-9ACE-4742-1ACCE7F8A8EC2438_72388.pdf

[142] Global System for Mobile Communications, 5G to power economic growth in Europe, finds GSMA study, ", GSM Association, 18 de setembro de 2018.

[143] EYGM, Optimizing the 5G opportunity in Europe, 2019

[144] Barclays Corporate Banking, 5G: A transformative technology - How the next network upgrade could supercharge your business and the UK economy, 3 de abril de 2019

[145] Deloitte, "5G Empowers - The future of Electricity", 2021 [Online] https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/energy-resources/deloitte-cn-er-5g-empowerment-future-power-en-211130.pdf

[146] McKinsey & Company, "The 5G era - New horizons for advanced electronics and industrial companies", January 2020 [Online] https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/the%205g%20era%20new%20horizons%20for%20advanced%20electronics%20and%20industrial%20companies/the-5g-era-new-horizons-for-advanced-electronics-and-industrial-companies.pdf

[147] http://www.5gensure.eu/

[148] 5G-Ensure, Results of the Open Consultation on "5G Security", 1st International Workshop on 5G Security, Sophia Antipolis, França, 16 de junho de 2016

[149] European Commission, Directorate-General for Communications Networks, Content and Technology, 5G Observatory Quarterly Report 13 Up to October 2021, outubro 2021

[150] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2030 Digital Compass: the European way for the Digital Decade, Bruxelas, Bélgica, 9 de março de 2021

[151] Commission Staff Working Document accompanying the document, Proposal for a Decision of the European Parliament and of the Council establishing the 2030 Policy Programme "Path to the Digital Decade", Bruxelas, Bélgica, 15 de setembro de 2021

[152] NIS Cooperation Group, Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity, julho 2020

[153] W. Buchanan, et al. Will quantum computers be the end of public key encryption? Journal of Cyber Security Technology, vol. 1, pp 1-22 (2017).

[154] P. Benioff. The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines. J Stat Phys, vol. 22, pp 563-591, (1980).

[155] C. H. Bennett. Logical reversibility of computation. IBM Journal of Research and Development, vol. 17, pp 525-532, (1973).

[156] R. P. Feyman. Simulating Physics with Computers. . Int J Theor Phys, vol. 21, pp 467-488 (1982).

[157] D. Deutsch. Quantum theory, the Church–Turing principle and the universal quantum computer. Proc. R. Soc. Lond. A, vol. 400, pp. 97–117 (1985).

[158] D. Deutsch et al. Rapid solutions of problems by quantum computation. Proceedings of the Royal Society of London A, vol. 439, 553–558, (1992).

[159] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124–134, (1994).

[160] B. Schumacher. Quantum coding. Phys. Rev. A, vol. 51, pp. 2738—2747, (1995)

[161] L. Grover. A fast quantum mechanical algorithm for database search. Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing, pp. 212–219, (1996)

[162] J. A. Jones, et al. Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer. J. Chem. Phys., vol. 109, pp 1648 (1998).

[163] I. L. Chuang, et al. Experimental Implementation of Fast Quantum Searching. Phys. Rev. Lett., vol. 80, pp 3408-3411, (1998).

[164] M. Amico, et al. Experimental study of Shor's factoring algorithm using the IBM Q Experience. Phys. Rev. Lett., vol. 100, pp 012305, (2019).

[165] C. Gidney, et al. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, vol. 5, pp 433, (2021).

[166] É. Gouzien, et al. Factoring 2048-bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory. Phys. Rev. Lett., vol. 127, pp 140503, (2021).

[167] P. Ball. First quantum computer to pack 100 qubits enters crowded race. Nature, vol. 599, pp 542, (2021).

[168] https://research.ibm.com/blog/ibm-quantum-roadmap

[169] S. Wiesner. Conjugate coding. ACM SIGACT News, vol. 15, pp 78-88 (1983).

[170] A. S. Holevo. Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel. Probl. Peredachi Inf., vol. 9,pp. 3–11. (1973).

[171] J. L. Park. The concept of transition in quantum mechanics. Found Phys, vol. 1, pp 23-33, (1970).

[172] W. K. Wooters, et al. A single quantum cannot be cloned. Nature, vol. 299, pp 802-803 (1982).

[173] C. H. Bennett, et al. Quantum cryptography: Public key distribution and coin tossing. Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore (now Bengaluru), pp 175–179, (1984).

[174] C. H. Bennett, et al. Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working! ACM SIGACT News, vol. 20, pp 78-80, (1989).

[175] A. K. Ekert. Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., vol. 67, pp. 661-663, (1991).

[176] J. S. Bell. On the Einstein Podolsky Rosen paradox. Physics Physique Fizika, vol. 1, pp 195-200, (1964).

[177] G. Brassard, et al. A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties. Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science, pp 362-371, (1993).

[178] A. J. Almeida, et al. Implementation of a two-state quantum bit commitment protocol in optical fibers. J. Opt., vol. 18, pp 015202, (2016).

[179] C. Crepeau. Quantum oblivious transfer. Journal of Modern Optics, vol. 41, pp 2445-2454, (1994).

[180] C. Doscher, et al. An introduction to quantum coin-tossing. Fluctuation and Noise Letters, vol. 2, pp. R125-R137, (2002).

[181] E. Verbanis, et al. 24-Hour Relativistic Bit Commitment. Phys. Rev. Lett., vol. 117, pp 140506, (2016).

[182] D. P.-Garcia, et al. Practical and unconditionally secure spacetime-constrained oblivious transfer. Phys. Rev. A, vol. 98, pp 032327, (2018).

[183] M. Lemus, et al. Generation and Distribution of Quantum Oblivious Keys for Secure Multiparty Computation. Appl. Sci., vol. 10, pp 4080, (2020).

[184] P. Shor, et al. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. Phys. Rev. Lett., vol. 85, pp 441-444, (2000).

[185] A. Muller, et al. Quantum cryptography over 23 km in installed under-lake telecom fibre. Europhys. Lett., vol. 33, pp. 335-339, (1996).

[186] A. Poppe, et al. Practical quantum key distribution with polarization entangled photons. Optics Express, vol. 12, pp. 3865-3871, (2004).

[187] N. Gisin, et al. Quantum cryptography. Rev. Mod. Phys., vol. 74, pp 145-195, 2002.

[188] S. Pirandola, et al. Advances in quantum cryptography. Advances in Optics and Photonics, vol. 12, pp. 1012-1236, (2020).

[189] R. Ursin, et al. Entanglement-based quantum communication over 144 km. Nat. Phys., vol. 3, pp 481, (2007).

[190] H. Takesue et al. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. Nat. Photonics, vol. 1, pp 343, (2007).

[191] J.-Y. Wang, et al. Direct and full-scale experimental verifications towards ground–satellite quantum key distribution. Nat. Photonics 7, pp 387, (2013).

[192] C. Elliott, et al. Current status of the DARPA quantum network. In Quantum Information and Computation III, vol. 5815, pp 138–150 (International Society for Optics and Photonics), (2005).

[193] M. Peev, et al. The SECOQC quantum key distribution network in Vienna. New J. Phys. 11, pp 075001, (2009).

[194] D. Stucki, et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. New J. Phys. 13, pp 123001, (2011).

[195] M. Sasaki, et al. Field test of quantum key distribution in the Tokyo QKD Network. Opt. Express 19, pp 10387, (2011).

[196] T.-Y. Chen, et al. Implementation of a 46-node quantum metropolitan area network. npj Quantum Inf, vol. 7, pp 134 (2021). Y.-Chen, et al. An integrated space-to-ground quantum communication network over 4,600 kilometers. Nature, vol. 589, pp 214-219 (2021).

[197] https://openqkd.eu

[198] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[199] M. Mehic, et al. Quantum Key Distribution: A Networking Perspective. ACM Computing Surveys, vol. 53, pp 1-41, (2021).

[200] IBM Institute for Business Value. The Quantum Decade: A playbook for achieving awareness, readiness, and advantage. (2021). Available from: https://www.ibm.com/downloads/cas/J25G35OK

[201] L. Chen L, et al. Report on Post-Quantum Cryptography (NISTIR 8105). Gaithersburg (MD): National Institute of Standards and Technology, (2016). Available from: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[202] https://qureca.com/overview-on-quantum-initiatives-worldwide-update-mid-2021/

[203] Bernstein D.J. et al. "Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild". In: Sako K., Sarkar P. (eds) Advances in Cryptology - ASIACRYPT 2013. ASIACRYPT 2013. Lecture Notes in Computer Science, vol 8270. Springer, Berlin, Heidelberg, 2013.AQUI BREAK

[204] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[205] https://www.cncs.gov.pt/docs/diretiva-2016.pdf

[206] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/

[207] https://www.cshub.com/cloud/interviews/harmonization-is-key-to-european-cloud-certification-scheme

[208] https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

[209] https://www.justice.gov/dag/page/file/1152896/download

[210] https://www.enisa.europa.eu/events/eventfiles/enisa-cybersecurity-certification-of-cloud-services-presentation

[211] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN

[212] https://www.cloudsavvyit.com/7694/what-does-schrems-2-mean-for-cloud-computing/

[213] https://novaconsumerlab.novalaw.unl.pt/inteligencia-artificial-regulamentos-e-plano-coordenado-da-uniao-europeia/

[214] https://dre.pt/dre/detalhe/lei/27-2021-163442504

[215] https://cije.up.pt/client/files/0000000001/4-ines-costa_1677.pdf

[216] https://dre.pt/dre/detalhe/decreto-lei/65-2021-168697988

[217] https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Centro Nacional de Cibersegurança
Rua da Junqueira, 69 | 1300-342 Lisboa
cncs@cncs.gov.pt
(+351) 210 497 400